
The battle has been won, but the war is not over: A study of the end-user remediation of mobile phone users infected by smishing-based malware and the misalignment thereof

Master thesis submitted to Delft University of Technology
in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in Complex Systems Engineering and Management
Faculty of Technology, Policy and Management

by

Artur Anton Geers

Student number: 4486811

To be defended in public on September 26th 2022

GRADUATION COMMITTEE

Chairperson : Dr.ic. C. Hernandez Ganan, Organisation and Governance

First Supervisor : Dr. S.E. Parkin, Organisation and Governance

Second Supervisor : Dr. A. Ding, Information and Communication Technology

External Supervisor : R. Teunissen, KPN Cyber Abuse

September 19, 2022



Acknowledgements

With this report, my Master's degree in Complex Systems Engineering and Management with a specialisation in Information and Communication, is concluded. This conclusion marks the end of my academic journey in Delft, which has lasted for 6 years. The time spent studying and living in Delft has taught me a lot and I am thankful for that.

For conducting the research in this report, I would, especially like to thank my first supervisor, Simon Parkin, who helped me find this topic and helped me, in cooperation with Carlos Hernandez Ganan, to form an inspiring graduation committee. The many hours meeting online, helping me with issues I encountered, suggesting me to research certain aspects and read very relevant articles, supporting and encouraging me in following all possible leads I could find and trying to make piece a coherent picture together from my sometimes incoherent updates, has helped me a lot with my research and I am thankful for the supervision.

Carlos Hernandez Ganan, the chair of the graduation committee, has helped me significantly too, for which I am also very thankful. In the meetings we had, Carlos helped me a lot by giving very critical feedback and helping me with organising the whole Master Thesis, including helping me with and reminding me of the forms and deadlines.

I would also like to thank Raymond Teunnissen, the supervisor from KPN, who helped me conduct and improve my research by providing me with all the data I was able to use, by facilitating the research I was able to perform on the KPN customers and data, and by connecting me with others inside and outside KPN. I am thankful for having gotten the opportunity to perform this research as part of KPN, even though it was not always easy getting information from others.

Aaron Ding, the second supervisor, has helped me significantly too, by always providing very critical feedback that has helped me focus on the important aspects and by including me in the research update talks that occur monthly, which have been inspiring and have helped me put my research struggles in perspective by hearing others discuss the issues they face and being able to ask questions about and weigh in on their research.

Furthermore, I would like to thank my parents and sister, who have facilitated my journey from much earlier and who have helped me during both my research and education in general. My friends have helped me tremendously as well, during the many hours on and off campus. I am very thankful for both my friends and family helping me out, entertaining me (when needed) and inspiring me.

Executive summary

The surge of services and tasks performed on mobile phones is accompanied by an ever-increasing amount of personal data about the owner. This has made mobile phones ideal targets for cyber criminals and it has translated into an increase in malware targeting mobile phones. Social engineering threat actors have very effectively adopted SMS texts, as these are universally trusted by phone users, for Flubot, a new and very dangerous malware. The malware spreads through SMS texts and secretly harvests personal and financial information. Because of the novelty of the malware and its tactics, academic and industrial knowledge is very scarce on how to remediate such infections and how to best involve victims.

This research is focused on better understanding how the remediation has influenced the impact Flubot has had on victims and smartphone users in general. A quantitative research approach, based on a survey of victims within a large Dutch telecom provider's client database, was used. This was aided by desk research, an interview with an active case of Flubot and expert input (employed by telecom providers and governmental bodies). The research divides the remediation process in four stages, namely cause, remediation, harm and experience. These four stages were then used to guide the quantitative research, including the results gained from surveys. For the selection of data subjects for the quantitative research, three different target groups were chosen. Only one target group yielded, the Flubot victims that have been detected through the IP - Command & Control server detection method, significant responses and results. The desk research, on the other hand, is mostly focused on the remediation advice, the evolution of Flubot itself (including the infection trend and malware updates that impact the remediation process) and the application of the Fogg Behavior Model on end-users regarding remediation, to better understand what might trigger certain target groups to or not to remediate the infection. The larger environment Flubot functioned in, was analysed too, as it was developed over time and by June of 2022 it had been taken down. This resulted in less urgency to participate in this research, less potential data subjects to reach and the need to redesign the research.

The quantitative research in combination with the desk research resulted in a number of findings. It was found that the detection methods used against Flubot, before it was taken down, were ineffective in detecting and stopping the spread of the malware. The consensus between government (based on their official stance) and industry was that there was no urgency to do much about the malware, which resulted from being unaware of the more recent workings of Flubot. Furthermore, it was found that victims were unaware of what Flubot was and how it was caused, even though they did remediate the infection, which lowers their ability to prevent future infections. It is important to prevent further infections, as similar malware does exist, functioning on similar principles, and there is a chance that Flubot might reappear. Regarding the remediation process, solely data loss and financial harm are addressed, however, psychological harm was found to be an important issue for victims too, which is completely unaddressed. Addressing the different types of harm can help prevent lasting impacts or at least lower the impact of the infection. In the later months of Flubot, end-users were completely left to their own device to suspect an infection and the accessible information is often inadequate to determine whether an infection had occurred, if the end-user would have been able to pinpoint the suspicion to be caused by Flubot.

The research is based on victims and there was no target group reached that had not been victimised. This makes for a possibly skewed understanding of the situation which should be researched. The data has been gathered through one of the largest telecom providers of the Netherlands, which is not necessarily representative for the whole Dutch industry. Researching other telecom providers in and outside the Netherlands could provide a more comprehensive understanding. The research has led to recommending an adaptive notification systems, improvements to the notifications currently used for both KPN (and other telecom providers) and services that have been imitated by Flubot or are likely to be imitated by smishing-based malware. The research has identified relevant aspects to be researched, namely the usage of an adaptive remediation process for end-users with different security behaviour intentions, the impact of Flubot on a more general population, not just victims, the usage of social triggers for creating a platform or environment that facilitates a self-sustaining cycle of improved security behaviour, and a detailed understanding of the influence of technical skill on the remediation of smishing-based malware. The identified research topics can improve the cyber environment, and the security thereof, for smartphone users.

Contents

Acknowledgement	ii
Executive summary	iii
List of Figures	vii
1 Introduction	1
1.1 Research outline	3
2 Background	5
2.1 Smishing-based malware (i.e. Flubot)	5
2.1.1 Similar malware	6
2.1.2 Detection methods	6
2.1.3 Flubot’s functionalities	7
2.1.4 Flubot evolution and timeline	8
2.2 ISP - telecom provider potential in this landscape	8
2.3 Possible cyber harm types	9
2.4 Behaviour analysis: Fogg Behavior Model	10
2.5 Preventive measures	10
2.5.1 Informing and educating	10
2.5.2 Operating system measures	11
2.5.3 Additional measures on the device	11
2.6 Reactive measures	12
2.6.1 Notifying	12
2.6.2 Walled garden notification	12
3 Selection of the knowledge gap	13
3.1 Literature review	13
3.1.1 Reasons for downloading smishing-based malware	14
3.2 Academic Knowledge Gaps	14
3.3 Research questions	16
3.3.1 SRQ 1: Are mobile end-users aware of a Flubot infection?	16
3.3.2 SRQ 2: How have end-users acted on the Flubot infection?	16
3.3.3 SRQ 3: Which types of harm have end-users experienced by Flubot and are there indicators?	16
3.3.4 SRQ 4: How have end-users perceived the remediation process?	16
3.3.5 SRQ 5: How do available Flubot detection methods, of a Dutch ISP and telecom provider, align with the end-users’ awareness?	17
4 Methodology	19
4.1 Quantitative research	19
4.1.1 Qualitative addition	20
4.2 Desk research	20
4.3 Target group 1: Aware uninfected end-users	22
4.4 Target group 2: Previously infected end-users	22
4.4.1 Survey	23
4.4.2 Analysis of survey results	25
4.5 Target group 3: Currently infected end-users	26

4.5.1	Interview	27
4.6	Limitations of the methodology	27
4.7	Ethics	28
5	Results	30
5.1	Target group 2: Surveys	30
5.1.1	Descriptive statistics	30
5.1.2	Demographics	30
5.1.3	Cause	32
5.1.4	Remediation	35
5.1.5	Harm	35
5.1.6	Experience	38
5.1.7	Correlations	40
5.2	Target group 3: Interviews	42
5.3	Desk research	42
5.3.1	End-user remediation advice	42
5.3.2	Flubot evolution	44
5.3.3	Limitation of current detection methods	46
5.4	Fogg Behavior Model applied to end-user remediation	46
5.4.1	Motivation	47
5.4.2	Ability	47
5.4.3	Prompt/trigger	47
5.4.4	For prevention	48
6	Discussion	50
6.1	Notification	50
6.2	Age	51
6.3	Profession and perceived skill level	52
6.4	Prior knowledge and cause infection	52
6.5	SMS texts received and likelihood of clicking on a text from an unknown sender	53
6.6	Suspicion and remediation	53
6.7	Harm	54
6.7.1	Types of harm linked	55
6.8	Satisfaction with the information and support provision	55
6.9	Changed phone interaction	57
6.10	(Incorrect) malware conclusions	57
6.11	Limitations of the conducted research	57
7	Conclusion	60
7.1	How has Flubot impacted consumers, of a Dutch ISP and telecom provider, with an infected mobile phone?	60
7.2	SRQ 1: Are mobile end-users aware of being infected by Flubot?	61
7.3	SRQ 2: How have end-users acted on the Flubot infection?	61
7.4	SRQ 3: Which types of harm have end-users experienced by Flubot and are there indicators?	62
7.5	SRQ 4: How have end-users perceived the remediation process?	62
7.6	SRQ 5: How do available Flubot detection methods, of a Dutch ISP and telecom provider, align with the end-users' awareness?	62
7.7	Contribution to the academic knowledge	63
7.8	Societal contribution	63
7.9	Recommendations	64
7.9.1	Companies imitated by smishing-based malware (e.g. DHL, UPS and Adobe) and companies likely to be imitated by smishing-based malware	64
7.9.2	KPN and similar telecom providers	64
7.10	Future research	66
	Bibliography	68
	A Notification of Flubot infection	73

B Notification on KPN forum to participate in interview	75
C Additional information provided by KPN on Flubot	77
D Email notifications and the survey pre-participating notification	78
E Set of (follow-up) questions for the semi-structured interview	82
F Survey	88
G Survey answers: Profession	97
H Summarised interview transcript	98
I Spearman's Correlation on survey result variables	100
J Active cases descriptive statistics	105
K Forum customer feedback on rigorousness of SMS auto block	106

Abbreviations :

2FA - Two-Factor Authentication
SFA - Single Factor Authentication
ISP - Internet Service Provider
C&C - Command Control
ECN - Electronic Communication Network
ECS - Electronic Communication Service
OS - Operating System IoT - Internet-of-Things
BYOD - Bring Your Own Device
VCFA - Verification Code Forwarding Attack
SETA - Security Education, Training and Awareness
TA - Threat Actor

List of Figures

2.1	The process and sequence of a Flubot infection (i.e. for Android phones) or subscription scam (i.e. for iPhones) from a victim’s perspective	6
2.2	The IP-CC remediation process [89]	7
2.3	The timeline of Flubot, according to Fox-IT [89]	8
2.4	Diagram of how telecom providers/ISPs (e.g. KPN) are positioned in the landscape of smishing-based malware infections, with the current detection mechanisms	9
2.5	Fogg Behavior Model, based on motivation, ability and a trigger (or prompts) ([102])	10
3.1	Research questions and sub research questions including the type of questions posed in the interviews and surveys	17
3.2	The remediation process divided in the four important aspects	18
4.1	Performed qualitative and quantitative research flow regarding the three target groups	21
4.2	The survey questions and possible answers, linked with the aspects or sub research questions to be answered (Demographics, SRQ 1 and SRQ 2)	24
4.3	The survey questions and possible answers, linked with the aspects or sub research questions to be answered (SRQ 3 and SRQ 4)	25
5.1	Histogram of the age distribution of the survey respondents, including the normal distribution	31
5.2	Grouped professions: working, unemployed and retired	31
5.3	Histogram of the perceived ability to recover and use a smartphone, on a scale from very inexperienced (1) to very experienced (5)	32
5.4	Chart showing through which source categories the 87 respondents came to know about Flubot	32
5.5	Answers given regarding whether the respondent suspected something on their phone, and the elaborations given if that is the case	33
5.6	Answers regarding whether the respondent had an inclination of the cause of the infection, and the elaboration given if that is the case	34
5.7	Histogram of the frequency of the average number of SMS texts the respondents received weekly, excluding friends and family	34
5.8	Histogram of the frequency of the likelihood of respondents to click on a SMS text from an unknown sender, from very unlikely (1) to very likely (5)	35
5.9	Answers on the question whether the respondent has remediated the infection and the elaboration given if that is not the case	36
5.10	Histogram of how long it took respondents to remediate the infection, out of the 67 respondents that did remediate the infection and excluding an outlier that took 60 days to remediate from the graph	36
5.11	Whether the respondents experienced harm and whether it was before or after being notified, included are the elaborations given about the harm (out of 46 respondents having submitted that harm had been experienced)	37
5.12	Chart of the harm types that have been selected and the rating of the impact that was awarded to the harm types	37
5.13	Graph of the average rating awarded to the harm types and the frequency of the harm type	38
5.14	Chart of the frequency of the ratings provided on the information and support provision by KPN	38
5.15	The categorised elaborations respondents gave regarding their satisfaction ratings	39
5.16	The elaborations respondents gave on how their interaction with their phone changed	40
5.17	Correlations found in the survey results, of a 2-tailed significance of 0.01 and less	41
5.18	Correlations found in the survey results, of a 2-tailed significance between 0.01 and 0.05	42

5.19	The timeline of Flubot supplemented with measures and key aspects of Flubot and its remediation ([89])	45
5.20	The criteria, including underlying principles that lead to behaviour change, according to the Fogg Behavior Model [102]	48
5.21	Fogg Behavior Model applied to three end-user target groups	48
5.22	Three target groups of Fig 5.21 applied in the activation graph	49
7.1	The current and recommended adaptive IP-CC notification process	65
A.1	The notification customers receive when an infected smartphone has been detected to their KPN broadband connection, part 1	73
A.2	The notification customers receive when an infected smartphone has been detected to their KPN broadband connection, part 2	74
B.1	Notification in Dutch posted on KPN forum to participate in an interview on why end-users did not click the malicious link inside a suspicious text	76
C.1	The additional information customers and potential victims are directed to, about Flubot and how it works	77
D.1	The email that was sent to, still active, cases to participate in the interview, regarding being contacted by telephone by KPN, i.e. the researcher	79
D.2	The email older cases were sent to participate in the survey	80
D.3	The notification older cases were shown before participating in the survey	81
E.1	The prepared set of questions for the semi-structured interview, conducted in Dutch and therefore prepared in Dutch, page 1	84
E.2	The prepared set of questions for the semi-structured interview, conducted in Dutch and therefore prepared in Dutch, page 2	85
E.3	The prepared set of questions for the semi-structured interview, conducted in Dutch and therefore prepared in Dutch, page 3	86
E.4	The prepared set of questions for the semi-structured interview, conducted in Dutch and therefore prepared in Dutch, page 4	87
F.1	The survey the respondents were shown regarding the first aspect, demographics	89
F.2	The survey the respondents were shown regarding the second aspect, cause, part 1	90
F.3	The survey the respondents were shown regarding the second aspect, cause, part 2	91
F.4	The survey the respondents were shown regarding the third aspect, remediation	92
F.5	The survey the respondents were shown regarding the fourth aspect, harm, part 1	93
F.6	The survey the respondents were shown regarding the fourth aspect, harm, part 2	94
F.7	The survey the respondents were shown regarding the fourth aspect, harm, part 1	95
F.8	The survey the respondents were shown regarding the fourth aspect, harm, part 2	96
G.1	All professions submitted grouped into two categories, namely: working and unemployed	97
I.1	Correlations, significance and N per variable correlation in SPSS for all ordinal and ratio variables, page 1	101
I.2	Correlations, significance and N per variable correlation in SPSS for all ordinal and ratio variables, page 2	102
I.3	Correlations, significance and N per variable correlation in SPSS for all ordinal and ratio variables, page 3	103
I.4	Correlations, significance and N per variable correlation in SPSS for all ordinal and ratio variables, page 4	104
K.1	Criticism on the rigorousness of the SMS auto block in the KPN forum, page 1	107
K.2	Criticism on the rigorousness of the SMS auto block in the KPN forum, page 2	108
K.3	Criticism on the rigorousness of the SMS auto block in the KPN forum, page 3	109
K.4	Criticism on the rigorousness of the SMS auto block in the KPN forum, page 4	110
K.5	Criticism on the rigorousness of the SMS auto block in the KPN forum, page 5	111

Chapter 1

Introduction

Cybercrime has been increasing exponentially in the last decade. It is estimated that of all the consumers becoming a victim of cybercrime by 2021, 68.8% have been victimized in just 2020, according to a survey performed on 10,000 participants in Western Europe, India, Japan, United States and Australia, by Norton [69]. Another study performed in 2021, published by Kshetri and Sharma, reported an increase of 600% of cybercrimes globally during the Covid-19 pandemic up to and including 2020 [53]. The economical losses as a result of cybercrimes have been estimated to add up to \$6 trillion dollars in 2020 alone and that amount of annual financial losses is estimated to increase up to \$10,5 trillion dollars globally in 2025 [63]. Worldwide, only the US and China have an economy that transcend these financial losses. These vast numbers have urged nations and organizations to increase cybersecurity. A study conducted by Anderson et al. in 2012 already concluded the disproportionate impact and costs cybercriminals have on society [5]. In a follow-up study from 2019 by Anderson et al., it was concluded that the ever-increasing quantities of personal information stored offline and online have been targeted increasingly, which has led to larger security breaches [4].

One of the major developments to improve cybersecurity of end-users is the incorporation of Two-Factor Authentication (2FA) for many services [53]. Single factor authentication is most commonly seen in the form of user login, this form is widely considered to be insecure because "Simple, obvious and easy-to-guess passwords, such as names and age, are effortlessly found via computerized secret key gathering programs" [3]. This development has been further fueled with the recent Covid-19 pandemic forcing most organizations and sectors to provide digital workplaces and services online. A survey performed by McKinsey, a global consulting firm, reported a seven year acceleration of digitally enabled products and services in not even a full year of the Covid-19 pandemic, which are intended to be long lasting [57]. 2FA is most commonly designed to use SMS texts as the second factor. Using 2FA based on SMS is considered safe, efficient and effective because of the simplicity, SMS texts are nothing more than a short message, and because of the possible reach as almost all citizens have a phone capable of receiving SMS texts [17, 43, 77]. The overall percentage of consumers having used 2FA has significantly increased from 28% in 2017 to 53% in 2019 to 79% in 2021, in a study performed by Cisco on 1039 adults in the United States and United Kingdom [17]. These 2FA designs that require a smartphone, in combination with an increase of services and applications being designed for smartphones, make a smartphone a very valuable piece of equipment that performs and manages an ever-increasing volume of tasks, services and valuable data [12, 13, 18, 36, 46].

Mobile devices, often an addition to the tasks performed by laptops and desktops but sometimes the replacement thereof, have become the most popular device the global population uses as 66.6% of the global population now owns a mobile phone as of 2021 [6]. The average user spends more than 4 hours each day on their phone, and since 2019 the smartphone has surpassed laptops and desktops in their share of total web pages looked up [49]. These developments have led to mobile devices being the main data generators and are instrumental for the overall cybersecurity of consumers [19, 46]. Furthermore, as opposed to stationary devices, mobile devices tend to lack a lot of security mechanisms. The vulnerabilities and value of mobile devices have not gone unnoticed by cybercriminals [12, 13, 36, 46]. This has led to mobile devices becoming the predominant targets for cybercriminals. In a study regarding the changing costs of cybercrime from 2012 till 2019 by Anderson et al., it was concluded that the targeted landscape has largely changed from PCs and laptops to smartphones [4].

Because of the arms race between cybercriminals and continuous cybersecurity improvements of mobile devices, cybercriminals have been forced to become more inventive and elaborate, the social engineering the

cybercriminals perform to trick and fraud consumers has become a much bigger threat [43, 45, 55, 77, 90]. One of the more prevalent and impactful tactics of cybercriminals to access mobile devices is by 'smishing' or SMS-phishing [18, 36]. This is an attack to steal personal or financial information from a mobile device by making use of SMS texts, instead of the more common phishing, that is conducted by using email. The occurrence of smishing has skyrocketed during the pandemic, namely an increase of 300% in the first three months in the United States in 2020 and in 2021 smishing has increased a further 80% globally [45, 55].

The steep increase in smishing is not necessarily such a big threat on its own, however it is when the success rate has been reported to be significantly higher compared to email phishing. Publications state that the success rate of smishing can reach up to 50%, whereas conventional phishing campaigns (i.e., email phishing) are reported to be effective a mere 3% of the time [43, 90]. Texts feel more personal than emails. Because of the simplicity of a text, which is one of the important drivers for implementing 2FA, it is easy to misdirect the end-user and they have not yet learned to mistrust mobile messaging like consumers have been taught to distrust emails [45, 78]. The increased effectiveness of smishing, combined with an increasing occurrence make it a big threat for consumers, businesses and networks, as 60% of global enterprises in 2021 have reported that their employees have been targeted by smishing [45].

Flubot, a specific type of smishing-based malware (i.e. malware spread through SMS), is the latest and biggest smishing example that has affected an enormous number of consumers and businesses in a fairly short time. Bitsight already detected 1.3 million IPs used by infected Android devices, from the moment the detection started in March 2021 till January 2022 [96]. Luckily, Flubot was taken down in June of 2022 by a global cooperation of cyber police forces. However, the risks posed by Flubot and other currently functioning smishing-based malware (e.g. SMSControllo and Anatsa) are still present [30, 59, 61, 76, 89]. This specific malware (i.e. Flubot) sends out messages to other phone numbers (generally in the same country), infecting other smart phones from the moment the text is opened and the link inside the text has been clicked on, often, to download a malicious external application. The messages were commonly imitating delivery services, which have become increasingly popular in the last five years and especially during the pandemic, making the smishing campaign only more effective [27, 81, 92].

Once the phone has been infected, the malware instructs the phone to send out a similar text to the contacts stored on the phone and other phone numbers. that the malware retrieves from an infected server, and hides it from the owner of the infected phone, leading to a chain of messages that appear to be trustworthy on first glance. Furthermore, the malware is able to spy on the phone without the user being aware of it, hiding notifications and certain texts from the user, leading to user credentials and sensitive information being recorded and stolen. The malware is so advanced it can prevent antivirus from being downloaded and battery-save mode from being turned on, to track all activity in the background constantly [81, 89]. This malware is more effective on Android phones than on iPhones (operating on iOS) and has evolved over time, including the message that is sent out by the malware [82].

The economical losses estimated to be caused by Flubot as a consequence of phones being hijacked and information being stolen are running in the millions (just in Western Australia in 2021 alone, 81 victims reported to have already lost a total of \$904.000). In these losses, the growing SMS chain that is being sent around, is included as it is common to have to pay per SMS or at least when a SMS limit has been reached [65]. Consequently, the individual network cell of the infected phone is likely to overload which in turn forces operators to block the emitting phone from sending SMS texts [37]. The SMS costs are either borne by the owner of the infected phone or by the provider as some Dutch telecom providers offer an unlimited SMS bundle in their subscriptions. The costs of these unlimited bundles are based on an average of texts being sent over time, according to the cyber abuse specialist at KPN [99], which does not account for a sudden surge in SMS texts due to the smishing-based malware.

Therefore, it is crucial for KPN and similar telecom providers to minimize or preferably negate smishing attacks to prevent the costs from skyrocketing. Furthermore, by mitigating or negating smishing the customer is helped which improves the customer satisfaction and cybersecurity of consumers and businesses. Smishing attacks are not completely considered the telecom providers' responsibility to solve as it largely depends on end-user behaviour (i.e. identifying a malicious text and reporting it or preemptively making use of additional security measures). The end-user is considered the weakest link in the cyber security chain and therefore the link that can improve the most [2, 7, 43]. Still, the European Article 40 EECC mandates that ECN (Electronic Communication Network) and ECS (Electronic Communication Service) providers have to take "appropriate

and proportionate technical and organizational measures to appropriately manage the risks" [37]. That is why the telecom providers' influence and positioning in this ongoing process and environment is instrumental and therefore central in this paper. Further elaboration of the telecom providers' positioning in the landscape that smishing-based malware functions in and why telecom providers are especially suitable for remediating these kinds of malware, will be given in the next chapter.

The research has been conducted as a part of the master's degree in Complex Systems Engineering and Management (CoSEM) in cooperation with the Dutch telecom provider and Internet Service Provider (ISP) KPN (KPN provided the data subjects for this study as it has a market share of 40% of the broadband household connections in the Netherlands, providing a representative share of the Dutch population). The research objective is to analyse how big the impact of Flubot is on mobile phone end-users, in this case users connected to KPN internet modems [14, 50].

This includes analysing and creating insights on:

- how Flubot works and how it has developed over time;
- how it is detected;
- how the understanding of Flubot has influenced how it is dealt with it by organizations;
- how infected consumers have dealt with the infection (given remediation advice);
- how infected consumers have been harmed by the infection and experienced the whole process (from the infection to the lasting effects the whole process has had on the victims);
- and finally, how well the end-user remediation aligns with Flubot.

Furthermore, an analysis has been performed on correlations between relevant aspects, to determine possible aspects to focus on when trying to minimize harm and infections. The insights gained can lead to the improvement of customer satisfaction, measures, remediation advice and the understanding of Flubot; its impact, the policy for it and measures influencing the (perceived) threat, leading to an improved cyber environment for consumers, businesses and the cellular and cyber networks. This thesis creates insights on the impact of being infected by Flubot, the remediation process that follows, and the perception of the mobile phone user on the whole process and the telecom provider specifically. Specific recommendations are made for telecom providers, policy makers and parties that are imitated by smishing-based malware, to facilitate the improvement of the cyber environment for smartphone users. The research performed in this paper is based on a quantitative research method, by means of a survey, and aided with an interview and expert opinion. The insights are created inside a highly complex socio-technical system where diverse private and public stakeholders and actors participate in, in which it is required to manage institutional, technical and process aspects. Where mobile end-users, telecom providers, non-profit security companies and Internet Service Providers have to interact with separate but interdependent social and technological subsystems, satisfying the characteristics of a complex socio-technical system according to Baxter & Sommerville [8]. This makes the research relevant for the master's degree in CoSEM, it includes technological (in particular Information and Communication Technology), social and institutional aspects. The research requires these aspects to be analysed, managed and influenced (i.e. designing solutions, including policy).

1.1 Research outline

In Chapter 2 the background of the topic being researched and the core concepts are addressed. An overview of Flubot; its functionalities and its evolution is also addressed in the background chapter, as well as the behaviour model that is applied in this paper and the different types of cyber harm Flubot victims might experience. In Chapter 3 the review of the literature on this topic is discussed, including the gaps in the academic and industry literature and knowledge that this research aims to fill. Chapter 4 elaborates on the methodology of the research, including the tools used, and the reasons for selecting specific research methods and how the survey and the interview have been prepared, performed and analysed. Chapter 4 also includes the exact phrasing of the questions posed in the survey, and the reasoning for choosing specific types of questions, including the variables they are turned into, for analysis. The methodology for the research in this paper includes the selection of data subjects, which, too, is addressed in Chapter 4. Chapter 5 provides the results of the desk research, the survey, including the correlations between the results of the survey, and the additional interview, which are then put into context and discussed in Chapter 6. In Chapter 6, the relations that have been found between the results of the survey, are combined and correlations that have not been found in these results, but have been

found in other papers, are addressed too. Furthermore, in Chapter 6 covers the question how representative the results are and the limitations of the research, including how well the results and insights created in this paper can be extrapolated to the larger population and wider landscape. The conclusion is provided in Chapter 7, including how well the results have answered the main and sub research questions, the societal and academic relevance, the recommendations for the specific involved parties as a result of the findings and suggestions for future research, based on additional knowledge gaps.

Chapter 2

Background

To provide a complete picture of what Flubot and similar smishing-based malware is, this chapter starts with background information on smishing-based malware, which is then followed up with Flubot specific developments, including a list of the important functionalities. Then other core concepts are addressed and elaborated upon to gain a comprehensive understanding of the (cyber) landscape of this malware and the research on this topic is situated in, including a figure showing the complexities as a result of the many stakeholders involved and how they are involved. The currently deployed detection and remediation mechanisms are addressed in this chapter too, as well as possible measures (both preventive and reactive) that are, generally, suitable for (smartphone) malware.

2.1 Smishing-based malware (i.e. Flubot)

The malware, also known as malicious software (software designed to interfere with a computer's normal functioning according to Merriam Webster Dictionary [58]), researched in this paper is based on mobile phone users clicking on fraudulent links inside SMS messages and often downloading a fraudulent application outside of the regulated application platforms (i.e. Google Play Store). Flubot, formerly known as Cabassous, functions as both a banking trojan (i.e. logging financial credentials, raiding any financial accounts including cryptocurrency applications and inflicting serious financial damage) and spyware (i.e. storing contact information and sending fraudulent texts to contacts, generally with the same country code, without showing it to the user of the infected device or it even being possible to find) [23, 45, 79].

A Flubot infection is different for Android phones than for iPhones. Android OS has been considered to be the lesser of the two alternatives when it comes to security and smishing-based malware has been impacting Android OS users significantly more for that reason. The biggest reason for Android OS being more vulnerable is that it used to be very easy to download applications outside the official channels (i.e. Google App Store), and even when downloading from the Google App Store, there is still a likelihood the application is malicious [36, 91]. Once downloaded, Flubot and similar types of malware, make use of the Accessibility services to control the Android device. This vulnerability is known to be exploited and efforts have been made to limit and or negate these vulnerabilities. However, this function is crucial for providing access to users with disabilities and cannot be deleted easily [68, 104]. iOS makes it impossible to download such malware as it is impossible to install outside Apple's walled garden, that is why iOS users are impacted differently and generally less. iPhone users are redirected to different kinds of social engineering, for example getting redirected to subscription scams [103]. Here the victim is asked to submit personal information, especially credit card or other financial information, leading to the victim getting stuck with subscriptions that are completely irrelevant and only benefit the malware operators.

For the Android phones, an infection leads to the phone connecting to a Command and Control (C&C) server ("a computer that issues directives to digital devices that have been infected with malware") and sharing with the server which applications are installed on the smartphone and all the contacts [97]. The C&C server returns a list with instructions on how to capture information from the different relevant applications, shares a list with phone numbers to send SMS texts to for the malware to keep spreading and the specific text that should be sent, including a link. The infected phone starts capturing all the data on the phone, turns battery-save mode off, starts sending the SMS texts and shares the information gathered from the keylogging and screen capturing (i.e. the means of gathering all the data shown on the screen and typed by the phone user), especially financial

information. This process keeps repeating until the victim realises that the phone is infected and eventually performs a factory reset to remediate the infection.

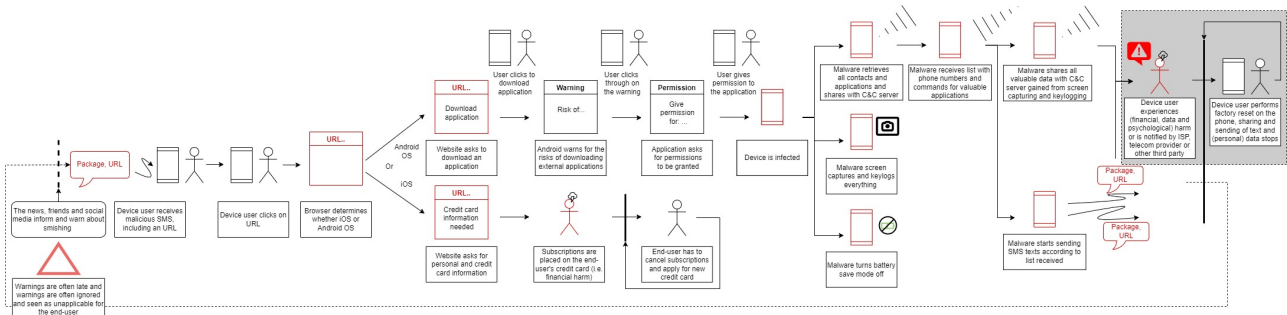


Figure 2.1: The process and sequence of a Flubot infection (i.e. for Android phones) or subscription scam (i.e. for iPhones) from a victim's perspective

Figure 2.1 shows the process of a Flubot infection, from the victim's perspective and where remediation is abstractly been shown to be a single step. Once the malware is deemed dangerous enough, information campaigns are initiated to prevent harm, which have their own downsides as is common with information campaigns (i.e. potential victims expect themselves to never fall for malware).

2.1.1 Similar malware

On June 1, 2022 an announcement was released by the Dutch police and Europol itself, among a larger list of outlets, that Flubot had been taken down [30, 76]. This meant that the spread of this particular smishing-based malware has stopped and therefore no new cases are expected to be reported. However, that has not mitigated the risks. The mechanics of sharing malicious links through SMS texts to infect phones, has been used by multiple other social engineering malware since 2017 [88, 89, 90]. Teabot, Anatsa, BRATA, SMSControllo, Anubis, Cerberus, Oscorp and Ubel (which is most likely a more developed version of Oscorp), and the latest addition, ERMAC 2.0 (based on Cerberus), are examples of mobile malware (generally only targeting Android phones) that use multiple ways of infecting mobile phones, and one of these ways is smishing [9, 21, 22, 42, 56, 59, 60, 87, 101, 105]. These social engineering attacks all rely partly, to a large degree or even completely (Flubot, SMSControllo and Anatsa) on smishing to spread and inflict harm. Of these Flubot was the most popular.

2.1.2 Detection methods

Two automated measures that are integrated by KPN to automatically detect phones infected with Flubot, are discussed in this paper. One is based on the internet traffic between the infected device and an infected C&C server, and the other is based on the SMS traffic. The latter method is based on the spike of SMS texts being sent as a result of the Flubot infection. The system monitors the amount of texts a phone sends and if a threshold of texts sent in a day is met, then that phone is marked as infected and it gets blocked. The owner gets a notification through an email about the block for further information and to remediate the infection. In this document this method is referred to as the 'SMS auto block' method and the cases of phones detected through this method are referred to as the 'SMS auto block cases'.

The former automated system relies on data provided by Shadowserver, a widely trusted non-profit security organization that shares trusted abuse data on the internet [15, 86, 100]. Shadowserver identifies connections between infected C&C servers and IP-addresses belonging to KPN (which infected Android phones connect to, if in a household with a KPN broadband connection) [99]. This method can only detect infected mobile devices connected to a KPN modem. If the mobile device makes use of the KPN cellular network then the mobile device cannot not be detected automatically, the same goes for infected mobile devices connected to broadband connections of other ISPs and telecom providers. The data provided by Shadowserver contains, among others, the timestamp (including the date), source and destination IP-address, country, city and device operating system [99]. This data is enough to identify KPN broadband connections (i.e. KPN modems) that have an infected device connected to them, and to attempt to notify broadband connection owners and, ideally,

the infected device users or owners. Unfortunately, it is not a given that the owner or user can be contacted successfully [15, 99]. The cases detected with this detection method are referred to in this document as the 'IP-CC cases', and the connections between the C&C servers and the KPN IP-addresses are 'IP-CC connections'. The remediation process IP-CC cases go through, is shown in Figure 2.2.

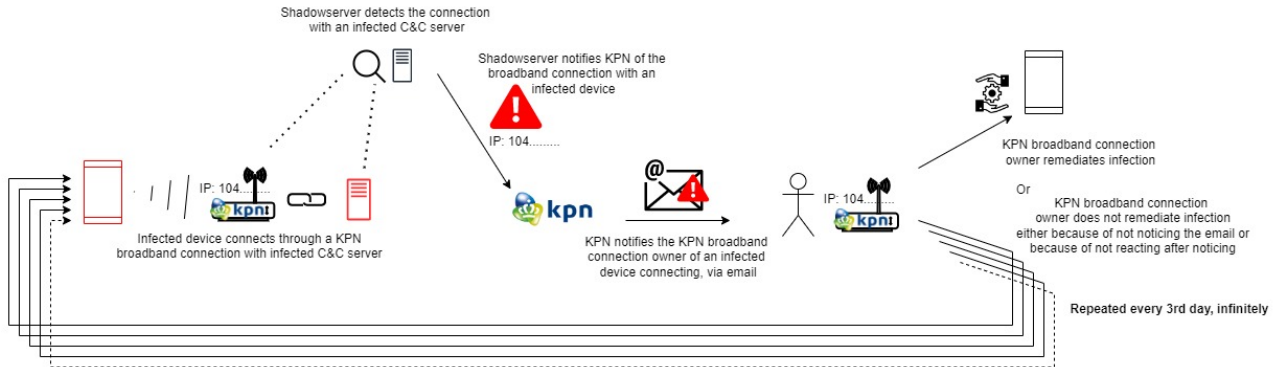


Figure 2.2: The IP-CC remediation process [89]

A simple depiction of the two detection methods in the larger complex systems they participate in, is shown in Figure 2.4 in Subchapter 2.2.

2.1.3 Flubot's functionalities

The more recent versions of Flubot can perform a list of tasks, some of which are performed constantly [68, 70]. The most important ones are [70, 89]:

- Adapting to region: the malware looks up the device's language and changes the texts of the app accordingly, also the country phone prefixes are adjusted for SMS traffic.
- Error Logging: to upload any errors that occurred in the malicious application for future improvements.
- Updating DNS: giving the attacker the ability to switch DNS once the DNS has been blocklisted.
- Intercepting notifications: all notifications an infected phone receives can be logged, this is mostly used for sensitive information and one-time passcodes, which is common when 2FA by SMS is used for services.
- Sending and intercepting SMS texts: the application retrieves a list of phone numbers and the according tricking texts, these numbers are then sent a text, if the retrieved phone numbers are not in the contact list of the infected phone. Flubot can also hide SMS texts received, especially important to not arouse any suspicion as a result of the one-time passwords being sent to the infected phone.
- Logging contacts: the contact list on the victim's phone, including names and phone numbers, will be sent to the C&C server.
- Checking and overlaying: a list of applications on the infected phone is sent to the C&C server to check for which ones there are overlays and injections, for the ones there are an inject or overlay will be configured on the infected device, i.e. every installed application that Flubot has an overlay or inject for, will be compromised.
- Disabling Google Play Protect: the safety check mechanism that is installed on Android phones can be disabled to prevent detection.
- Uninstalling apps: Flubot can uninstall certain apps once they are in the foreground.
- Opening URL: URLs that are shared by the C&C server can be opened on demand on the victim's device, e.g. to pay the attacker through advertisements or by visiting websites that steal the user's data.
- Keylogging: by using Android's Accessibility Service, a function used by the Android framework to make it possible to provide alternative navigation feedback for users with disabilities, it is possible to grab all text on the screen and steal that information [104].
- Disabling Battery Saving: by disabling the apps from being put on hold for the purpose of saving the battery, Flubot can actively perform its functionalities while the phone "sleeps".

2.1.4 Flubot evolution and timeline

When the research started (i.e. February of 2022) it was unclear which exact functions Flubot was performing, nor was it known which version of Flubot was predominant. However, by July 2022 an increasing amount of research on Flubot had been published. By March of 2022, according to Dor, Moshailov and Paganini, Flubot had already reached version 5.2 [68, 70]. Fox-IT, a cybersecurity company, went even further later on and stated that version 5.2 was already circulating by the end of January, and added to that that versions up to 5.6 have circulated since May 2022 [89]. From the first versions of Flubot having appeared in early 2020, the current versions have significantly improved. The arms race between the Flubot Threat Actors (TAs) (i.e. the subjects responsible for developing and operating Flubot) and the security experts trying to mitigate the malware, has led to Flubot having developed significantly and making it only harder to detect and to remediate it. Where it used to be possible to block communication between infected devices and infected C&C servers by using DNS blocklists in versions up to 4.9, this was not useful in version 5.0 anymore, as it eludes these DNS blocklists completely by communicating via DNS-Tunneling-over-HTTPS [68, 70, 89]. In January 2022 already 30.000 of the 170.000 cases recorded by bitsight, were of Flubot 4.9 and up. This percentage increased over time as older versions were easier to stop [96].

Furthermore, version 5.1 had been updated to generate more domains (choosing from a list of 30 domains instead of 3 previously) and version 5.2 made it possible for the attackers to change the domain generation algorithm remotely, as opposed to the previous versions that made use of the month and year for domain name generation (which is very predictable). Version 5.2 also made it possible to make (international) calls secretly, without the device owner being able to notice it, which can be used for pay-through-phone services [68, 70, 89]. Later versions of Flubot 5.2-5.4, active from January 2022 made it possible for the malware to send longer texts by splitting them up and by intercepting the texts received before it was possible for the phone to auto detect and possibly mark the text as dangerous or as spam. These updates were accompanied with cases of another malware, i.e. Medusa, being spread through the Flubot malware too [89]. This was the second time another malware made use of the Flubot distribution network. Teabot had previously made use of the Flubot distribution network in version 4.9. However, unlike previously with Teabot, with Medusa it was suspected, by Fox-IT, that the Flubot Threat Actors (TA) not only sold or shared their distribution network but cooperated and were advised by Medusa TAs to implement the multiple messages function. This suggests that these TAs have gone one step further in joining forces to further improve their malware and create bigger profits. In the latest version of Flubot (i.e. 5.6), the malware could be spread through MMS too, however the effectiveness of that development has not been proven as the malware was taken down shortly after [89]. Fox-IT has made a whole timeline of the different versions of Flubot, shown in Figure 2.3 below.

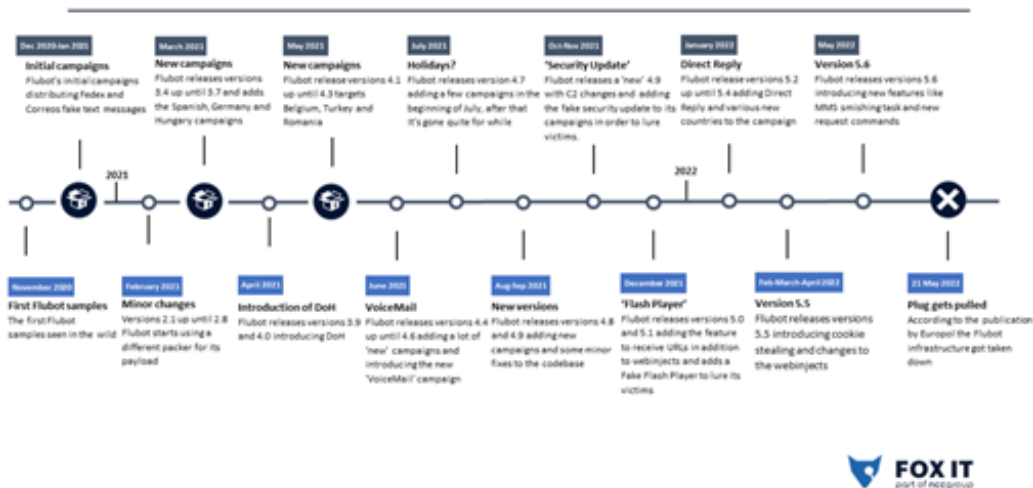


Figure 2.3: The timeline of Flubot, according to Fox-IT [89]

2.2 ISP - telecom provider potential in this landscape

ISPs that are also telecom providers (e.g. KPN) are uniquely situated in the cyber-physical landscape where they have access to the mobile internet, broadband connections and SMS-traffic of mobile end-users. Therefore, their provision of services provides them with significant power when it comes to mobile malware, in particular

smishing-based malware. It is possible to (temporarily) block mobile devices once it has been determined the device has been infected and is infecting others [99]. Furthermore, as mandated by European Article 40 EECC, ECN and ECS providers have to take "appropriate and proportionate technical and organizational measures to appropriately manage the risks" [37]. This implies that it is not only desired and logical that ISPs and telecom providers take appropriate action, but also required by the European Union.

The detection methods ISP/telecom providers have, in cooperation with the information provided by security companies, such as Shadowserver, make them uniquely capable of addressing the remediation of smishing-based malware. Figure 2.4 shows how KPN, in this case, is involved in the whole remediation process. Telecom providers are also sources for counting the amount of cases, which is used by government agencies, i.e. National Cyber Security Center (NCSC), to determine the urgency for needed measures, including information campaigns [64].

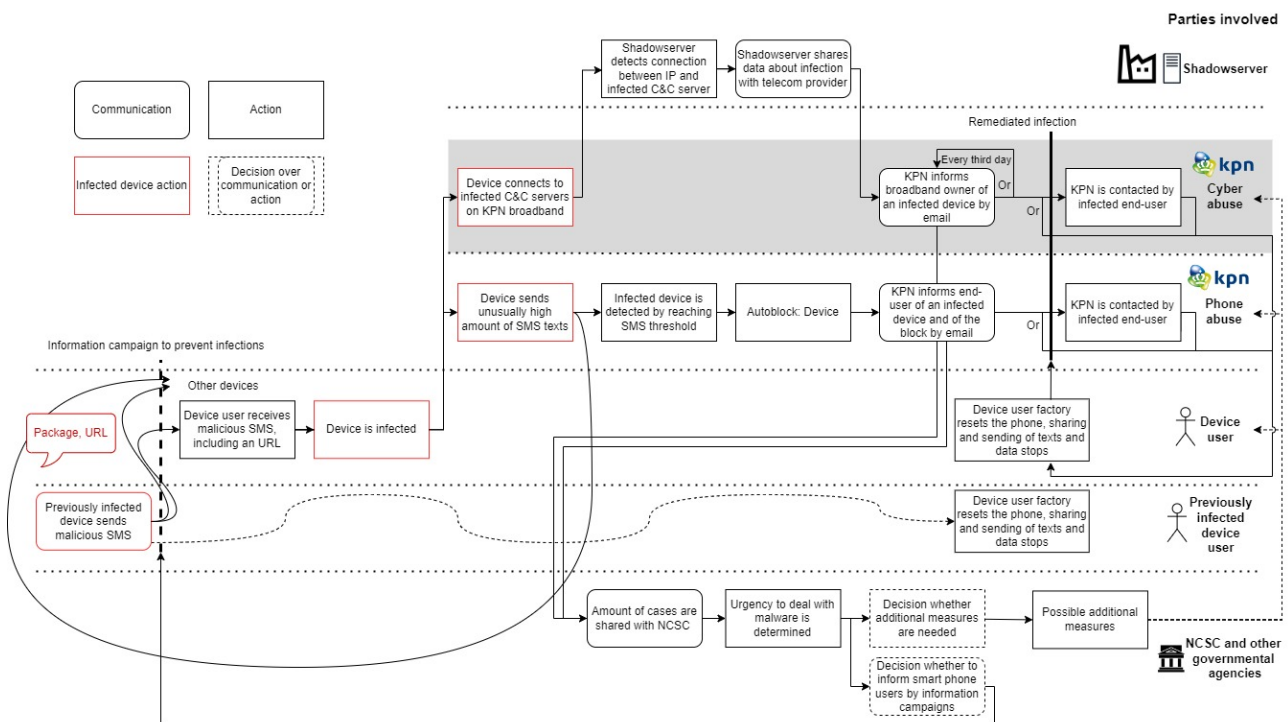


Figure 2.4: Diagram of how telecom providers/ISPs (e.g. KPN) are positioned in the landscape of smishing-based malware infections, with the current detection mechanisms

The diagram above shows an abstract version of how the different parties involved perform tasks (or actions), including informing other stakeholders and having to make certain decisions and which other stakeholders are included in the different action sequences.

2.3 Possible cyber harm types

In articles and information campaigns about Flubot it becomes very clear that victims are likely to experience financial and data loss, however the impact of such malware is bigger than just financial and data loss [39, 70, 82, 98, 103]. Therefore, to understand the impact of Flubot on the end-users comprehensively, different types of harm need to be specified. Agrafiotis et al. have formulated a taxonomy of the different types of cyber harm that end-users might experience. Harm can be divided in *physical or digital harm* (i.e. "harm describing a physical or digital negative effect on someone or something"); *economic harm* (i.e. "harm that relates to negative financial or economic consequences"); *psychological harm* (i.e. "harm which focuses on an individual and their mental well-being and psyche"), *reputational harm* (i.e. "harm pertaining to the general opinion held about an entity"); and *social and societal harm* (i.e. "a capture of harms that may result in a societal context or society more broadly") [1]. To create a comprehensive understanding of the impact of Flubot, it is important to understand not just which types of harm have been experienced, but also the extent of the impact of the

different harm types. Such an understanding helps with creating insights on which harm to prioritize and to address when informing the end-user of a malware infection in later stages.

2.4 Behaviour analysis: Fogg Behavior Model

To understand the behaviour end-users display during the different phases of a smishing-based malware infection, the comprehensive Fogg Behavior Model used by Bouwmeester et al., among others, to analyse behaviour change in IoT infections, will be applied in this research too [11]. Fogg's behaviour model has also been applied by Parkin et al. to determine whether it can be generalized to security behaviour, specifically researching trigger moments for security [72]. Das et al. have applied Fogg's behaviour model to describe and analyse an end-user's predicament of what is needed to get that end-user to change their behaviour, i.e. to determine what the exact security and privacy behavioural triggers are [24]. The Fogg Behavior Model is based on three aspects that are needed for an individual to change their behaviour, namely motivation (i.e. how badly someone wants something), ability (i.e. how capable a person is in doing something), and a trigger (i.e. an event that happens to someone) [32]. This model describes that the stronger the motivation, or the more someone is capable of doing some action, the more likely the behaviour is going to change when a trigger is experienced. The trigger, prompt, cue, call to action, can be an incentive that leads to perform a target behaviour (immediately), ranging from a notification, to being told by someone, to seeing an add [32].

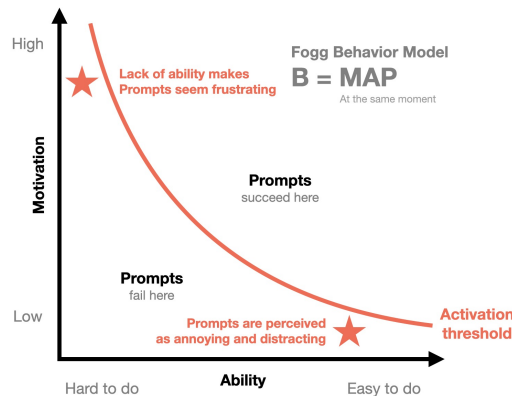


Figure 2.5: Fogg Behavior Model, based on motivation, ability and a trigger (or prompts) ([102])

2.5 Preventive measures

To get an understanding of how smartphone users fall for Flubot and smishing-based malware in general, it is important to understand which measures are currently in place that might affect a user and possibly prevent them from getting infected, or what the limits are of the measures.

2.5.1 Informing and educating

Numerous information campaigns have been introduced to inform mobile phone users on smishing-based malware, their consequences and what to and not to do. For example, in the Netherlands, the national police, KPN, and a number of Dutch banks have initiated campaigns [41, 98]. Educating and informing mobile phone users is a common tactic to limit the effectiveness of phishing attacks, similarly to smishing attacks [19, 36]. However, according to Forget et al. and Wash and Rader, more is not necessarily better when it comes to informing end-users [33, 108]. Information campaigns vary in effectiveness depending on the means of notifying, the notification itself and the target audience it is supposed to reach. Regarding Flubot, it is possible for an end-user that suspects a security issue, to not connect the dots (i.e. that it might be malware). Even if a malware infection is suspected, it is still hard to determine which malware and what the appropriate actions are [81]. Furthermore, to keep advice concise and actionable for the average end-user there is a risk that crucial aspects of the advice are left out for the non-average end-user [35].

Regarding the SMS text that (potential) victims receive, Siadati et al. have researched the effectiveness of including warnings inside 2FA texts, which can be extrapolated to this topic. It was found that by including a single warning at the beginning of the 2FA SMS text, that said something like "Please ignore this message if you did not request a code", people were unlikely to disclose the code included in a 2FA text and more aware of any social engineering attempt [43, 90].

A more impacting proactive measure is training phone users to detect possible dangers and to act appropriately on those dangers, and not just informing. An example of training phone users is the incorporation of security education, training and awareness (SETA) programs by corporations, as the harm of malware are not restricted to consumers. In 2018, a third of the Chief Information Security Officers stated that employee security education and training is the most important priority for the cyber security of a company, according to the Financial Services Information Sharing and Analysis Center [83, 85]. This priority also applies to individuals, meaning that it is crucial for an individual's cybersecurity to improve their awareness about digital threats. However, the effectiveness of SETA programs and, in general, improving the end-user's awareness is debatable when it comes to distinguishing phishing links. According to Pattinson et al. and Reeves et al., SETA programs are often ineffective because of the weak relationship between an employee's level of cyber security training and their capacity to prevent a cyber threat [75, 83].

Parsons et al. went even further and found that providing individuals with frequent cyber security training might hamper their ability to differentiate phishing emails from legitimate ones, compared to individuals with less frequent training [74]. One of the reasons for SETA programs having a potentially adverse effect on cyber security is that employees, just like individuals, experience cyber fatigue [83]. Cyber fatigue, or security fatigue, has been a focus in the field of cyber security and it encompasses the disengagement of security-related behaviour as a result of being overwhelmed by the constant cyber security notifications and measures one is expected to follow and to pay attention to [83].

Research performed by Forget et al. confirms that educating or informing computer users does not always lead to beneficial outcomes [33]. In some cases, disengaged users seem to display less risky behaviour and are therefore more secure. The findings of Forget et al. will be extrapolated to this research as they concern similar security issues.

2.5.2 Operating system measures

Currently there are two operating systems that account for almost the entire smartphone market. Android Operating System (OS) and Apple's OS (iOS), according to Statcounter, account for 99.4% (59.7% and 39.65% respectfully) of smartphones in the Netherlands and 99.12% (66.77% and 32.35% respectfully) globally [93, 94]. This means that the majority of the smartphone owners own an Android, and if not, then almost certainly an iPhone. In an effort to curb the safety and cyber security concerns of Android phones, Android OS has been updated to make it harder to download from outside the Google App Store, forcing the end-user to consider the risks by showing warnings and pop-ups, which it previously did not do clearly [18, 104]. However, the effects of these warnings are limited and end-users still continue downloading external software. According to a survey performed by Jörgensson on 100 mobile phone users, 37% of users download external applications, i.e. not the official application platform [46]. This is corroborated by the constant and undiminished spread of Flubot and other smishing-based malware.

2.5.3 Additional measures on the device

Research has shown that there are additional preventive measures that can be implemented on the smartphone to prevent mobile phone users from falling victim to smishing. Most of the measures found are based on SMS-text analysis, where an application downloaded on the phone or an algorithm used by the telecom provider should be able to detect smishing texts based on the content (i.e. whether certain words likely to be used in smishing texts and links are included). These measures seem to be promising and more and more research and knowledge on that topic is accumulating [18]. However, in the Netherlands SMS texts are constitutionally protected under the secrecy of correspondence, Article 13, meaning that it is not allowed for anyone to read or scan your texts unless a judge has intervened or for national security purposes [38, 73]. This makes it illegal for Dutch telecom providers to make use of such SMS text filtering. It is possible to incentivize and encourage mobile phone users to make use of such SMS text filtering applications themselves, persuading users to download such applications. Unfortunately it is unclear how effective the SMS filtering applications are against smishing-based

malware, as Flubot tends to change messages to avoid the risk that the malicious texts are detected [39].

Another method, mentioned by Chorghé and Shekoker, is the implementation of URL blacklisting, where a database is maintained with websites that are suspected of being used for phishing and smishing and when a user is about to access these blacklisted websites a warning is shown and the page is not loaded [18]. This measure can be implemented preventively, by blacklisting the sites that the end-user gets to see when clicking on a malicious link, after a sizable group of end-users has become victim and the links they clicked on have been shared with the database. The efficacy of this method depends on the percentage of malicious websites being added to the database and on whether the database is constantly updated.

2.6 Reactive measures

2.6.1 Notifying

The responsibility of dealing with mobile phone malware befalls partly on the end-user [2, 43]. It generally is the end-user that is the weakest link in the security chain and that is where most of the cybersecurity improvements can be made, in the case of Flubot, the end-user is less capable of determining whether an infection has occurred because of Flubot's ability to hide itself and its operations, however there is room for improvement [2, 7, 43]. Besides, the measures implemented and performed by ISPs, telecom providers, operating system providers and governmental institutions, end-users are to be equipped with knowledge on how to deal with mobile phone malware reactively. A notification that includes advice on how to deal with a mobile malware infection, such as Flubot, should provide mobile device users with the information needed to remediate the infection or at least provide them with sufficient information to facilitate the remediation otherwise or through other parties. Notifying consumers with advice on how to remediate infections has been researched, however, most of that research is focused on internet users in general and computer users more specifically, as the computer has been the main electronic device consumers have been using up to a couple of years ago [4, 6]. Additional research on appropriate notifying of computer users shows that different user groups need different education and triggering, leading to the conclusion that there is no one-size-fits-all way of notifying and educating computer users effectively [108].

2.6.2 Walled garden notification

Cetin et al. have researched the efficacy of two methods for notifying an IoT user with a malware infection [15]. One method is email-only notification and the other, more promising, method is the walled garden notification (i.e. by restricting the connections the user can make on the internet and notifying them in the process). This measure could be applied to limit the harm posed by smishing-based malware, thereby, limiting the spread of the infection. A parallel drawn from the research performed by Cetin et al. that can be applied in this research, except from employing walled garden notification as a measure, is that of the same issues arising when contacting infected device owners. It is hard to contact large populations effectively and efficiently. Mail works the best, however it does not reach everyone [15].

Given the core concepts mentioned in this chapter, the landscape Flubot functions in and the background of the topic at hand, the next chapter includes the literature search and the review that follows, providing the academic knowledge gap that this research aims to fill and contribute to.

Chapter 3

Selection of the knowledge gap

Crucial for gaining a comprehensive understanding of the current state of academic knowledge on the topic discussed previously, a literature search has been conducted to determine if and where the academic and industrial knowledge gaps are located in the vast and ever-expanding array of literature published.

3.1 Literature review

For the literature review, specific search words were used in combination with boolean operators to narrow down the search results to a workable amount. Different topics were searched for, and, where necessary, multiple search terms were used for the same topic. The search results have also been narrowed down to articles published since 2017, as Flubot itself appeared for the first time in 2020 but its less-sophisticated predecessors have been around since before the Covid-19 pandemic. The first occurrences of literature on smishing date back to 2017, therefore literature on mobile phone malware is limited to articles published since 2017 [88, 90]. Due to the high-paced technological innovations the literature on the topic needs to be as recent as possible, limiting the risk that the information being outdated. The reason for only selecting 5 years worth of literature.

After the selection of articles found, with these search terms and conditions, a forward and backward approach has been applied to find more literature that aligns with the topic at hand. Literature found through this approach is not necessarily excluded if published before 2017 as it is deemed relevant to the research. Some articles from before 2017 have been included in this research too after consideration on how applicable the literature is.

Topic	Version	Search term	Publishing years	Results
1	1	remediation advice mobile phone malware	All	7.350
1	2	remediation advice mobile phone malware AND flubot	All	0
1	3	remediation advice mobile phone malware	2017 - now	3.330
1	4	"remediation advice" AND malware AND ("mobile phone" OR "smart phone") AND flubot	All	0
1	5	remediation advice AND malware AND ("mobile phone" OR "smart phone") -patient -health	2017 - now	1220
1	6	("remediation advice" OR remediation OR remedial) AND malware AND ("mobile phone" OR "smart phone") -patient -health	2017 - now	203
2	7	(user OR advice) remediation) AND "phone malware" OR "mobile malware" AND interview	2017 - now	53
3	8	"fogg behavior model" cybersecurity smartphone	2017 - now	24
4	9	(mobile malware) AND threat AND prioritization AND ("telecom provider" OR telco) -covid	2017 - now	191

Table 3.1: Academic search results in Google Scholar with search terms

Topic 1: User remediation for mobile phone malware For the first topic, the search results have incrementally been lowered to 203. The search was performed to gain the general literature needed that encompasses most of the research performed in this paper. Remediation advice and similar wording have been

included in the search term in combination with phone and malware to find all the necessary articles on this topic. A large number of healthcare related articles have been published that were part of the search results, however those articles are not relevant for the literature required for this review and were therefore excluded.

Topic 2: connection with interviews The first search already provided plenty of literature that is based (partially) on surveys, however there was insufficient literature on the usage and academic practices regarding interviews in the context of this topic. Therefore, the second topic is more directed towards interviews performed in the context of mobile malware and user remediation. The search led to 57 articles of which some have been included in this paper as inspiration and for a better understanding of how interviews have been conducted on this topic.

Topic 3: connection with the behaviour model An initial article from the previous searches led to the decision to make use of a behaviour model. To gain a further understanding of the usage and application thereof, it was decided to perform the third topic search including the term behaviour model. Making use of a behaviour model helps with analysing how end-users do and do not behave in the current situations they often find themselves in before, during and after the infection. A workable number of 24 search results has been found on the Fogg Behavior Model and on the security of phones.

Topic 4: connection to telecom providers The fourth topic searched is on how telecom providers, such as KPN, analyse mobile malware threats. A significant part of recently published literature is about Covid. Therefore, it was decided to exclude Covid related search results. The search yielded a significant amount of 191 results that have been combed through.

The literature searches were performed partially by making use of Google Scholar and Scopus to gain a wide range of scientific articles, however there is a scarce volume of scientific literature on this topic as it is a fairly new one. Therefore, the scientific search in this paper is complemented with reports and articles published by cybersecurity companies, industry magazines and the telecom provider and ISP industries, found through Google Search. This provides a comprehensive understanding of not only the limited academic but also industry knowledge and practices on this topic. The literature search was aided by expert opinions to further improve the comprehensiveness of the research.

3.1.1 Reasons for downloading smishing-based malware

The literature review has provided literature on the factors that lead to smartphone users downloading external applications that have been shared through SMS. Downloading external applications, is considered a big security threat and often the cause of cyber intrusions. Bosamia et al. identified unintentional installation of rogue and malware applications as one of the biggest financial threats [10].

When looking at why end-users click on malicious links, six reasons have been found for why mobile phone smishing attacks are successful. According to Goel and Jain, the reasons are: 1) Small screen size; 2) Bulk Data; 3) Open Source Platform; 4) Simple login interface; 5) Lack of Awareness and 6) Downloading Apps from third parties [36]. In Table 2 explanations are given for these security concerns, the last column indicates which articles mentioned these reasons. Reason 6, is not applicable to Flubot, however it is applicable for other smishing-based malware and, therefore, kept in this paper.

3.2 Academic Knowledge Gaps

Having read the academic literature selected through the literature review, some gaps have been established.

Knowledge gap 1: Lack of research on the efficacy of remediation for smishing-based malware victims An ever-increasing body of academic literature has been published on user behaviour regarding cybersecurity, including a small number of articles on remediation of mobile phone infections. However, no academic literature has been published on the efficacy of remediation (advice) on mobile phone users infected by smishing-based malware. Numerous articles on the topic of user behaviour and remediation state that mobile phone security is a new topic that needs to be studied further. Additionally Chorge and Shekoker state that very little research been done on anti-phishing tools for smartphones [15, 18, 36].

Vulnerability	Explanation	Sources
Small screen size	It is hard to check the legitimacy of the page as there is less of a page to check and full URLs are not displayed in the mobile browser, and, even, if a link would be shown many end-users would not be capable of making a correct distinction.	[36, 74, 83, 90]
Bulk data	A significant amount of personal and valuable information is stored on the smartphones making it a desirable target, including financial credentials.	[18, 36, 46]
Open Source Platform	Smartphones generally operate on open source platforms, such as Android. The kernel is open in Android, making it accessible for malware writers to develop and publish malicious applications. Users download these applications running the risk of infecting their mobile phones.	[36, 91]
Simple login interface	Mobile applications tend to have simpler user login interfaces than desktop versions, making it easier to develop a fake application or web page.	[36]
Lack of Awareness	"Users do not take the security of smartphones seriously either due to lack of knowledge or due to their irresponsible behaviour."*	[18, 36, 43, 46, 47]
Downloading Apps from third parties	Attackers use third party application stores for spreading malicious programs and applications. Applications that are freely available can be downloaded and installed by the smartphone users. Sometimes to trick the users, the attackers develop legitimate applications and release them in the application store. Then they modify the applications to include the malicious content and release an update	[36]

Table 3.2: Vulnerabilities, their explanations and in which articles they are referenced

* = Lack of knowledge also affects mobile phone users that do take the security of their phone seriously, as Forget et al. have found, user engagement does not always lead to better security outcomes [33].

Knowledge gap 2: Lack of policy for smishing-based malware for end-users and customers of telecom providers There is literature on measures against smartphone phishing and in general smartphone threats and malware, especially about the considerations of Bring Your Own Device (BYOD) to the work environment [28, 110]. However, these measures and policies do not fully encompass the issues applicable for Flubot or similar smishing-based malware. The fast developing nature of malware and technology, i.e. the arms race that is happening in the cyberspace between malware developers on one hand and software developers and security experts on the other, especially regarding smartphones, is an interesting development to which measures against threats and policies for safe cyber environments always have to catch up. The novelty of Flubot in combination with this catch-up, is why there is currently no academic literature on policies for smishing-based malware. Especially, regarding end-users and customers of telecom providers, as the positioning of telecom providers makes them the most suitable to enact change.

Knowledge gap 3: Lack of research on the influence of technical skill and profession on security behaviour Studies have found that (self-perceived) technical skill and technically aligned professions do not automatically translate into better security behaviour. Forget et al. and Wash and Rader found in their studies on security behaviour regarding computers, not smartphones, that misaligned perceptions of expertise and inaccurate knowledge about computer security often lead to negative impacts on computer security [33, 108].

Furthermore, it is clear that people have different degrees of interest and are behaving differently based on their involvement, expertise and perceived judgment of the security landscape, as shown by these studies. However, no such studies have been performed in the smartphone landscape which is similar but not the same, therefore the influence of perceived technical skill and profession on the remediation process will be looked for in this research.

3.3 Research questions

The uncovered and selected academic knowledge gaps result in the formulation of a set of main and sub research questions that aim to fill the knowledge gaps. To gain an understanding of Flubot and the impact it has had over time, this research will answer the following main research question:

"How has Flubot impacted consumers, of a Dutch ISP and telecom provider, with an infected mobile phone?"

To answer the main research question comprehensively, the research is divided into five sub research questions, namely:

3.3.1 SRQ 1: Are mobile end-users aware of a Flubot infection?

To get an insight into how often Flubot victims are aware of the infection, and whether they suspect anything that is wrong with their smartphone, ideally, related to Flubot. Furthermore, this question provides an insight into whether the suspicions the victims may have are accurate, possibly finding out about triggers that have not been established as of yet in literature. Additionally, determining whether victims have heard of Flubot before and, if so, how they came to know about it, adds to the understanding of the awareness and notoriety of Flubot. This includes, determining what the victims think caused the Flubot infection to get an insight into how accurate any prior knowledge on Flubot is.

3.3.2 SRQ 2: How have end-users acted on the Flubot infection?

To determine whether end-users are able to accomplish the remediation and, if not then why not, to gain an insight into what stops victims from remediating the infection. This provides an additional insight regarding where to invest resources efficiently to improve the end-users' ability to remediate the infection. Furthermore, to determine how long it took to remediate the infection. This gives an insight into the urgency the victims experience and how quickly they, on average, act on the notification of being infected and get to remediating, influencing the extent of the harm experienced.

3.3.3 SRQ 3: Which types of harm have end-users experienced by Flubot and are there indicators?

To determine what type of harm mobile end-users have experienced, whether it be financial, emotional, professional or other type of harm. Harm in general can be hard to quantify, therefore, the different types of harm, as formulated by Agrafiotis et al., are used to get a more comprehensive understanding of the impact of Flubot on victims [1]. By determining possible correlations between types of harm an understanding can be gained of which types are likely to coincide and it could help in determining other types of harm victims might have experienced but not noticed yet. The severity of the impact is crucial in allocating resources for remediation efficiently, therefore, the severity of the types of harm is analysed as well. The influence of the remediation advice and the measures on the harm experienced by victims, is determined as well, by pinpointing whether the harm has been experienced before or after receiving a notification.

3.3.4 SRQ 4: How have end-users perceived the remediation process?

To determine how victims have experienced the remediation process, it is necessary to understand how the remediation advice and the additional support provided by KPN have been experienced and whether the victim might have experienced any lasting effects due to the infection and remediation. Because Flubot is an illusive malware, the experiences of end-users do not necessarily have to align with the reality of what is being done or performed behind the scenes, therefore it is important to keep in mind, when possible, how the remediation process is conducted and not just how the remediation process is perceived by the victims, and vice versa. Furthermore, the influence of the remediation process on the victim's behaviour will also be determined, to gain an understanding of whether it is likely that victims will get infected by similar malware in the future.

3.3.5 SRQ 5: How do available Flubot detection methods, of a Dutch ISP and telecom provider, align with the end-users' awareness?

This sub research question is formulated in such a way to create an understanding of how well the current detection approaches suit the remediation and end-users' awareness, due to the nature of malware and technology, i.e. developing very rapidly, as opposed to the nature of measures and policies, i.e. tending to lag behind. Especially, because smishing-malware, Flubot in particular, has only been around for a couple of years. An understanding of the landscape of smishing-based malware helps to create an understanding of how well the remediation measures and advice align with the evolution of Flubot.

The main and sub research questions are shown in Figure 3.1. As the research is based mostly on a survey and partly on an interview, the questions needed to be asked, to gain as much value as possible from both the interview and the survey, are shown in the figure too. The color-coding in the figure shows how the questions will be formulated in the survey (i.e. with what kind of possible answers). In the last column of Figure 3.1 additional aspects, such as demographics and correlations, are shown that are beneficial for creating a comprehensive understanding and to better answer the main research question.

Research question	Sub research questions	Questions included in the survey and interviews	Other aspects to be answered
How has Flubot impacted consumers, of a Dutch ISP and telecom provider, with an infected mobile phone?	1: Are mobile end-users aware of being infected by Flubot?	<ul style="list-style-type: none"> Before being notified, did the end-user know of smishing-based malware like Flubot? [yes/no] If yes: how did the end-user come to know about Flubot? Before being notified, did the end-user suspect any infection on their phone? [yes/no] If so, what caused the suspicion? Is the end-user aware of what could cause a Flubot infection? [yes/no] If so, what does the end-user think is the cause of the infection? 	
	2: How have end-users acted on the Flubot infection?	<ul style="list-style-type: none"> Did the end-user remediate the infection? If so, how long did it take the end-user to remediate the infection, after becoming aware of the infection? If not, why didn't the end-user remediate the infection? 	
	3: Which types of harm have end-users experienced by Flubot and are there indicators?	<ul style="list-style-type: none"> Given the definitions of the types of cyberharm, which types of harm have the end-users experienced as a result of Flubot? If any type of harm has been selected, further elaborate the experienced harm and whether it occurred before or after being notified 	<ul style="list-style-type: none"> Correlation between types of harm Correlation between types of harm and other indicators
	4: How have end-users perceived the remediation process?	<ul style="list-style-type: none"> How has the end-user experienced the information provided in the notification? [very good, good, neutral, bad or very bad] Further elaborate the answer How has the end-user experienced the support provided throughout the remediation? [very good, good, neutral, bad or very bad] Further elaborate the answer Has the end-user changed their interaction with the smartphone, due to the infection? If so, how did the interaction change? 	
	5: How do available Flubot detection methods, of a Dutch ISP and telecom provider, align with the end-users' awareness?	<ul style="list-style-type: none"> How many SMS texts does the end-user receive on average from unknown senders? How likely is an end-user to click on a SMS text from an unknown sender? Demographics: Age, Profession, Technical capability in usage/remediation 	<ul style="list-style-type: none"> Evolution of Flubot Effectiveness of measures against Flubot
			<ul style="list-style-type: none"> Representativeness of sample Influence of demographics

Binary answers or multiple intervals on a range where only one answer can be selected
 Open answer
 Range of answers (not scaled) where multiple answers can be chosen from
 Numerical value

Figure 3.1: Research questions and sub research questions including the type of questions posed in the interviews and surveys

The process of the remediation, from infection to lasting impacts after the remediation, is rather long. To be able to better answer the five proposed sub research questions, the remediation process is divided into four important aspects. Figure 3.2 shows the four aspects, including their relationships.

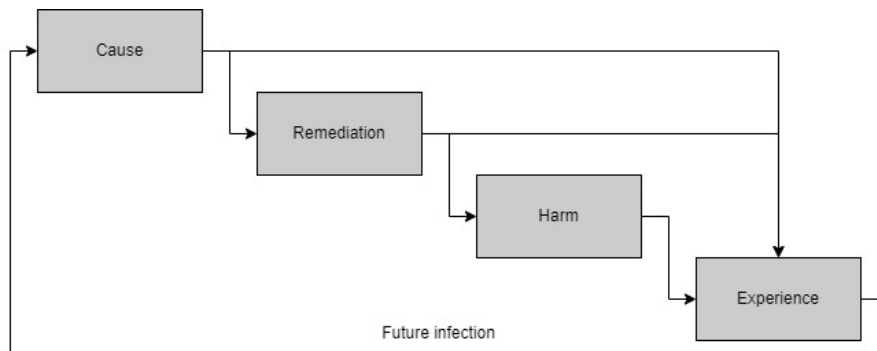


Figure 3.2: The remediation process divided in the four important aspects

An understanding of what has caused the infection, for the victim, impacts whether it is possible to find an appropriate remediation. Furthermore, understanding (correctly) what has caused the infection can either help with the lasting impact the infection has had, or make it worse. An incorrect understanding or even no understanding or inclination of what might have caused the infection might leave the victim with a feeling of insecurity regarding their smartphone usage.

The remediation, especially the time between the infection and the remediation, influences whether harm is experienced and, if no harm is experienced, whether the infection has made a lasting impact on the victim regarding their security behaviour in the long term (i.e. being more cautious with clicking on links).

The harm a victim might experience has an impact on the lasting experience as well, as the more impact the harm has, the stronger and longer the impact on the victim the infection will have.

The lasting impact, including any changes in the behaviour of the victim regarding security, determines whether it is likely that they will fall victim to a similar malware for a second or third time.

The main and sub research questions, that are meant to fill the identified knowledge gaps, that have been formulated and separated out in this chapter, are used for elaborating how the research in this paper is performed. The methodology of this paper is elaborated in the next chapter.

Chapter 4

Methodology

In this chapter the framework for the methodology is described, starting with the quantitative research, on which this paper is mostly based, in Subchapter 4.1 and the supporting research in Subchapter 4.2, including the desk research and qualitative addition. These two Subchapters include the research methods employed, reasoning for employing these methods and on which literature the whole research approach is based. The reasoning for the selection of the three target groups is then laid out in Subchapters 4.3, 4.4 and 4.5. Whereafter, the limitations of the research approach are named in Subchapter 4.6, ending with the ethics of the research (methods) in Subchapter 4.7.

The research performed in this paper is largely based on quantitative research, through means of a survey, that has been supplemented with an interview and expert input, i.e. qualitative research, and desk research. The design of methodologies has not been used for this or similar topics, it is common to use one or two of these research methods. The combination of using both quantitative and qualitative research methodologies, makes it possible in theory to gain new in-depth insights based on the qualitative research (i.e. interview) and then generalize the insights with quantitative research, which makes it ideal for the relatively scarce knowledge and literature on smishing-based malware; its impact and the environment it functions in, as the topic has only arisen in the last couple of years. Due to similarities with malware for computers and other types of malware for phones, it is possible to extrapolate already existing knowledge, practices and apply them for this specific type of evolving malware and smishing-based malware, especially to improve the understanding of end-users' abilities to deal with such threats.

4.1 Quantitative research

The quantitative research is built around a survey that was sent out to a large sample of infected users to determine whether the end-users were aware of an infection and if so, if the infection was remedied, how the respondents have experienced the remediation, whether harm was experienced due to the infection and if there are underlying correlations that can be gathered from the results. Using surveys to get an understanding on user behaviour regarding mobile security, was shown to be useful by Yao et al. in a study exploring "knowledge, attitudes, behaviours and user experience regarding mobile security", by Jorgensson to analyse the emerging threat landscape on mobile platforms and, relevant to this research, on whether malware had been detected, and, if so, how it had been remediated, and by Das et al. to determine triggers for security and privacy behaviour, specifically to determine triggers by making use of the Fogg Behavior Model [24, 46, 109]. The difficulty of using surveys in research is that a balance has to be found between keeping it as short as possible for respondents to not get the feeling that it would take too much time, and, on the other hand, asking as many questions possible to get the most information and data out of the respondents (i.e. by asking as many questions as possible). When trying to keep the right balance where the most value is gained from the answers provided by respondents and achieving the highest number of respondents possible, it is important to keep in mind that questions have to be posed in such a way that all the respondents understand the question correctly, without making all the questions a story or directing the respondents in certain directions regarding how to answer certain question. This balancing act can be tested by using test groups, unfortunately there was not enough time for such a setup. Therefore, feedback from different experts and research was integrated in creating and refining this survey [52, 71, 99].

The information gained from surveys creates a comprehensive understanding on the impact of Flubot, its remediation and the process the data subjects go through. Furthermore, the data gathered with the surveys

shows statistical insignificant and significant correlations between aspects asked and demographics provided by the respondent. Age, for instance, tends to correlate with bigger impacts and with being less capable of using and restoring smartphones according to scientific literature, these correlations are looked for and discussed in Chapters 4 and 5 [66, 67]. Furthermore, correlations that have been found in other studies and that are missing in this study, are discussed too.

4.1.1 Qualitative addition

The qualitative research addition, to the quantitative research and the desk research that the research is based on, includes an interview with an unaware victim and communication with experts on this topic to gain a comprehensive understanding of the existing industry knowledge and insights. The comprehensive understanding provided by talking to experts also helps with better formulating survey and interview questions. The expert opinions and additional interview with an unaware victim help with interpreting the results gained from the answers gained from the survey and other analyses.

The expert opinion consists of information and feedback gained from experts employed at KPN (a Phone Abuse specialist and a Cyber abuse specialist), Fox-IT (a malware analyst), and the TU Delft (researchers). These experts have consulted on or informed on certain aspects of this research or certain fields relevant to this research, via email or via online meetings. The expert opinions have been included in this research as references. Furthermore, governmental policies have been included in this research, including the information and feedback from the NCSC spokesperson, which is considered input from governmental bodies throughout this research.

The qualitative data gathering and analysis based on the semi-structured interview with the victim of Flubot is empirical. The semi-structured interview was designed with a set of questions and possible follow-up questions prepared beforehand to guide the interview, as seen in Figures E.1 E.2 E.3 E.4. It is necessary to treat the interviewee as a person and not just a data source because a malware infection can have a significant impact on a person, it is important to not make the interviewee feel worse about themselves. Furthermore, in the process of acquiring information and by doing so, informing the end-user, semi-structured interviews provide room to acquire additional information as the interviewee is not restricted by giving simple or numerical answers and the interviewer has the possibility to ask questions not previously thought of or considered. The same reasoning for using semi-structured interviews was reported by Das et al., to be able to direct discussions and the participants' memories towards changes in behaviour, "while still allowing participants the flexibility to expand on their undoubtedly unique experiences" [25]. The interview was performed with the intention of gaining an understanding in how end-users experience the current Flubot infection, how it has impacted them, how they deal with the issue at hand, given remediation advice, and how they experience the provision of remediation advice and support, including the usability thereof. The semi-structured interview was designed to gain insights through remote think-aloud observations, as performed by Bouwmeester et al., where the respondent was asked to share all the steps and thoughts experienced in the process of being informed about an infection and thereafter remediating the infection, or what the interviewee was planning on doing if no notification has been received [11].

Besides infected users, a small sample of mobile phone users expected to not have been infected by Flubot has been searched for and contacted. The latter group was selected to determine what made these subjects ignore the text, triggered them to not click on the malicious text or prevented them from downloading the malicious application. Finding these subjects was done by focusing on a forum where users posted about receiving a suspicious text that might be the result of smishing-based malware. These potential data subjects are considered valuable as they could provide insights on which indicators, that can be considered 'out of the box' or overlooked, end-users can, and possibly should, use to determine whether a text is suspicious or malicious.

4.2 Desk research

The many improvements Flubot has gone through, Flubot's changing landscape, the relatively scarce knowledge about Flubot that was available at the beginning of the research and the lack of academic knowledge that is available on the impact of smishing-based malware on end-users, has created a landscape where a lot of processes regarding Flubot happen separately and in parallel. As part of the research, to create a comprehensive understanding of Flubot; its impact on end-users and how everything functions in this complex environment, a significant amount of desk research was conducted. This includes connecting data about cases from KPN and other online repositories and data sources regarding policies and detection methods, and looking at how the urgency from the Dutch government and the telecom providers fit in the larger picture. The desk research

leads to assumptions regarding certain conflicts inside this complex system, which are corroborated by experts as there is no academic literature and a very limited number of industry articles that contain any relevant information.

The desk research consists of three aspects, namely researching the (completeness of the) available remediation advice (including the one sent by KPN), researching the evolution of Flubot with the current detection methods (employed by KPN), whilst accounting for the cases that have been registered by different sources, and applying the Fogg Behavior Model to the end-user remediation. The Fogg Behavior Model is only applied to the end-users because the end-users are the only ones, in the current situation, that have the power to perform a remediation or prevent an infection in the first place. It is important to determine how the end-users can be helped with dealing with malware, such as Flubot, as it is not a given that other stakeholders can prevent infections or curb the spread. These aspects give an insight into how well the detection and remediation methods function, how well they are aligned with the end-users' awareness and how end-users might be effectively triggered to perform remediation. The Fogg Behavior Model is applied to end-users because, even though end-users have a hard time determining whether an infection has occurred, they are the ones capable of remediating the infection, not any other party involved. Other involved stakeholders, such as telecom providers and ISPs, have only some of the Flubot spreading but not completely. Over time, the responsibility to remediate infections has mostly become the end-user's, as current measures employed are incapable of detecting and stopping Flubot. The application of the Fogg Behavior Model includes target groups regarding both reactive and proactive measures, and the most suitable triggers for the different target groups.

The overall research focuses on three target groups. The first group is the group of mobile phone users that have not been tricked into getting their mobile device infected with Flubot. This group has been contacted for interviews to understand their thought process and what it was that prevented them from falling for the smishing-malware that did trick others, however no subject has responded as will be discussed in Subchapter 4.3. The second target group consists of a larger group of previously infected device owners. This target group is the primary focus of this research as they will provide the quantitative data. Data subjects were initially selected over two different periods. One period is recent infections and the other period is older infections, the intention of using two different periods is to see whether older versions of Flubot have impacted the victims differently, the implication of older infections is that it is likely the victims will have a harder time with remembering their thought process accurately, however, the groups have been combined for analysis after all, as discussed in Subchapter 4.4. The third and smallest group selected is current infections, as not all infections have been remediated and some are still ongoing, it is valuable to gain insights on why remediation has not happened yet. The three target groups, their sizes and how many data subjects and results they have resulted in, are shown in Figure 4.1.

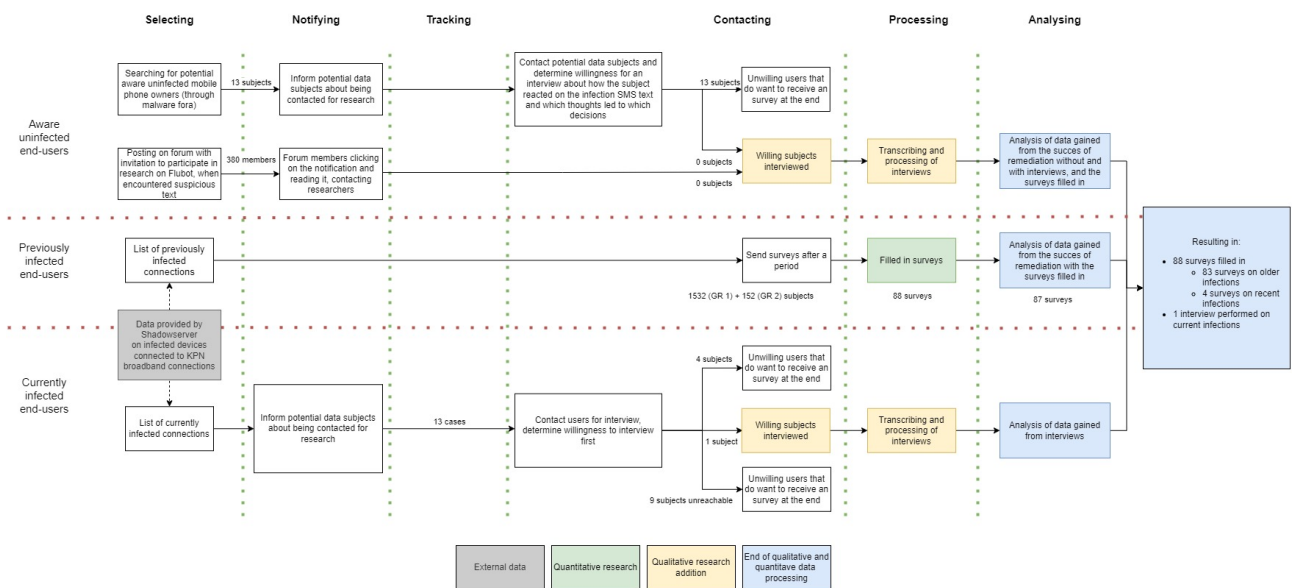


Figure 4.1: Performed qualitative and quantitative research flow regarding the three target groups

The research flow, as shown in Figure 4.1, is designed to fit the different target groups and to be able to analyse the results from the groups. The figure shows how many data subjects have responded and how many results have been gathered. Furthermore, the distinctions between different research methods and aspects are shown. The results gathered are discussed in the next subchapters.

4.3 Target group 1: Aware uninfected end-users

Target group 1, the aware uninfected users, have been looked for and selected initially by searching through the KPN forum for posts about seeing and reporting a suspicious text. By using search words describing the text as suspicious and containing a link (i.e. "suspicious SMS text including link"). Additional search terms were formulated that included smishing, sms phishing and Flubot. From the initial search 15 customers, going back two years as before that the issues were less likely to have been related to Flubot, were found, selected and contacted through email and through the KPN forum platform. After not getting any responses, a general notification was posted on the KPN forum for all forum visitors to be seen, requesting to participate in research if the reader had received a "(suspicious) SMS text including a link, not being sent by an acquaintance". The post had been liked 15 times and been seen 80 times after a week. In Figure B.1, the notification that was posted on the forum is shown. The notification was posted in Dutch because that is KPN's policy. Eventually, after 22 days (from June 7th till June 30th), the post was clicked on and seen by 380 customers and KPN forum members, however, no member reacted to the request in the post to answer questions and participate in the research, which meant no results were acquired from this target group.

4.4 Target group 2: Previously infected end-users

The second target group, the IP-CC cases provided by Shadowserver, was initially divided into two groups. The selection and tracking method for these cases can be relatively inaccurate, because it is nearly impossible to determine exactly which mobile device has been infected. Only a best guess can be made, based on how often an Android connected to a certain KPN broadband connection. No distinction is made between different phones through the detection system, only the IP-address of the KPN broadband connection is stored and how often it is registered by Shadowserver. Therefore, a first selection was made to only include cases of infections that had been registered at least 3 times by Shadowserver, to exclude infected phones that have only once connected somewhere or even twice, because of visiting a place incidentally and never returning. This selection resulted in 50 different cases in the last 3 months (06/3/2022-06/6/2022). The first group is relatively small and because some cases have been registered up to 80 days, even now, some cases have still not been resolved and are, therefore, unlikely to be resolved anytime soon. Therefore, the cases that were excluded previously were added as a second group. Besides creating a larger sample, including the second group might provide victims that resolved the infection right after the first or second notification. This is not unlikely as people that notice a warning about an infection, are likely to remediate the issue. Countering the decision to exclude the cases that showed up only once or twice initially, as it less likely that a person that has either ignored or not noticed the 60th (for example) notification would suddenly remediate the issue after the 61st notification, especially compared to victims reacting after the first or second notification. The second group, of cases where an IP-address was registered once or twice, accounted for 67 different cases in the same period. With both groups, once requests for participating in the survey had been sent out, nine email addresses were instantly returned as they did not exist. These two groups totalled 111 cases, including the 9 non-existent email addresses.

To gain a larger sample, the time span was increased, going further back and including cases up to six months ago. This larger second batch, including the previous 102 cases, totaled 247 IP-addresses, regardless of how often an IP-address was registered by Shadowserver. The second batch resulted in four submitted surveys, all the submissions were cases that were registered once or twice. This distribution of four submissions by one group (of one or two registrations) and zero submissions by the other group (of three or more registrations), leads to the hypothesis that there is little point in contacting and warning end-user by email more than twice. The hypothesis is based on the assumption that if an end-user has not reacted by the second time, it is unlikely it will happen any time after that. This hypothesis is why it was decided to focus solely on cases that were registered once or twice, saving resources needed for other aspects in this research. To get more results, a further month's worth of cases was added in the 3rd batch, which in the period of the 9th of November till the 6th of December amounting to 741 cases. The further back the cases go, the less reliable the answers will be in general, the reason for not going back infinitely. The thought processes and impressions the surveyee had, during the infection and the following remediation, are especially hard to recollect accurately after 7 months. If there was

any impact that the infection had on the surveyee, the impact might be recollected more accurately, especially with a bigger impact. Around the beginning of November a spike was recorded in KPN cases, therefore it was decided to add six more days worth of cases which would lead to many more cases without having a significant impact on the accuracy of the memory of the Flubot infection, adding 684 cases. In total, 1.532 cases for Group 1 (whom received 1 or 2 notifications) and 152 cases for Group 2 (whom received 3 or more notifications) have been sent a request to participate in the survey, of which 88 cases have responded by filling in and submitting a survey (all submissions are from GR1 cases).

4.4.1 Survey

Target group 2 cases were sent a request to participate in the survey firstly, including a link for the survey, as shown in Figure D.2. Then, if the data subject decided to click on the link, the opening statement was shown to inform the subject of the implications, as seen in Figure D.3. These two first steps are designed to inform the data subject and to make sure that the data subject understands the purpose of the survey and what is done with the data. After clicking through, on the opening statement, the data subject is forwarded to the first aspect of the survey (demographics). Which includes the questions seen in Figure 4.2. After having answered each aspect a following aspect is shown, totalling 5 aspects (demographics and the four aspects of remediation described in the previous chapter, see Fig 3.2), the last two aspects are shown in Figure 4.3. In these figures, the exact questions are shown, including the possible answers that can be given, which aspect they belong to, which sub research question they answer and when it is possible to answer them (some questions were not shown to the data subject to not pose redundant or irrelevant questions). The last column shows when certain questions were shown to the respondent, to keep the survey as short as possible and to prevent conflicting or double answers as much as possible.

Demographics

The data subject was asked to give their profession, age and perceived technical ability (from 1 to 5) to gain an understanding whether the performed study is skewed towards younger or older or more or less tech-savvy data subjects. In previous studies these factors have shown to skew the results, therefore it is important to determine if that is also the case in this research [33, 54, 67, 86, 108].

Cause

After having answered the demographics questions, the data subject was forwarded to the second aspect, i.e. cause (see Figure 4.2). It was first determined whether the end-user knew about Flubot or any smishing-based malware before being notified and, if that was the case, then how the end-user came to know of such malware. To gain an understanding on how known Flubot, and similar malware, was and how the awareness was shared from one to another. Then, the end-user was asked whether there were any suspicions regarding the mobile phone being infected. If the respondent had a suspicion, the respondent will be asked for elaboration. The next question was about whether the data subject knows what caused the infection as it is not specifically mentioned in the notification that the infected mobile phone owner receives. It is possible to find out what caused the infection, however the end-user has to click on the link in the notification or look for it themselves (see Figures A.1 A.2). Knowing what caused the infection can prevent future infections of similar malware. To get a better indication of how likely a future infection is, the last question of the first page was posed less subtly on how likely a respondent is to click on links inside a text from an unknown sender. The second to last question was posed to determine whether infections are more likely to happen with end-users that receive more texts from unknown senders, based on the average amount of texts received from unknown senders.

Remediation

To get an understanding of how end-users have acted on the Flubot infection, the respondent was asked if the respondent thinks the infection was remediated successfully and if so how long it took the respondent (see Figure 4.2). Because of the nature of Flubot it is almost impossible to determine whether a remediation was successful, therefore the question is about whether the respondent thinks the remediation was successful and not whether it actually was successful. If the respondent did not think the remediation was performed or successful, then the respondent was asked to elaborate on what obstructed them from (successfully) remediating the infection.

Sub research question	Aspect (of the Flubot process)	Question title	Question	Possible answers or free text	Only shown question if answered:
	Demographics	Demo_AGE	Fill in your age	Free text (a numerical value)	
		Demo_PROFESSION	Fill in your profession	Free text	
		Demo_SkillLevelSmartphone	How experienced are you in using and remediating a smartphone? On a scale from very unexperienced (1) to very experienced (5)	1; 2; 3; 4; 5	
1: Are mobile end-users aware of being infected by Flubot?	Cause	1_PriorKnowledge	Prior to being notified by KPN, have you heard of sms-phishing malware, like Flubot, before?	Yes; No	← "Yes" at question 1_PriorKnowledge
		1_Source	How have you come to know of smishing-malware, like Flubot?	Employer; Family; Friends; News; Government; Telecom provider; Social media; Previous infection; Other; free text	
		1_Suspicion	Prior to being informed, did you notice something off or anything suspicious about your smartphone?	Yes; No	← "Yes" at question 1_Suspicion
		1_SuspicionElaboration	Elaborate what you noticed	Free text	
		1_InclinationCauseInfection	Do you have an inclination what could have caused the infection?	Yes; No	← "Yes" at question 1_InclinationCauseInfection
		1_InclinationCauseElaboration	Elaborate what you think the cause is	Free text	
		1_AverageWeeklySMS	How often on average do you receive SMS texts per week? Excluding friends and family	Free text (a numerical value)	
		1_LikelihoodClickingUnknownSender	How likely is it that you will open a URL link inside a SMS text from an unknown sender? On a scale from very unlikely (1) to very likely (5)	1; 2; 3; 4; 5	
2: How have end-users acted on the Flubot infection?	Remediation	2_Remediation	Have you remediated the Flubot infection?	Yes; No	← "Yes" at question 2_Remediation
		2_DaysTakenRemediation	How many days, after being notified, did it take for you to remediate the infection?	Free text (a numerical value)	
		2_RemediationElaboration	Elaborate why you did not manage to remediate the infection	Free text	← "No" at question 2_Remediation

Multiple answers possible =

Figure 4.2: The survey questions and possible answers, linked with the aspects or sub research questions to be answered (Demographics, SRQ 1 and SRQ 2)

Harm

The third aspect the respondent was asked, was about harm. Data subjects might not understand or be able to differentiate between the types of harm that were mentioned and asked in the survey without any additional information, therefore a short description of the types of harm was given. The first question was about whether harm was experienced prior to or after having been notified, if the respondent experienced any harm at all. Then, if harm was experienced, the data subject can choose multiple types of harm and for every type of harm that the end-user has experienced, a rating between 'almost no impact' to 'very impactful' was asked to get an understanding of the graveness of the harm. It was also possible to answer the question with "no harm" experienced (see Figure 4.3). Additionally, the data subject was asked to elaborate on the harm to get a better understanding.

Experience

To get an understanding of how the end-users have experienced the remediation process and, ideally, what could be done better to lessen the impact of the infection, the data subject was asked to rate the information provided in the notification and to rate the support provided by KPN. Then, the respondent was asked to elaborate on

their satisfaction with the information and support provided. Finally, the respondent was asked whether the infection and remediation thereof has changed how the data subject interacts with their mobile phone (i.e. how the data subject uses their mobile phone), including an elaboration on how it has changed.

Sub research question	Aspect (of the Flubot process)	Question title	Question	Possible answers or free text	Only shown question if answered:
3: Which types of harm have end-users experienced by Flubot and are there indicators?	Harm	3_HarmWhen	Given the types of harm, have you experienced harm as a consequence of Flubot?	Yes, prior to being notified; Yes, after being notified; No	←
		3_HarmPhysicalDigital	Physical and digital harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or "No impact"	No harm; 1; 2; 3; 4; 5	"Yes, prior to being notified" or "Yes, after being notified" at question 3_HarmWhen
		3_HarmEconomic	Economic harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or "No impact"	No harm; 1; 2; 3; 4; 5	"Yes, prior to being notified" or "Yes, after being notified" at question 3_HarmWhen
		3_HarmPsychological	Psychological harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or "No impact"	No harm; 1; 2; 3; 4; 5	"Yes, prior to being notified" or "Yes, after being notified" at question 3_HarmWhen
		3_HarmReputational	Reputational harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or "No impact"	No harm; 1; 2; 3; 4; 5	"Yes, prior to being notified" or "Yes, after being notified" at question 3_HarmWhen
		3_HarmSocietal	Societal harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or "No impact"	No harm; 1; 2; 3; 4; 5	"Yes, prior to being notified" or "Yes, after being notified" at question 3_HarmWhen
		3_HarmElaboration	Elaborate on the harm you have experienced, including the severity of the impact	Free text	"Yes, prior to being notified" or "Yes, after being notified" at question 3_HarmWhen
4: How have end-users perceived the remediation process?	Experience	4_Satisfaction InformationProvision	How would you rate the information provision in the original email about the remediation of flubot? On a scale from very bad (1) to very good (5).	1; 2; 3; 4; 5	
		4_SatisfactionSupport	How would you rate the available support and the provided tools from KPN? On a scale from very bad (1) to very good (5).	1; 2; 3; 4; 5	
		4_SatisfactionElaboration	Elaborate your experience	Free text	
		4_ChangedPhoneInteraction	Has the infection changed how you interact with your smartphone?	Yes; No	←
		4_ChangedInteraction Elaboration	Elaborate the changed interaction	Free text	"Yes" at question 4_ChangedPhoneInteraction
5: How do available Flubot detection methods, of a Dutch ISP and telecom provider, align with the end-users' awareness?					

Figure 4.3: The survey questions and possible answers, linked with the aspects or sub research questions to be answered (SRQ 3 and SRQ 4)

4.4.2 Analysis of survey results

In the survey a number of different questions were asked, which span different types of questions to be able to gain statistical and empirical insights, see Figures 3.1 4.24.3 and Appendix F for the whole survey F.

The survey starts with demographic questions (Demo_AGE) about the age of the respondent, where it is possible to fill in a value, which was converted into a ratio scale variable. Throughout the survey there are two more ratio scale variables, namely 2_DaysTakenRemediation and 1_AverageWeeklySMS.

There is a multiple choice question included (1_Source converted into 1_SourceFamily, 1_SourceFriends, 1_SourceNews, 1_SourceSocialMedia, 1_SourceTelco, 1_SourceEmployer, and 1_SourceGov), which, for analysis, was turned into nominal scale variables for all the different options included and suggested by surveyees, in the last option it is possible to fill in one's own category. This means that every category, listed and suggested, gets their own column with values zero for not being applicable or one for being applicable. The last option in that question is "other", where the respondent gets to fill in an answer themselves if the data source was not listed in the provided answers (as used by Jörgensson and Wash et al. [46, 107]).

Ranked variables A number of Likert scale questions (Demo_SkillLevelSmartphone, 1_LikelihoodClickingUnknownSender, 3_Harm converted into 3_HarmPhysicalDigital, 3_HarmPhysicalDigital, 3_HarmEconomic, 3_HarmPsychological, 3_HarmReputational, and 3_HarmSocietal, 4_SatisfactionInformationProvision, and 4_SatisfactionSupport) were posed where the range either goes from one to five (as used by Yao et al., Jörgensson and Wash et al., [46, 107, 109]), or zero to five (zero implying that a specific harm has not occurred at all). The Likert scale questions turn into interval scale variables in the statistical analysis, providing scores from zero or one, to five. The zero or one options are the lowest values, and ranked answers, and five is the highest. For the 3_Harm, the question was framed such that the respondent did not have to answer the question if the harm was not applicable, the zero option ("No harm") means the same when translating the answers into variables. For the 3_Harm question it was designed such that the more impact a specific type of harm has, the higher the respondent is supposed to rate it.

In the survey a number of yes or no questions were posed (1_PriorKnowledge, 1_Suspicion, 1_InclinationCauseInfection, 2_Remediation, 4_ChangedPhoneInteraction). These were often followed up with open-ended questions for elaboration, the same setup has been used by Yao et al. [109]. This keeps the survey as short as possible, only asking for elaborations when useful, by using as many yes or no questions the respondent is least likely to find the survey to take too long and is most likely to finish the survey. The answers to the yes or no questions are converted into zero for "no" or one for "yes", making it suitable for statistical analysis as a nominal variable. A similar setup is used for 3_HarmWhen, where the answers are either "No harm", "Harm experienced prior to being notified" and "Harm experienced after being notified", with the answers being translated into values 0, 1 or 2, respectively.

The remaining questions (Demo_PROFESSION, 1_SuspicionElaboration, 1_InclinationCauseElaboration, 2_RemediationElaboration, 3_HarmElaboration, 4_SatisfactionElaboration, 4_ChangedInteractionElaboration) are open-ended questions which are not meant for statistical analysis but for empirical insights. The answers provided in the questions were clustered when possible and then interpreted.

SPSS (25) was used for statistical analysis, as Choueiry found SPSS to be the most commonly used statistical software used in research papers in between 2016 and 2021 [20]. By using Spearman's Rank Correlation Coefficient, when analysing ordinal and interval/ratio variables, it is possible to determine strong and weak correlations between the set of variables and to get a better understanding of the correlation. It makes it possible to look for correlations that can then be researched further and explanations that can be looked for. Because Pearson's Correlation Coefficient requires the variables to be continuous (i.e. interval/ratio), which is not the case for most of the results gained from the surveys, Spearman's Rank Correlation Coefficient was used as it requires the variables to be either ordinal or interval/ratio. The statistical and empirical analysis results are discussed in the next chapter.

4.5 Target group 3: Currently infected end-users

The remaining active Flubot cases were selected as a target group because, even though it is unlikely that the infections are causing any more harm except for unnecessarily burning through the battery and occupying storage, it is possible that all the actions and data is being screen grabbed and keylogged still. Fortunately, nothing can happen with that data as the network has been taken down. To completely remediate the remaining infections, these cases have been selected as a target group and contacted to find out why they have not done anything about the infection, what they know of Flubot, whether they have encountered any harm and how easily they can remediate the issue at hand.

On June 1, government agencies published that Flubot had been taken down. On this date, the tracking of remaining dormant cases started [30, 76, 89]. From that date till the 22nd of June 13 IP-C%C cases, that have

been notified more than twice, were recorded. It was decided to filter out cases that have been notified once or twice because Flubot had already stopped spreading for 22 days and that makes it likely that these infections have been recorded in other places, or are possibly even one of the other 13 cases (i.e. counted double). The contact information was used to mail them first and to inform them of being contacted a week later (see Figure D), whereafter these cases were contacted over the phone to inform them that their device was still infected and to inquire about their willingness to participate in this study by answering some questions regarding the Flubot infection.

Initially, of the 13 cases contacted, only 4 cases answered the phone, of which 1 case gave permission and consented to being interviewed. Of the 9 cases that did not answer the phone, three numbers did not exist anymore, and the remaining six phone numbers were not available at that moment. The six unavailable phone numbers were then contacted repeatedly in the hopes of contacting the end-users, however six additional attempts, during different periods of the day on different days, led to no contact. Further attempts at using other contact information for three of the latter six numbers also did not yield any results, exhausting all possibilities to contact and inform these active cases.

4.5.1 Interview

To gain in-depth insights on how end-users go through the remediation process, what their thought process is and what they stumble upon during the process, an interview has been conducted in a semi-structured fashion, see Appendix E for the prepared list of questions.

To make sure that the interview was conducted with the right data subject, the interview started first with a small introduction why the data subject was called, whereafter questions were asked to determine whether the right data subject was on the other end of the phone call. Continuing with the person of interest, information was provided on the research, the conditions under which the interview was conducted and the results published, including the data usage and storage and the possibility to opt out or to leave out certain information. Whereafter, the data subject was asked for consent to participate and to be recorded. If the data subject gave consent, the interview started.

To prevent the risk of the interviewer creating a bias during the interview, the demographics were asked at the end of the interview. The remaining questions are similar to the questions asked in the survey, however posed as open questions to gain more insights. Because active cases have still not remediated the infection, it is important to determine why the infection had not been remediated. By asking, it is possible to determine whether the interviewee tried remediation and failed or did just not remediate at all.

4.6 Limitations of the methodology

Because the data provided by Shadowserver only shows whether the infected device is connected to a KPN broadband connection on that day, it could very well mean that a device has not remediated at all after not showing up anymore in the more recent Shadowserver datasets. This is possible if the device did not connect to a broadband connection belonging to KPN but to a competitor or even just not making use of a broadband connection, for that period of time. This makes it nearly impossible to make a distinction between remediation or just switching places. Furthermore, it is possible that an infected phone connects regularly to multiple KPN broadband connections, showing up as multiple cases and it is not possible to filter these cases out with the accessible information, running the risk of counting the detectable case double.

The approach to use surveys and interviews without any additional data to back up any results, might lead to answers not being accurate regarding what actually happened (for instance, that a respondent thinks that the infection has been remediated or which harm can be attributed to a Flubot infection). This applies especially to the think aloud approach used for the interview, where an interviewee might feel pressured to give correct answers or answers that the interviewee thinks are desirable, instead of the true thought process and steps undertaken, this issue has been raised by Bouwmeester et al. too [11].

The sample size of interviewed data subjects is limited due to the limited resources allocated for this research and this does affect the representativeness of the results on the larger population. It is also possible that the interviewees and surveyed are more interested in or involved with the topic and that might lead to skewed results as was the case with Rodriguez et al., technical ability will be factored into the results and the discussion [86].

The target group for the survey spans seven months, which is not a very long time period. However, the correspondents were asked to remember specific details of events that might have taken place six or even seven months ago. The difference in accurately being able to recall the remediation of the infection, might be big, especially because some have barely been impacted by the remediation. Others, might not even have registered reading the notification that was sent by KPN, making it even harder to recall or place what this survey is about.

Making use of surveys with open-ended questions can lead to vague or unclear answers that cannot be used for further analysis. In semi-structured interviews it is possible to ask for clarification or an elaboration if an answer is vague or unclear. However, that is not possible with surveys as there is no possibility for feedback, especially, when privacy of the respondents needs to be guaranteed and anonymous surveys are used. Ideally, test rounds would be performed before the actual surveys and interviews were conducted to improve the usability of the answers by determining which questions, and phrasing especially, might lead to ambiguous answers. However, due to the limited resources and time available for this research these testing rounds have not been included.

Using industrial reports, knowledge and expertise might lead to information being steered towards the industry's goals and interests. The objectivity of the industrial knowledge and information is hard to determine, which is less the case with academic knowledge and findings. Furthermore, using search engines, such as Google, can lead to skewed search results because of the personalised search results Google provides. This means that not everyone is shown the same search results with the same search words.

4.7 Ethics

In accordance with the Menlo Report, the principles for ethical assessment of ICT Research are addressed and followed [26].

Respect for Persons Everything discussed and conducted in this paper has been done according to the principles and with approval of the human research ethics committee of the faculty of Technology, Policy and Management of Delft University of Technology. All participants in this study have given informed consent for participating (i.e. being recorded and their anonymised data being published afterwards or the aggregated data of their answers being analysed and published afterwards), after being informed of the implications and intentions of participating in this research. Both target groups (Target group 2 and 3) have been informed that they were free to stop participating at any moment (i.e. do not have to continue submitting answers if they do not feel like it or can just stop the interview whenever they want). The data from the surveys has been stored without any identifiable personal information and been stored securely and solely on a storage that only the researcher has had access to. The recording of the interview was transcribed, anonymised and summarised to lose any identifiable personal information and then it too was stored on the same storage. The contact information (including name, phone number and email address) that was needed to contact the data subjects has too been stored on the storage and will be discarded after the research is finished. The data has been used and stored according to the privacy and data minimisation rules and principles. The anonymised and summarised transcript of the interview, stripped from any personally identifiable information, has been included in the appendix, see [H](#).

Regarding the think-aloud protocol employed for the interview, the subject was made to feel safe by addressing any possible risks and encouraging the subject to answer without judgment from the researcher. It was mentioned that if the subject did not want to answer, after consenting, or wanted any of their answers to not be recorded, that the request would be honored.

Respect for Stakeholders Regarding the cooperation with KPN, the telecom provider and ISP, providing all the needed data, all their safety, privacy and security guidelines and policies have been adhered to when using their data, tools, programs and facilities. All their data has not left their premise or their laptop, until it was generalized and anonymised and approval was given for using it in the research. Everything mentioned about KPN, their working methods and processes, and their cooperation has been approved by KPN employees. No competitive or sensitive information has been published, named or shared.

Justice Regarding justice, all data subjects and target groups have been treated the same and had equal opportunity to participate. Everyone has had the same chance to provide feedback, ask questions about the research or the implications thereof, or ask to be removed from the research (results). The email to get in contact with the researcher was added to all notifications sent out to participants and potential data subjects. No groups have been excluded based on prejudice. Attributes of persons have only been included for this research if deemed relevant for analysis, such as age, however no selection was based on attributes (i.e. target groups were selected and invited to participate, regardless of their inherent attributes, such as age, religion, sex, technical competency).

The benefits of the recommendations and insights created in this research are not meant for specific groups over others, however, as much as possible of the findings in this paper is steered towards the stakeholders that are best located in this complex system to deal with smishing-based malware. The benefits of the insights gained in this paper are kept, as much as possible, to a minimum for the malware TAs. To obstruct malware TAs as much as possible in their malicious operations and to lower the burdens on smartphone users, relevant processes and methods are addressed and analysed for future improvements.

Beneficence Beneficence has been a fundamental aspect of this research too, no processes of KPN have been disturbed that could negatively impact their beneficence. In the process of informing data subjects about being contacted or requesting to participate, it has been mentioned clearly that an infection was detected to make sure the data subjects, by ignoring the research, would still be unaware of the infection. In the interview the data subject was informed of which steps to take, at the end of interview, to remediate the issue. Contact information was provided for further help, if necessary at the end of the interview as well.

Because of the relatively scarce information on smishing-based malware, such as Flubot, and because the measures against the malware have not always been proven to be effective, or even publicly known in some cases, there is a fine line that has to be maintained in this research. This research cannot divulge too much information on the effectiveness of measures and the effectiveness of Flubot itself, to prevent it from becoming a how-to guide for malware developers and threat actors. Though most of the information in this research can be found on the internet, trade-offs have been made to reach the biggest social and academical contribution while still improving the (cyber)security of smartphone users, especially Android owners. A single detection method has been left out of the paper as it is considered sensitive information, the insights and findings of this paper account for this detection method and are completely applicable in the current landscape of smishing-based malware. Furthermore, no specifics regarding the detection and remediation methods (i.e. threshold amount for SMS auto block) are given that might help the TAs with better designing smishing-based malware.

In the next chapter the results of the research, following the methodology and ethics described in this chapter, are shown and described. The next chapter includes the results of the survey, the interview and the desk research.

Chapter 5

Results

The results gained from the answers submitted in the surveys, the interview and the desk research are shown and described in this chapter. The survey answers (of Target group 2) are shown and described in Subchapter 5.1, which is followed up with the information gained from the interview (of Target group 3) in Subchapter 5.2. Subchapter 5.3 lays out the desk research results, including an analysis of the available end-user remediation advice, the evolution of Flubot and the limitations of current detection methods. In Subchapter 5.4 the Fogg Behavior Model is applied to end-user remediation. Because Target group 1 did not produce any results, no results of that group are mentioned.

5.1 Target group 2: Surveys

Originally, Group 1 and 2 were divided to see any changes through the answers for different time periods of the infections. However, because the former group (i.e. most recent cases) is much smaller and, as a result, a low number of surveys has been submitted (4), it is decided to combine them with the latter (i.e. older cases) group (84 surveys), totalling 88 submissions.

For the purpose of analysis and to filter out unusable data, a first review of all the answers shows that one respondent did not provide serious answers, therefore the submission by that respondent is excluded from analysis. The first unusual answer provided by this respondent is the age, namely 577, a suspiciously high number. The second unusual answer is that the respondent on average receives 100 texts per week, which is much higher than the average number and significantly higher than any other submission. Furthermore, all the yes or no questions were answered with no and for profession the answer provided is the Dutch word for crook or raskal.

The remaining 87 submissions are used for analysis. The elaboration questions were combed through, to see if similar or duplicate answers have been given, and the answers are grouped, when possible. The answers to the elaboration questions are included as figures in the paragraphs.

5.1.1 Descriptive statistics

In this subchapter the results of the survey are shown and elaborated with context. Throughout this subchapter "prior to being notified" and "before the notification" is used occasionally. The notification is the email a KPN broadband connection owner gets sent once KPN receives an IP-CC case by Shadowserver (see the notification in Figure A). The results gained from the Microsoft Forms surveys are converted through Excel and then SPSS to create charts that are more easily interpreted, described and shown, including the means and the distributions of the results. For open-ended answers, draw.io is used to categorize submitted answers and to make it more readable. The figures that show the open-ended follow-up questions are added to the appropriate questions in this subchapter.

5.1.2 Demographics

Age On average the age of the respondents is 63, ranging between 36 and 81. The distribution of ages over the whole respondents sample, including the normal curve is shown in Figure 5.1 below. It shows that the respondent group is relatively old.

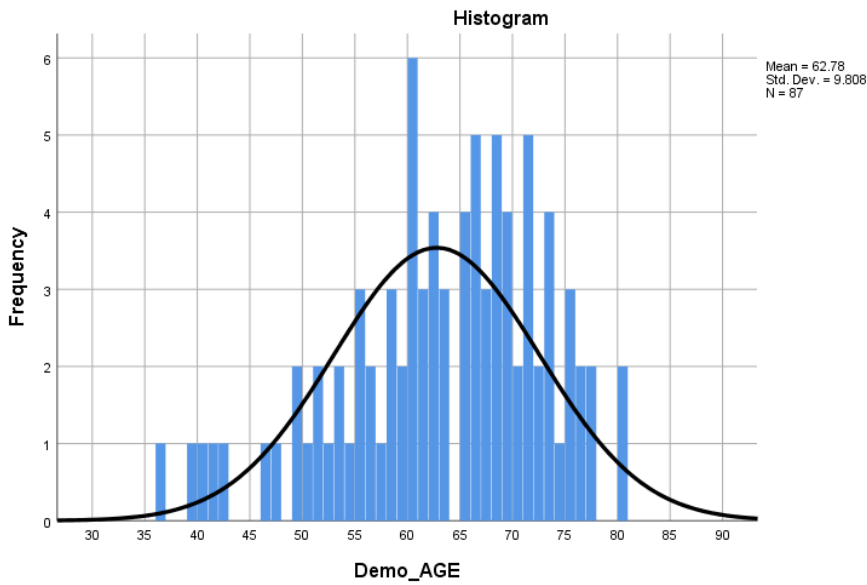


Figure 5.1: Histogram of the age distribution of the survey respondents, including the normal distribution

Profession The professions the respondents listed can be grouped in three groups, namely unemployed (17 subjects, of which a portion answered with being a housewife, and others had submitted working disability as their profession), retired (31 subjects) or working (37), see Figure 5.2 for a simple overview of the jobs and see Figure G.1 for the complete list of professions. One provided answer is "yes", regarding profession, therefore it can be assumed the respondent is employed. It is likely the respondent either did not understand the question or decided not to provide that information. A second respondent did not fill in anything for profession, but because the age of that respondent is 66 it can be assumed that the respondent is retired (because the age of retirement in the Netherlands is 66, with the age of retirement being lower for some professions) [84]. These assumptions resulted in a distribution of 38 working respondents, 17 being unemployed and 32 being retired. Interestingly, of all respondents, only one subject works in ICT, the subject having listed DevOPS engineer as their profession, this is reflected in their perceived smartphone usage and remediation capabilities as it is rated the highest (5 out of 5). In Figure G.1 the different professions are seen and when professions have been named multiple times. The variety of jobs and the portions of respondents being unemployed and retired shows that a wide sample of the population has responded to the survey and not necessarily a tech-savvy group. Furthermore, that someone’s profession is unrelated to a ICT-related field does naturally not imply that the respondent is not tech-savvy or that the job tasks are completely unrelated to the ICT-field, as ICT-related tasks and skills are embedded in more and more fields and jobs. The answers are not clear enough to determine which professions include ICT-related tasks and skills.

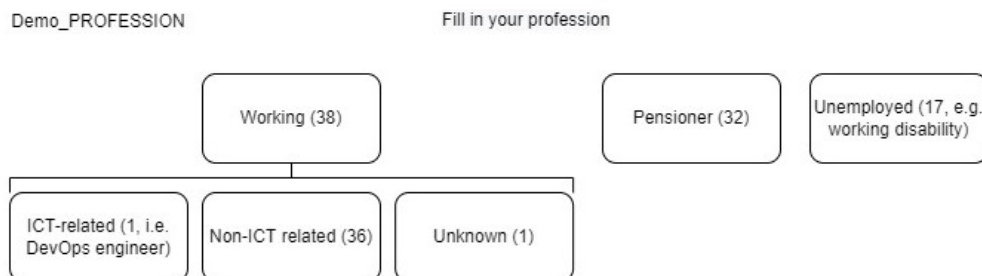


Figure 5.2: Grouped professions: working, unemployed and retired

Perceived ability of recovering and using smartphones The respondents, on average, rate their experience regarding recovering and using smartphones to be moderate (3.06 out of 5), as seen in Figure 5.3. The sample size, in general, considers themselves to be moderate with recovering and using smartphones. Only

10 respondents (11.5% of respondents) consider themselves to be very inexperienced and the majority (70 out of 87 respondents, i.e. 80.5%) rates themselves in the relative middle of the Likert scale (from 2 to 4). The distribution shows that the responding group is not necessarily tech-savvy or technologically illiterate.

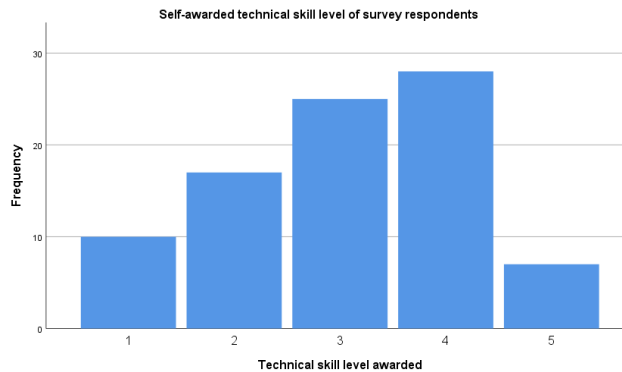


Figure 5.3: Histogram of the perceived ability to recover and use a smartphone, on a scale from very inexperienced (1) to very experienced (5)

5.1.3 Cause

SRQ 1: Prior knowledge of Flubot Around half the sample (48.3%) knew about Flubot before being notified, meaning that a slight majority of the sample had not heard of Flubot beforehand, making it less likely to defend against it. The most popular source for hearing about Flubot is news outlets (34.5%). The second most popular source is social media (20.7%) and the third most popular source is friends (18.4%). Figure 5.4 shows the different categories listed in the survey and how often they were selected, the question was posed as multiple choice, meaning that the respondent was able to select multiple answers. Only one respondent used the additional 'other' category, where filled in "Rabo (a Dutch bank), but I am not sure", therefore the answer is left out of the categories.

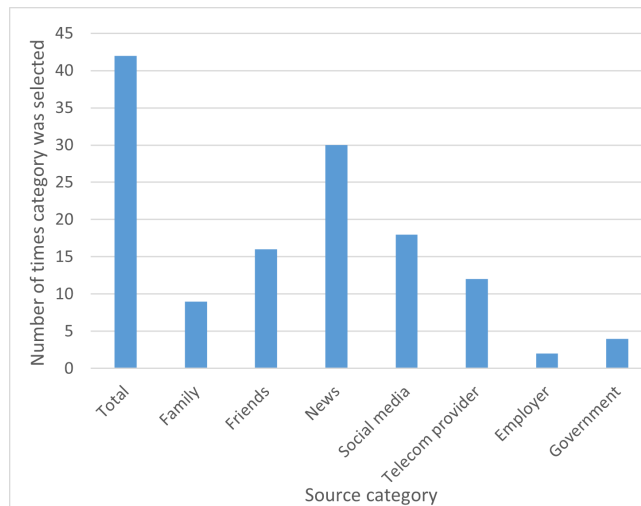


Figure 5.4: Chart showing through which source categories the 87 respondents came to know about Flubot

SRQ 1: Suspicion The majority of the respondents (59.8%, i.e. 52 respondents) did not suspect anything on their phone, before being notified, and of the 35 respondents suspecting something, 34 replied with an elaboration. The answers are quite diverse and not always unrelated to each other, as shown in Figure 5.5. Four respondents downloaded a suspicious application and two suspected something after not being able to delete the application they just had downloaded, meaning that the latter respondents had downloaded an application they most likely suspected of being either unnecessary or malicious. "Increased texts being sent", "Texts and calls from unknown senders", and "(un)known contacts asking/informing whether the respondent was hacked" are

very much related to each other, just as "High phone bill". As a consequence of a Flubot infection, the phone starts texting, and sometimes calling others without the knowledge of the owner of the infected smartphone, leading to a high phone bill and receivers (of the secretly sent SMS texts) responding to the texts (i.e. asking whether the sender of the malicious texts was hacked). It is very likely that these suspicions are accurate and interrelated, meaning that different respondents noticed different aspects of the same issue. Furthermore, not all answers can be attributed to Flubot, for instance, losing control over the phone is not necessarily a consequence of Flubot, meaning that it is possible that the respondent recollected a different infection and mixed that one up with the Flubot infection that was asked about. The answer does not make the suspicion less true or applicable, however the suspicion of the four respondents answering "Lost control over phone", as seen in Figure 5.5, has most likely been caused by something that is not Flubot. Except for that specific answer, all other suspicions can be attributed to Flubot. Hence, the suspicions are relatively accurate or the sample is now at least aware of what could be a red flag regarding Flubot, which increases the likelihood of using this knowledge in a similar future situation.

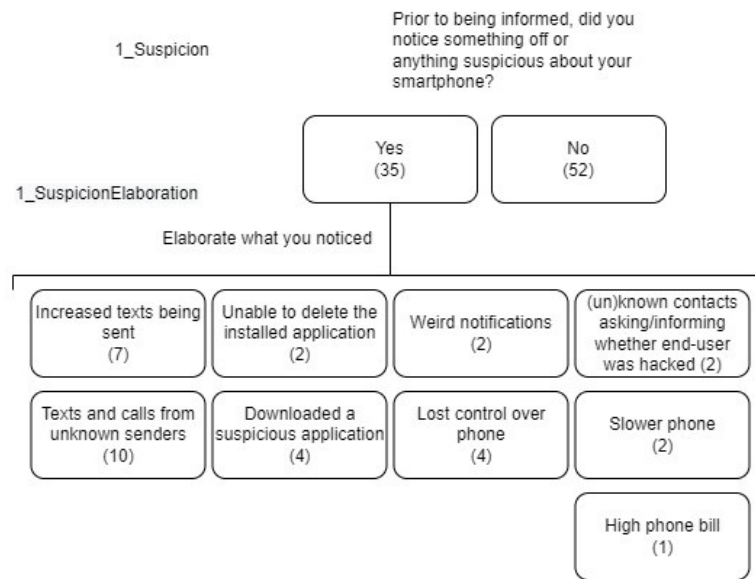


Figure 5.5: Answers given regarding whether the respondent suspected something on their phone, and the elaborations given if that is the case

SRQ 1: Inclination of the cause of the infection A slight majority of the respondents (52.9%) has an idea of what has caused what the infection, which is alarming in itself, as it means that almost half the respondents (47.1%) has no idea of the cause and not everyone's idea of the cause being correct. Future infections, of similar malware, are very likely if the end-user is not aware of the cause of an infection, setting that group up for future harm as malware attacks have been increasing and there is no sign that that growth is going to stop.

Of the respondents having replied with "Yes" to question 1_InclinationCauseInfection, as seen in Figure 5.6, two answers are unlikely to have been the actual cause of the infection. "Foreign number through WiFi" and "Called back to unknown number" are not known causes of Flubot infections or other similar smishing-based malware. These two answers can be symptoms of the infection, the latter answer can be the cause for an increased phone bill however that is not how Flubot or smishing-based malware is spread. Another answer given, "Hack", is a vague answer. A phone can be hacked by downloading malware, which does not narrow the selection down to Flubot or smishing-based malware, or by someone guessing the correct password, for example, which is completely unrelated to Flubot. Also, "Malicious (DHL) email (about parcel)" is also not related to Flubot. If the malicious parcel email is the actual cause of the infection then the answers do not regard Flubot, it is likely that the respondent assumed an email to be the cause when the actual cause of the infection was a malicious parcel SMS text. The remaining answers (from 35 respondents, or 40.2%) are assumed to be accurate and the actual cause of the Flubot infection. 10 answers are "malicious DHL link while waiting for a parcel", 16 are "Malicious link" (18.4%) and 9 are "Downloaded malicious app through SMS" (10.3%), nothing about these answers shows any discrepancy with Flubot. "Malicious link" is ambiguous as the answer does not tell how the link was shared, therefore it is assumed that the answers are about sms-phishing

as "sms-phishing malware" was mentioned twice specifically, throughout the survey, before the respondent was shown this question. Furthermore, in the email notifications that the respondent received with the warning of the Flubot infection, a link was included with additional information about Flubot where SMS texting is named specifically (See Appendix C). Interestingly, a share of respondents (11.5%) was tricked because of the timing of the malicious link and expecting an actual parcel. This percentage might be higher as the respondents, possibly, did not go into such detail. This shows that the timing of the Flubot campaigns has a significant impact on the likelihood of the malicious links working.

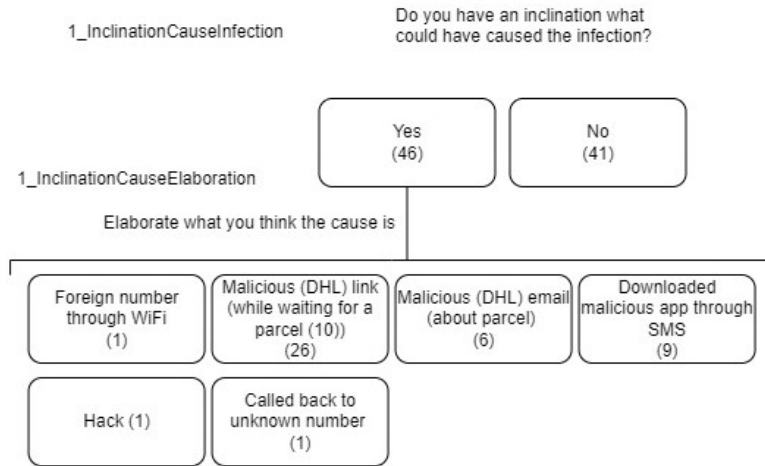


Figure 5.6: Answers regarding whether the respondent had an inclination of the cause of the infection, and the elaboration given if that is the case

Average SMS texts received weekly On average respondents received just above four SMS texts weekly (4.31) from unknown senders, excluding friends and family, as shown in Figure 5.7. 88.6% of the respondents receive in between 0 and 5 SMS texts weekly on average. Two texts per week is the most common number (37.9%). Of the remaining cases, a couple of cases received 10 (4 cases; 4.6%), 15 (2 cases; 2.3%), 20 (1 case; 1.1%), 40 (1 case; 1.1%), or 60 (2 cases; 2.3%) texts. This means that most respondents generally did not receive a large volume of texts.

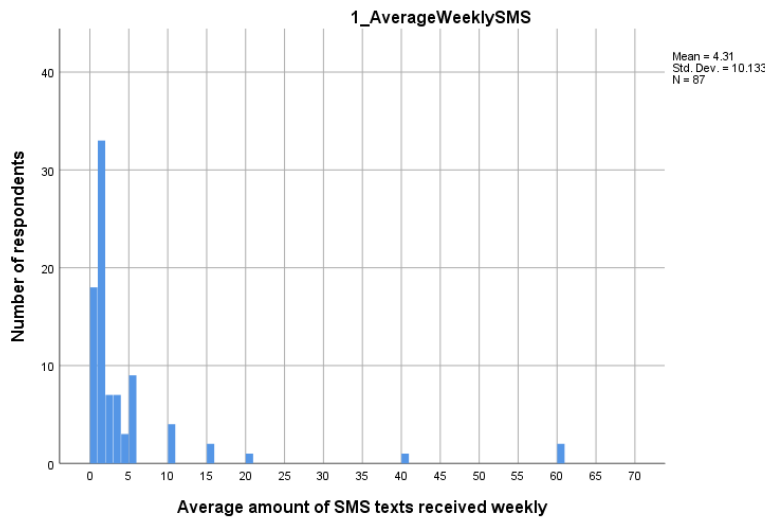


Figure 5.7: Histogram of the frequency of the average number of SMS texts the respondents received weekly, excluding friends and family

Likelihood of clicking on a link from an unknown sender The respondents are unlikely to click on SMS texts from unknown senders, with the average score being 1.72 on a scale from 1 (very unlikely) to 5 (very

likely), as seen in Figure 5.8. This unlikeliness is important to prevent the further spreading of smishing-based malware, with 50 respondents (57.5%) deeming it very unlikely (i.e. rating a one) to click on a text from an unknown sender and 19 respondents (21.8%) deeming it unlikely (i.e. rating a two). However, it is important to notice that 11 respondents (12.6%) are in between likely and unlikely to click on unknown texts (rating a three), and seven respondents are likely to click on unknown texts, of which one respondent even very likely. This raises the issue that 20.7% of respondents (rated three or higher) are not unlikely to click on SMS texts from unknown senders, of which 8% even likely (rating four or higher), putting these groups, especially the latter group, at substantial risk for further infections and harm.

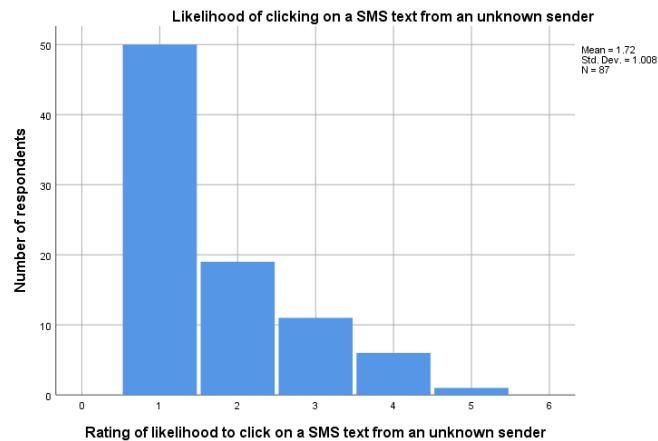


Figure 5.8: Histogram of the frequency of the likelihood of respondents to click on a SMS text from an unknown sender, from very unlikely (1) to very likely (5)

5.1.4 Remediation

SRQ 2: Remediation success 77% of the respondents had remediated the (i.e. 67 respondents), meaning that almost a quarter of the respondents (23%) had not remediated the infection. Two (2.3%) of the free text responds, as seen in Figure 5.9, on why the respondent had not remediated the issue yet have given "unusable phone" as their answer, this likely means that the phone was discarded or replaced and just not remediated. However, for the others (20.7%) it raises concerns as it is possible that these respondents still have a dormant infection, setting them up for future harm if Flubot reappears, or other malware starts to make use of the already existing Flubot infrastructure. This is further exacerbated by the other answers as 11 respondents (12.6%) were unaware of the infection, possibly two more (2.3%) as their answer "No way of knowing" is ambiguous and could either mean that the respondents did not know how to remediate or that they did not know that there was an infection at all. One respondent (1.1%) found the fixing cost to be too much, one respondent (1.1%) mentioned that it was not their phone, another two respondents (2.3%) did not know how to remediate, and the last two respondents (2.3%) said that the infected phones were not used as a reason for not remediating the infection.

SRQ 2: Remediation duration in days It took respondents, if they remediated the Flubot infection, on average 3.4 days, as shown in Figure 5.10. 52.9% of respondents, had remediated the infection in the first two days, it took an additional 21.8% of respondents up to 7 days to remediate and there are two outliers, one where (1.1%) it took 14 days and one (1.1%) that took 60 days. It took the respondents, that remediated the infection after three to seven days, fairly long. That long window makes it possible for the malware to do more harm to the respondents, who by then have been aware of the issue at hand for quite some days already.

5.1.5 Harm

SRQ 3: Harm and when A slight majority of the respondents (52.9%) has experienced a type of harm, as formulated by Agrafiotis et al [1]. In the survey it was asked whether the harm was experienced before or after being notified, exactly half of the respondents that experienced harm experienced it prior to being notified and the other half after being notified, as seen in Figure 5.11. The elaborations the respondents gave, vary from discomfort (most common answer, 16 times answered; 18.4%) to financial harm (13 answers; 14.9%), as a result of an increased phone bill, to not trusting the smartphone or banking services anymore (8 answers;

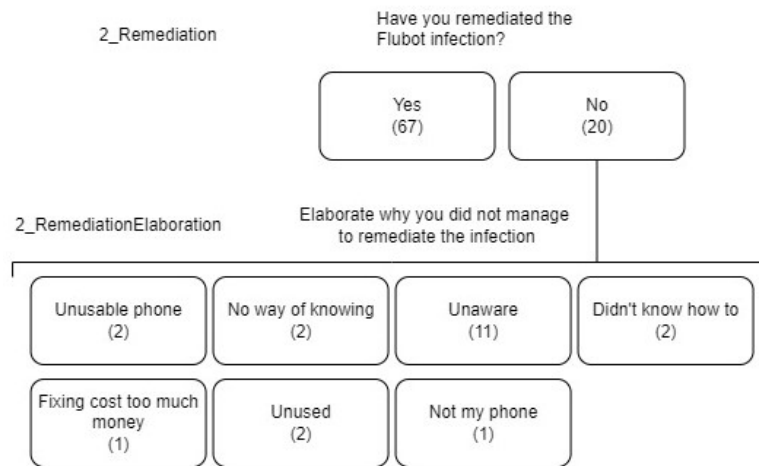


Figure 5.9: Answers on the question whether the respondent has remediated the infection and the elaboration given if that is not the case

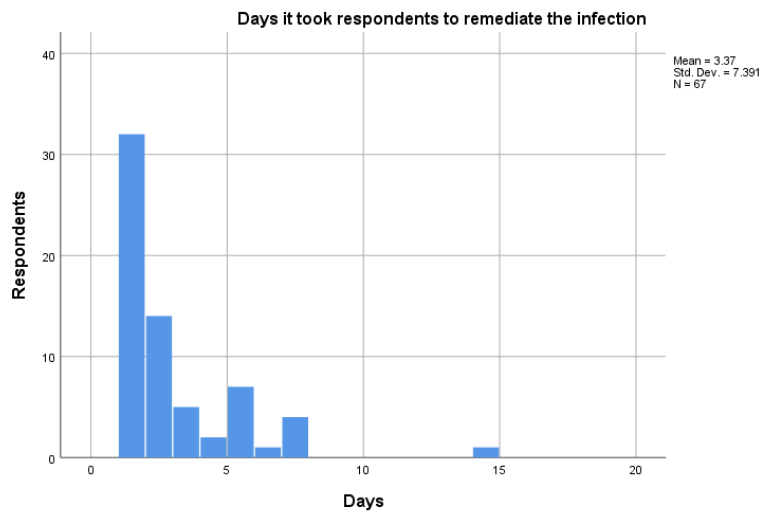


Figure 5.10: Histogram of how long it took respondents to remediate the infection, out of the 67 respondents that did remediate the infection and excluding an outlier that took 60 days to remediate from the graph

9.2%), to lost data (6 answers; 6.9%). Three respondents even replaced their phone completely, which is a hefty financial burden. Alarmingly, 6 respondents (6.9%) have received aggressive and some even threatening texts from the numbers their infected smartphones spread the Flubot infection to. That is also the biggest difference between experiencing harm before and after the notification in the sample, the (threatening) aggressive texts have only been experienced before being notified. The other answers are relatively the same for both categories (i.e. before and after being notified) and similar frequencies of the other answers too. Some respondents named multiple aspects in their elaboration, that is why there are more answers than respondents per category.

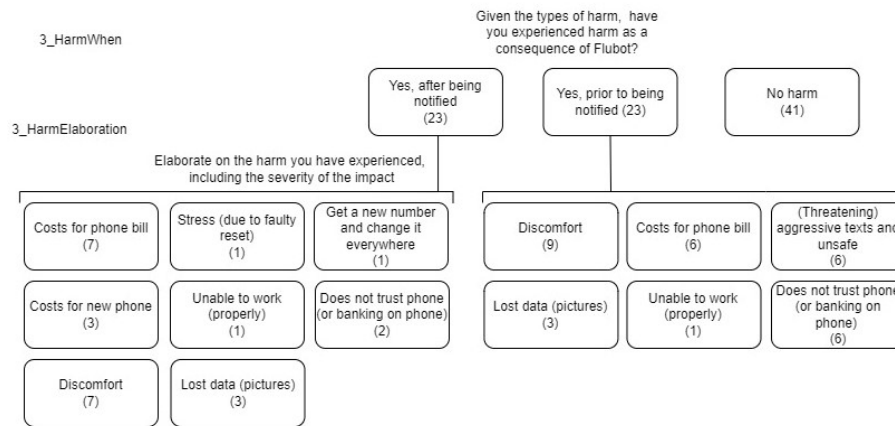


Figure 5.11: Whether the respondents experienced harm and whether it was before or after being notified, included are the elaborations given about the harm (out of 46 respondents having submitted that harm had been experienced)

Harm types selected, quantitative The 46 respondents that submitted to have been harmed by Flubot got to choose the different harm types and rated the impact of the harm types, it was possible to select multiple harm types. These ratings are shown in Figure 5.12. Reputational and societal harm are by definition relatively close to each other, which is shown in the results, where these two categories score almost exactly the same, predominantly in the lower ratings. Physical/digital and economical harm are more similar to each other when it comes to the frequency of ratings being more skewed towards the higher ratings, meaning respondents experienced these types of harm more heavily. Psychological harm has been experienced very moderately, where the majority of respondents have awarded the harm a 2, 3 or 4 (on a scale from 1 to 5), the three ratings having been awarded almost equally.

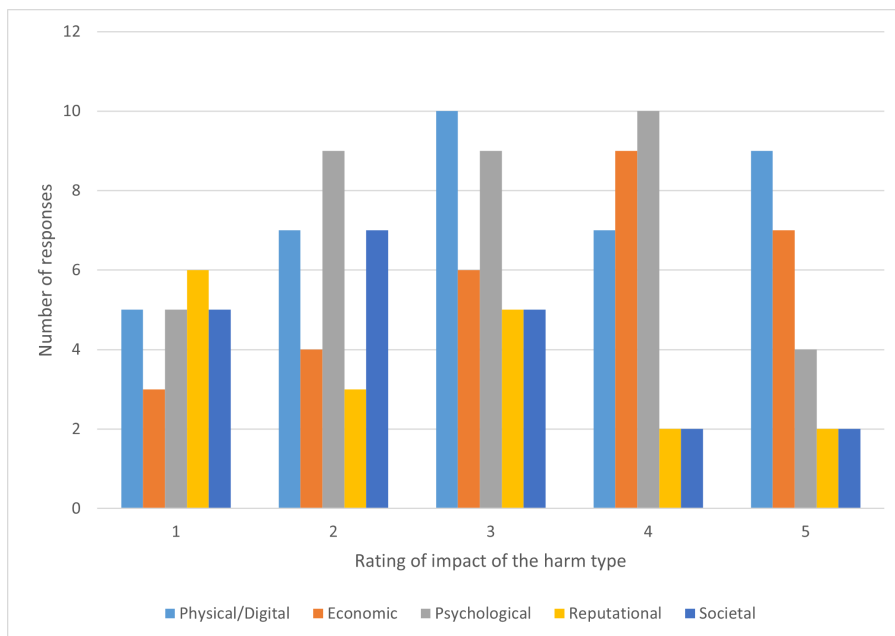


Figure 5.12: Chart of the harm types that have been selected and the rating of the impact that was awarded to the harm types

The averages of these ratings and the frequencies these harm types have been experienced are shown in Figure 5.13. It is shown more clearly that psychological harm has been experienced on average as a 3.0, so moderately impactful, and has been experienced very often, by 42.5% of the respondents. The most experienced harm is physical/digital harm, being experienced by 43.7%, and this category has also been the category with the second highest impact, scoring a 3.2 on average. The harm type that has the most impact is economic harm, scoring a 3.45, the frequency of having experienced economic harm is lower than the latter two types

discussed, experienced by 33.3% of the respondents. The societal and reputational harm are similar to each other, as mentioned previously, experienced far less often (24.1% and 20.7% respectively) and the impacts of these types of harm are the least severe (rated around 2.5).

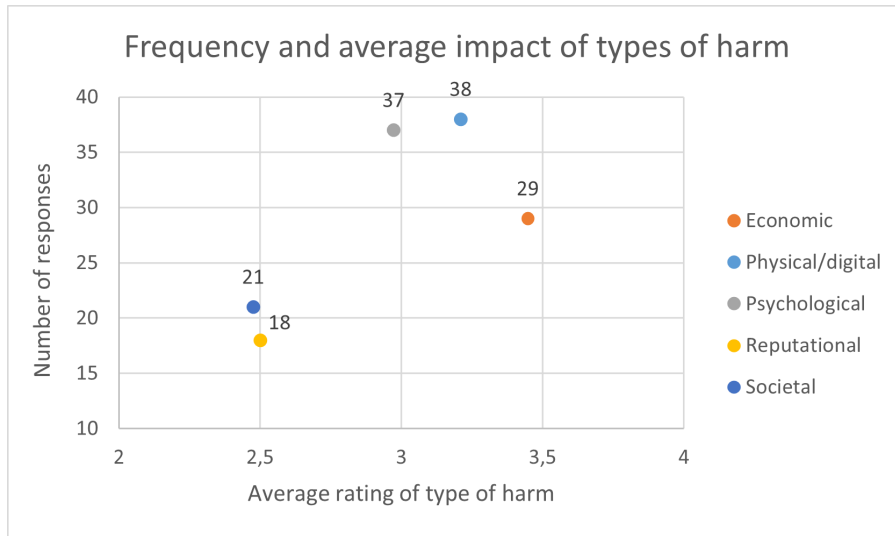


Figure 5.13: Graph of the average rating awarded to the harm types and the frequency of the harm type

5.1.6 Experience

SRQ 4: Satisfaction with the information and support provision The average satisfaction with the information provided by KPN is 3.17, which is slightly higher than the average satisfaction with the support provided, 3.14 (see Figure 5.14). That means that the respondents are moderately satisfied with the support and information provision. For both aspects, the ratings are relatively evenly spread out over the five possible ratings. With the moderate rating (3) being the most popular for both aspects (28.7% for information provision and 25.3% for support provision).

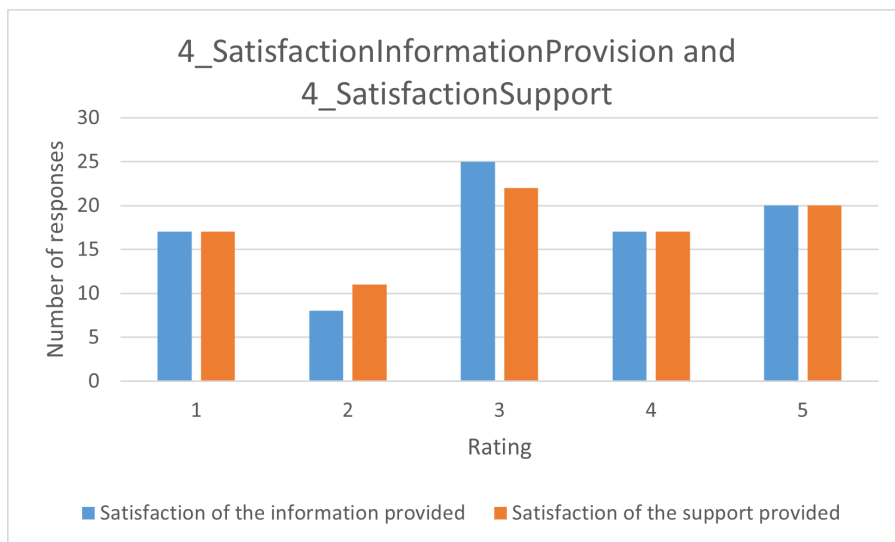


Figure 5.14: Chart of the frequency of the ratings provided on the information and support provision by KPN

Elaborations The elaborations the respondents provided on the previous question (i.e. rating the satisfaction with the information and support provision), have been categorised as either positive, neutral or negative, as seen in Figure 5.15. The answers are relatively evenly spread over the three categories with a slight skew towards the positive as is expected with the ratings being relatively evenly spread too and the average being just above 3 for both categories. According to 13 different respondents (14.9%) the notification is said to be clear and according to 10 respondents (11.5%) the help was quick, with two other respondents (2.3%) submitting

some answer close to the latter two but not exactly the same. Interestingly, 10 respondents (11.5%) have not remediated the issue themselves and further two respondents (2.3%) mentioned that neither KPN nor their notification was needed. 10 more respondents (11.5%) have said that the remediation was not performed by themselves, however no further elaboration to those answers was given. Slowness and timing has been answered most frequently as a negative elaboration, either with KPN being slow to block the phone (5.7%) and also being slow to unblock the phone (1.1%), or KPN taking long before clarifying the issue (2.3%), or having to wait till the next day to get in contact due to business hours (1.1%). Remarkably, one respondent (1.1%) has stated to have been misled by KPN that nothing was wrong, even though an infection has been detected on that IP-address. Furthermore, one respondent (1.1%) has lost their data due to the KPN store employee not informing the respondent correctly of the implications of performing a factory reset. Also surprisingly, one respondent (1.1%) finds the measures to be too rigorous. The remaining two negative responses (2.3%), understandably, are about having to pay for the phone bill. 66 answers have been given, meaning that 21 respondents (24.1%) have not answered this question.

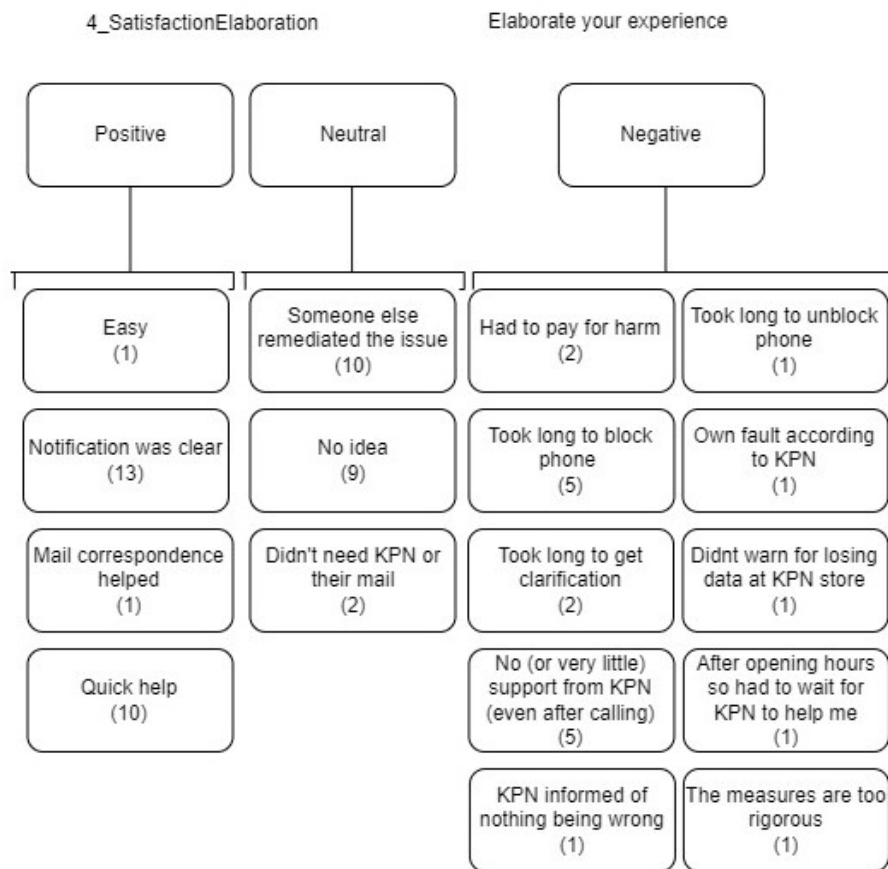


Figure 5.15: The categorised elaborations respondents gave regarding their satisfaction ratings

SRQ 4: Changed phone interaction For the last question posed in the survey, respondents have answered that the majority (62.1%) has changed their interaction with their phone because of the infection, as seen in Figure 5.16. This means 37.9% of respondents have not changed how they interact with their phone. The elaborations respondents gave on how their interaction has changed, vary from a very broad and all-encompassing answer like "More careful" (most frequent, 27.6%), to a more specific answer of "Not clicking on (email) message from unknown sender" (25.3%). Of the latter answer, 10% stated specifically to not clicking on email messages which is not effective in preventing smishing-based malware and most likely the result of being misinformed or drawing incorrect conclusions. Other precautions that respondents have taken following the infection are installing anti-virus software (2.3%), being more careful with installing applications (2.3%), buying a new phone (1.1%), not using financial applications anymore (1 response; 1.1%), and only answering the phone if it is a known number (1.1%). The latter measure is unrelated to Flubot malware, meaning that here too a respondent has been either wrongly informed of the cause or has drawn an incorrect conclusion of what could have been the cause. It is possible that the respondent is mixing up Flubot with other malware they might have experienced, or assume to be the point of discussion. One respondent (1.1%) abstained from giving an elaboration.

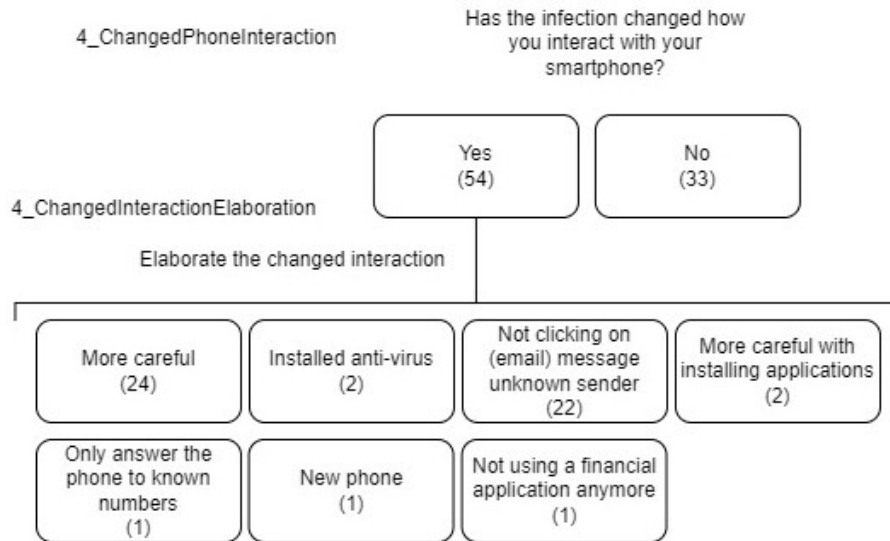


Figure 5.16: The elaborations respondents gave on how their interaction with their phone changed

5.1.7 Correlations

The survey included different types of questions, the answers provided have been converted to three types of variables for descriptive statistics, namely nominal, ordinal and scale variables. For further analysis, ordinal and scale variables are used to determine whether significant correlation coefficients exist in the sample, as an indication for the larger population. The ordinal and scale variables that have been included for this analysis are shown in Appendix I. Spearman's Rank-Order correlation has been performed on these variables. The analysis shows some significant correlations, as seen in Figures 5.17 5.18. The most statistically significant correlations are (correlation is significant at the 0.01 level (2-tailed)):

- 1. Demo_SkillLevelSmartphone and 4_SatisfactionInformationProvision: a correlation of 0.324 and a 2-tailed significance of 0.002 with a N of 87. This means that a higher perceived skill level of smartphone usage and remediation correlates to a higher satisfaction experienced by the information provided by KPN in the context of the Flubot infection, and vice versa.
- 2. 1_AverageWeeklySMS and 1_LikelihoodClickingUnknownSender: a correlation of .402 and a 2-tailed significance of 0.000 with a N of 87. This means that a higher average weekly number of texts received correlates to a higher likelihood of a respondent clicking on a text from an unknown sender.
- 3. 1_LikelihoodClickingUnknownSender and 3_HarmReputational: a correlation of 0.444 and a 2-tailed significance of 0.002 with a N of 48. This means that a higher likelihood of clicking on a text from an unknown sender correlates to the reputational harm being experienced by Flubot as more impactful, and vice versa.
- 4. 3_HarmEconomic and 3_HarmReputational: a correlation of 0.434 and a 2-tailed significance of 0.002 with a N of 48. This means that a more impactful reputational harm experienced by Flubot correlates to a more impactful economic harm experienced by Flubot, and vice versa.
- 5. 3_HarmEconomic and 3_HarmSocietal: a correlation of 0.492 and a 2-tailed significance of 0.000 with a N of 48. This means that a more impactful societal harm experienced by Flubot correlates to a more impactful economic harm experienced by Flubot, and vice versa.
- 6. 3_HarmPsychological and 3_HarmReputational: a correlation of 0.517 and a 2-tailed significance of 0.000 with a N of 48. This means that a more impactful reputational harm experienced by Flubot correlates to a more impactful psychological harm experienced by Flubot, and vice versa.
- 7. 3_HarmPsychological and 3_HarmSocietal: a correlation of 0.538 and a 2-tailed significance of 0.000 with a N of 48. This means that a more impactful societal harm experienced by Flubot correlates to a more impactful psychological harm experienced by Flubot, and vice versa.

- 8. 3_HarmReputational and 3_HarmSocietal: a correlation of 0.879 and a 2-tailed significance of 0.000 with a N of 48. This means that a more impactful societal harm experienced by Flubot correlates to a more impactful reputational harm experienced by Flubot, and vice versa.
- 9. 4_SatisfactionInformationProvision and 4_SatisfactionSupport: a correlation of 0.620 and a 2-tailed significance of 0.002 with a N of 87. This means that a higher satisfaction experienced by the support provided by KPN correlates to a higher satisfaction experienced by the information provided by KPN in the context of the Flubot infection, and vice versa.

Correlation nr	Question title	Question	Correlation	Significance 2-tailed	N	Correlation nr	Question title	Question	Correlation	Significance 2-tailed	N
1	Demo_SkillLevelSmartphone	How experienced are you in using and remedating a smartphone? On a scale from very unexperienced (1) to very experienced (5)	0.324	0.002	48	6	3_HarmPsychological	Psychological harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or 'No impact'	0.517	0.000	48
	4_SatisfactionInformationProvision	How would you rate the information provision in the original email about the remediation of flubot? On a scale from very bad (1) to very good (5)					3_HarmReputational	Reputational harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or 'No impact'			
2	1_AverageWeeklySMS	How often on average do you receive SMS texts per week? Excluding friends and family	0.402	0.000	87	7	3_HarmPsychological	Psychological harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or 'No impact'	0.538	0.000	48
	1_LikelihoodClickingUnknownSender	How likely is it that you will open a URL link inside a SMS text from an unknown sender? On a scale from very unlikely (1) to very likely (5)					3_HarmSocietal	Societal harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or 'No impact'			
3	1_LikelihoodClickingUnknownSender	How likely is it that you will open a URL link inside a SMS text from an unknown sender? On a scale from very unlikely (1) to very likely (5)	0.444	0.002	48	8	3_HarmReputational	Reputational harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or 'No impact'	0.879	0.000	48
	3_HarmReputational	Reputational harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or 'No impact'					3_HarmSocietal	Societal harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or 'No impact'			
4	3_HarmEconomic	Economic harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or 'No impact'	0.434	0.002	48	9	4_SatisfactionInformationProvision	How would you rate the information provision in the original email about the remediation of flubot? On a scale from very bad (1) to very good (5)	0.620	0.002	87
	3_HarmReputational	Reputational harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or 'No impact'					4_SatisfactionSupport	How would you rate the available support and the provided tools from KPN? On a scale from very bad (1) to very good (5)			
5	3_HarmEconomic	Economic harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or 'No impact'	0.492	0.000	48						
	3_HarmSocietal	Societal harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or 'No impact'									

Figure 5.17: Correlations found in the survey results, of a 2-tailed significance of 0.01 and less

The less statistically significant correlations are (correlation is significant at the 0.05 level (2-tailed)):

- 10. Demo_SkillLevelSmartphone and 4_SatisfactionSupport: a correlation of 0.221 and a 2-tailed significance of 0.040 with a N of 87. This means that a higher perceived skill level of smartphone usage and remediation correlates to a higher satisfaction experienced by the support provided by KPN in the context of the Flubot infection, and vice versa.
- 11. 1_LikelihoodClickingUnknownSender and 3_HarmPsychological: a correlation of 0.348 and a 2-tailed significance of 0.015 with a N of 48. This means that a higher likelihood of clicking on a text from an unknown sender correlates to the psychological harm being experienced by Flubot as more impactful, and vice versa.
- 12. 1_LikelihoodClickingUnknownSender and 3_HarmSocietal: a correlation of 0.299 and a 2-tailed significance of 0.039 with a N of 48. This means that a higher likelihood of clicking on a text from an unknown sender correlates to the societal harm being experienced by Flubot as more impactful, and vice versa.
- 13. 3_HarmEconomic and 3_HarmPsychological: a correlation of 0.341 and a 2-tailed significance of 0.018 with a N of 48. This means that a more impactful psychological harm experienced by Flubot correlates to a more impactful economic harm experienced by Flubot, and vice versa.

Correlation nr	Question title	Question	Correlation	Significance 2-tailed	N	Correlation nr	Question title	Question	Correlation	Significance 2-tailed	N
10	Demo_SkillLevelSmartphone	How experienced are you in using and remediating a smartphone? On a scale from very unexperienced (1) to very experienced (5)	0.221	0.040	87	12	1_LikelihoodClickingUnknownSender	How likely is it that you will open an URL link inside a SMS text from an unknown sender? On a scale from very unlikely (1) to very likely (5)	0.299	0.039	48
	4_SatisfactionSupport	How would you rate the available support and the provided tools from KPN? On a scale from very bad (1) to very good (5)					3_HarmSocietal	Societal harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or "No impact"			
11	1_LikelihoodClickingUnknownSender	How likely is it that you will open an URL link inside a SMS text from an unknown sender? On a scale from very unlikely (1) to very likely (5)	0.348	0.015	48	13	3_HarmEconomic	Economic harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or "No impact"	0.341	0.018	48
	3_HarmPsychological	Psychological harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or "No impact"					3_HarmPsychological	Psychological harm: Give an estimate of the impact of the harm, on a scale from low impact (1) to high impact (5) or "No impact"			

Figure 5.18: Correlations found in the survey results, of a 2-tailed significance between 0.01 and 0.05

5.2 Target group 3: Interviews

The interview that was performed, recorded, transcribed and anonymised (see Appendix H), with a single target group 3 subject provides answers that are in line with the results of the survey.

The takeaways from the interview are that:

- the subject did not use the email address that was provided to KPN anymore and was using a newer one for some time already;
- therefore the subject had not read the warnings about Flubot.
- given that a notification would have been received, the data subject claimed that they would have been likely to have taken action..

Descriptive statistics on active cases The KPN broadband connection of the interviewed data subject reported six different cases. A new case was created, for the same KPN IP, every time a connection has not been detected between a KPN IP and an infected C&C for a fixed number of days. Whereafter, the Flubot infection was detected again. This happened six times in total on this IP address. The event counters (i.e. the number of times a Flubot connection was detected on separate days on the same IP address of the KPN broadband connection, before a new case was started), starting from November 2021 till the 22nd of June 2022, totalled 126 times.

The 14 remaining active cases or customers have logged long infections too. The most recent infections detected on these IP-addresses are from February 2022 but the oldest are from August 2021. The average infection length, assuming it is a single infection for all these cases, is 7.6 months for these customers. The number of times the infections have been registered, ranges per IP-address from 40 times to 156 times, and is registered 103.6 times per IP-address on average. The detections have been spread out over a number of periods, ranging from 2 to 15 periods. The results are shown in Appendix J.

5.3 Desk research

5.3.1 End-user remediation advice

There is only one full measure to completely remediate a smishing-based malware, namely, factory resetting the mobile device. Flubot is notoriously hard to detect for end-users. If the end-user is not warned by a telecom provider, for example, it is up to the end-user to determine a Flubot infection. It is likely that the end-user is faced with the consequences of such an infection, e.g. by receiving an increased phone bill or seeing unwanted transactions. If the end-user detects something to be amiss on their phone and, somehow, suspects it to be caused by Flubot, it is still hard to determine whether a Flubot infection has actually occurred. The remediation advice is not of much use when it comes to determining whether a smartphone is infected, most of the accessible articles on Flubot do not mention anything about how to determine an infection, including KPN's notification and additional support web page [62, 82, 103, 106].

Europol and the Dutch Police do mention the same message regarding how to detect a Flubot infection, namely: "There are two ways to tell whether an app may be malware: if you tap an app, and it doesn't open

or if you try to uninstall an app, and are instead shown an error message" [30, 76]. Unfortunately, these instructions are still vague and imply that if an application does not open, it may be malware, and not just an application that has not been updated or just simply does not work anymore, which is not unheard of. Only if the end-user starts looking specifically for ways to determining whether their smartphone is infected with Flubot, it is possible to find more concrete instructions. The most concrete guideline the end-user might find online is to "Check to see if your phone has a Voicemail application with a blue cassette in a yellow envelope as its logo. Also check for delivery service apps, like FedEx or DHL" [16, 44]. Many search results from Google, regarding "How to determine Flubot infection", do not mention actionable steps to take, only what to do if an infection has occurred [30, 34, 62, 76].

Once an infection has been established, it is important to prevent further harm. A bandage to stop some of the bleeding is preventing the phone from connecting to the internet completely to prevent any data having been captured by the malware to be shared. It is crucial to not use any applications with sensitive information, especially financial apps or web pages where sensitive information is filled in or saved. Keylogging and screen grabbing (i.e. the malware being able to see and log everything happening at that exact moment) might still happen, and share all that information once an internet connection is made. Then there is the sending of SMS texts, disconnecting from the internet will not prevent SMS texts from being sent or being captured by the software. However, it will prevent further contact lists from being accessed through the infected C&C servers, so no new numbers will be added to the list of numbers being sent a SMS, including malicious links. Flight or safe mode, where a smartphone has no connection to the internet or any other wireless connection, is the only solution for an end-user to completely prevent any further harm, if important (financial) data has not been stolen already. By placing this larger bandage, i.e. turning flight or safe mode on, the end-user is given the opportunity to find and perform the best remedy for the infection, i.e. performing a complete factory reset.

After the reset, it is important for the end-user to load the latest back-up of the phone, before the infection. The next step in some of the advice is to change passwords for accounts and services used from the expected beginning of the infection or, to be safe, all the crucial applications [106]. Except for the harm already having been inflicted on the end-user, before performing the factory reset, the end-user might lose additional data which had not been backed-up in the chosen back-up version. This is an issue the end-user should be informed of, when being notified of the infection and the needed remedy. Looking on the internet, similar remedies are given. To cater to the needs of end-users not wanting to lose any recently stored or gathered data, it is often recommended to perform a back-up of the data that the end-user would like to keep (see Figure A.2). Making a back-up of the data can be done safely if the phone is not connected to the internet. However, keeping the phone unconnected and ideally in flight or safe mode, is rarely mentioned. KPN does mention this on the KPN site, once you have clicked on the link in the notification mail. Unfortunately, the notification mail itself does not mention this side note [82]. This means that if the end-user follows the instructions of the notification mail, the malware is screen grabbing everything that the end-user is doing on that phone and, potentially, sending more SMS texts, putting others in danger and racking up a bill for texting, whilst the end-user is making, or planning to make, a back-up of all the data expected to be lost in the factory reset. An end-user should be informed of the available options and remedies, for them to make an informed decision and to not feel misdirected or misinformed afterwards. Time is needed for an end-user to make an informed decision, i.e. by putting the phone in flight mode. Currently, most advice is directed towards performing the factory reset (see [30, 76, 103, 106]). The advice often addresses the issue of having to back-up pictures and other data you might lose in the factory reset A.1 [62]. However, this leaves the end-user exposed to further harm and others are potentially put in danger of getting infected as long as that infected device is not quarantined.

Because the end-user is (completely) unaware of the potential harm that is being inflicted due to the nature of the malware, it is hard and, in some cases, nearly impossible for the victim to determine at what moment the harm was inflicted. This leads to the perception that the harm was ongoing, even after the factory reset, giving the victim a wrong impression that the remediation did not work or the telecom provider being too late with their measures, in some cases regarding the request of victims to telecom providers to block their phone to prevent further harm, see Figure 5.15. Unfortunately, the applications of the telecom providers that show the outgoing phone calls and phone bill are often delayed, making it very confusing for the victim. Furthermore, when it comes down to harm inflicted on others, there is absolutely no way for a victim to see how (many) others have been impacted. Only one information source on the internet, which is accessible for victims, mentions anything about the possible further spread and suggest warning others [106]. Currently, most advice is directed towards performing the factory reset and sometimes includes information about the need for saving pictures or other data that might get lost, by backing it up. Only when looking specifically for flight or safe mode inside the

search term, advice on putting the Android smartphone in flight or safe mode whilst backing the data up and performing the needed factory reset, will be shown. It cannot be expected of victims, who have been informed that their Android device has been infected, to include such specific terms in their search. Especially, when the victim is already surprised by or wary of the warning as there is almost no way of determining whether the device is actually infected.

5.3.2 Flubot evolution

At the start of conceptualizing and scoping the research, an understanding was established of Flubot being under control, specifically for KPN. The number of IP-CC cases were going down and the SMS auto blocks detected and disconnected less and less phones [52, 99]. Based on these assumptions, the research was originally designed to survey older and current infections, sampled by both SMS auto block and IP-CC connection cases, which at the beginning of the research were assumed to have accounted for 200+ new cases per week. However, during the research period more accurate numbers were given by KPN, weekly 10-20 IP-CC cases and 30-50 SMS auto block cases. The misconception of Flubot being under control was due to Flubot evolving significantly, as does most of the newest malware and technology, and at the end of May 2022 it was taken down by an international cooperation between cyber police units. This had effects on the approach and execution of the research. It led to a search for answers, as the global cases trend did not correspond with KPN's trend. The NCSC, the Dutch National Cyber Security Center, had a similar perception to that of KPN, that after the end of 2021 Flubot had not been the threat it used to be, and degraded the threat to a lower level [64].

The evolution of Flubot, elaborated in Chapter 2, provided an insight into the development and improvement of the aforementioned malware [68, 70]. However, when looking at the measures taken against Flubot, specifically inside KPN, it became clear that measures had not been improving at the same rate as the malware, nor was it even known to all relevant departments and bodies that the malware had improved so much. It was not known, before, that the newer versions of Flubot made use of DNS-Tunneling-over-HTTPS, essentially circumventing DNS blocklists. Coincidentally, the NCSC had stopped updating their DNS blocklists as of the end of 2021. The NCSC reported that the reason for not updating the DNS blocklists is because the threat-level of that malware had been lowered and it was therefore no longer necessary to update the DNS blocklists, not that the measure had become ineffective [64]. The NCSC based their threat-level assessment purely on the number of cases that had been detected. Luckily for the NCSC, the newer Flubot versions would not have been slowed down with DNS blocklists, so the impact of the decision to stop updating DNS blocklists only made it easier for older Flubot versions to roam free. The older versions were soon to be overtaken by the newer versions anyway.

The measure used by KPN to auto block phone numbers once a SMS threshold has been reached, was a very effective way of flagging and limiting the impact of Flubot. It was in KPN's best interest to curb the SMS traffic as most customers have an unlimited SMS bundle, meaning that the customers (i.e. victims) do not incur directly for the costs made by Flubot infections, but KPN does, unless the customer has a limited SMS bundle in their subscription. By stopping infected phones from sending more texts, KPN's financial costs are limited. Unfortunately for KPN and end-users, data has shown that Flubot also adapted to these limits and started sending less texts daily through infected phones, to numbers much harder to distinguish from reasonable usage, especially with the newer versions [52]. This means that cases of older Flubot versions are easily stopped but the newer versions are harder to detect and, consequently, to stop. This created a situation where it was hard to estimate how many Flubot infections there were and how urgent it was to curb Flubot.

The second measure employed by KPN (i.e. the IP-CC connection) has been used the longest and has been successful too. The issue with this method is that the notification states that the customer has to figure out which Android device is infected, without any additional information on how to figure that out. At the end of email, there is a link included for additional information and likely to be used by victims that do not know which device to remediate, however the site that the end-user is redirected to contains hardly any information on how to pinpoint which phone to remediate. This makes remediation very hard in households with multiple Android phones. It should be noted that it can be considered counterintuitive for a victim to click on a link in an unexpected notification, clicking on an unknown link is the cause of the infection, especially as the client is unlikely to experience anything directly from Flubot in the earlier stages. And even if the factory reset was successful for the correct phone, because of the lack of direct feedback, customers might end up resetting other Android devices afterwards unnecessarily. On the other hand, because there is no direct feedback, some end-users might perform the factory reset on the incorrect phone, leaving the infected phone untouched and assuming every-

thing is safe again, until a new notification pops up three or more days later. As long as the infection keeps getting detected by Shadowserver on that IP-address, the customer will receive email notifications every third day. A design flaw of this means of informing someone is that, as has been corroborated by the only interview performed, the email address connected to a broadband connection might not be the email the customer uses regularly. This means that the customer might not see any of the notifications and remain unaware of the infection.

The updated versions of Flubot (i.e. 4.9 and newer were detected and registered from October 2021 till the end of Flubot), as mentioned in Chapter 2, are capable of changing the domain name generator remotely, using a wider variety of domain names, and making use of DNS-tunneling-over-HTTPS. This means that the newer versions are able to circumvent the IP-CC connection, i.e. from October 2021 the growing share of newer versions was not detectable by their IP-CC connection. The infections with the newer versions might only have been detected by the SMS auto block, which too became less effective after some time. In figure 5.19 it is shown when the number of cases started to be considered low, a few months after Flubot 4.9 was registered for the first time. In November 2021 older versions of Flubot were the majority of cases, which is confirmed by Bitsight’s finding that by January 17.6% of cases were of Flubot 4.9 or newer, and that explains why there was still a peak in November of Flubot cases [96].

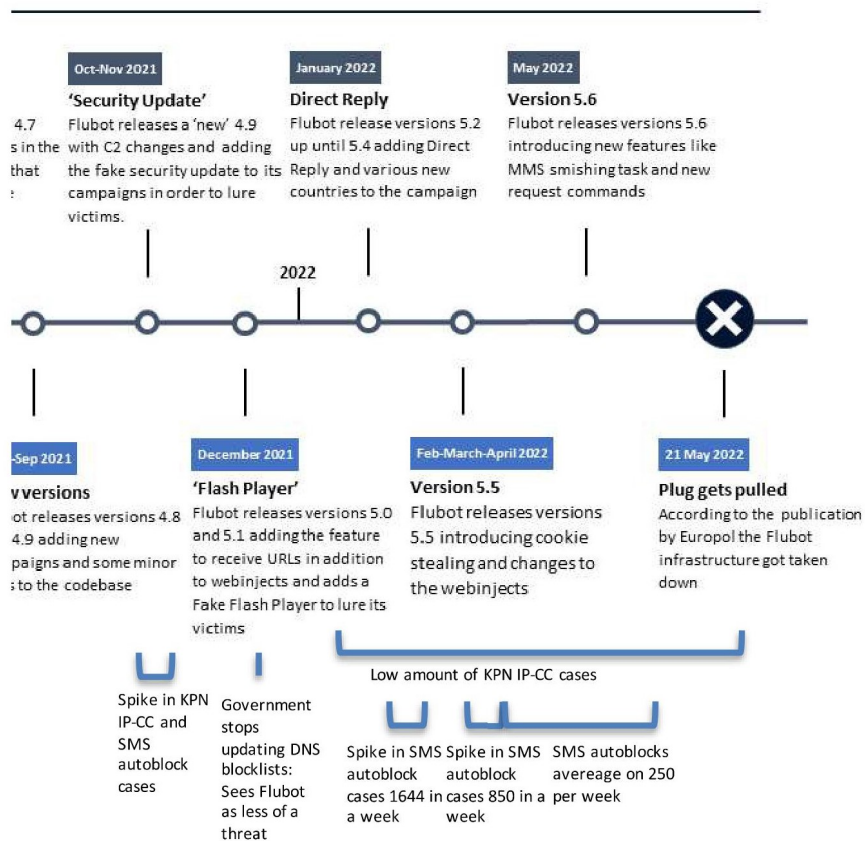


Figure 5.19: The timeline of Flubot supplemented with measures and key aspects of Flubot and its remediation ([89])

The SMS auto block measure had encountered two more peaks in 2022, whilst there was no IP-CC peak anymore. This confirms the finding that the newer versions of Flubot were able to circumvent IP-CC detection by Shadowserver, however, the infections were still caught by SMS auto block. Up till the end (i.e. May 2022), there were far more SMS auto block cases registered than IP-CC cases, which had not been clearly communicated between the relevant departments within KPN, this explains why it was unknown that the IP-CC detection method was outdated and only catching a sliver of the larger pool of infections [52].

Understandably, the urgency to fight Flubot had decreased for both government and KPN as the detected cases had decreased over time. Not coincidentally, the decision of the NCSC to stop updating DNS blocklists as a result of their decision to downgrade the threat-level of Flubot, was based on fewer Flubot cases by December, when newer variants started appearing more and the older variants were detected and, presumably, stopped by the measures employed. The effectiveness of the measures used against Flubot, up to 2022, should not be underestimated, as the peaks in both SMS auto block and IP-CC cases did only last for a few weeks at a time. The SMS auto block measure was useful for much longer even.

5.3.3 Limitation of current detection methods

With the current measures in place, only older versions of Flubot are caught and remediated. This means that there is no clear picture of the total number of cases there were in the Netherlands. Because of the Flubot network having been taken down by the international police collaboration, the spreading of the virus has stopped and only infections before the take-down might stay around for some time. However, because there is no sight on the newer versions of Flubot, there is no clear picture of how many remaining infections have been remediated and how many there are still lingering.

J-CAT (Joint Cybercrime Action Taskforce) It is a global (mostly European) task force that includes cybercrime departments from a range of countries, has only existed since 2014 and performed 118 operational actions till 2021 [29]. This task force focuses on the "key cybercrime threats and targets by facilitating the joint identification, prioritisation, preparation, initiation and execution of cross-border investigations and operations by its partners" and "J-CAT chooses and prioritises which cases to pursue based, among other things, on proposals from the country liaison officers" [29]. For this task force to target Flubot, the threat of the malware must have been considered dangerously high, as the relatively small list of operational actions are directed towards severe crimes and people responsible for them, such as dark web platforms, child trafficking rings and dangerous hacker groups responsible for large ransomware attacks. This means that the decision, to comprehensively tackle Flubot, was made before the end of 2021, when Flubot had shown its effectiveness (i.e. the large number of cases), or that the decision was made after 2021 and that it was known inside the cyber police departments, and potentially other governmental agencies, that Flubot was posing a significant threat, even though the registered number of cases went down in the beginning of 2022 in the Netherlands and the threat level had been lowered by the Dutch National Cyber Security Center [64]. The latter possibility implies that it was known that the detection and remediation methods in place were insufficient. However, because no stakeholder, including the J-CAT and the NCSC, was able to confirm this, it is hard to prove that it was known or suspected inside the J-CAT and other governmental organisations that the detection and remediation methods either were or were expected to be insufficient to curb Flubot.

5.4 Fogg Behavior Model applied to end-user remediation

Even though the Flubot network has been taken down, which means that the malware has stopped spreading and that infected devices do not harm the end-user actively anymore, it does not mean that it has no impact on the device. There is a chance that the malware keeps turning the battery save mode off, as is one of the functions of Flubot, essentially draining the phone unnecessarily, lowering the lifetime of the phone. Furthermore, Fox-IT confirmed in their blog the suspicion raised, that it is possible for the Flubot network to be restarted from a different hosting service, making use of the already contaminated devices [89]. Therefore, it is crucial to incentivise the owners of currently infected devices to remediate the infection before these devices can be used to give Flubot a boost if it reappears. Convincing end-users to reset their device to factory settings now that the effects of the dormant malware are essentially unnoticeable is much harder, unfortunately.

The Fogg Behavior Model is applied to the situation an end-user finds himself in when notified of a Flubot infection by KPN (and their dormant infections), i.e. the more an end-user is motivated to remediate a dormant infection and the easier it is to remediate an infection, the more likely the end-user is to change their behaviour and perform the remediation when a trigger occurs (e.g. being informed by KPN of a Flubot infection). The criteria for behaviour change, including the underlying aspects are shown in Figure 5.20. It is important to not overestimate the possibility for behaviour change. It is commonly assumed that the right phrasing with the right examples could always trigger a person to change their behaviour, which is an overestimation of what triggers can do, according to research performed by Herley [40]. That assumption is based on the fact that people make an incorrect cost-benefit analysis of their situation and are ill-informed. However, Herley has found

that end-users tend to make very rational decisions, given their perception and position. This should be kept in mind when discussing any external or intrinsic motivators of end-users and the possibility to change any behaviour.

5.4.1 Motivation

In general, the motivation to remediate an infection depends on the person, whether the end-user takes cyber threats seriously or not, which is influenced by whether the end-user has been impacted negatively by a cyber threat before. Experienced pains tend to have a strong impact, stronger than the same experienced pleasure (i.e. losing 100 dollars has a stronger impact than winning 100 dollars), pain is the first of three drivers of motivation as seen in Figure 5.20. The motivation needed to incite behaviour change can be increased by raising cyber threat awareness or by informing end-users of the impacts and risks of smishing-based malware for example, once a prompt (i.e. a warning or notification of being infected) occurs [48, 102]. These tactics are used to play into the end-user's fear, the second driver of motivation.

Furthermore, the social rejection that can happen after spreading the Flubot virus, e.g. by others sending back texts to the infected victims, is the last driver of motivation. By informing the end-user of possible social rejection that can result from being slow to remediate an infection or getting infected in the first place, the end-user might start fearing the social rejection too, increasing the motivation to do something about the infection, if there is an infection [102].

"Social motivations (i.e., motivations driven by values or wanting to help/please others) are much stronger and longer lasting than instrumental motivations (i.e., motivations related towards gaining material reward or avoiding material cost)" according to Herley [31, 40]. This makes social acceptance, the opposite of social rejection, and pleasure, the opposite of fear, more valuable and effective aspects to focus on when trying to motivate an end-user in remediating an infection or even behaving more securely. Furthermore, social motivators tend to work better when secure online behaviour is observable [25, 31]. This means that when secure behaviour can be seen by peers, it helps to motivate secure behaviour. Das et al. came to a similar conclusion, that social triggers leading to a user's behaviour change or already secure behaviour, in general, make it four times as likely that the end-user will share that with others [24].

Another finding by Das et al. was that people with low security behaviour intention, i.e. "the intention to behave in a manner consistent with expert-recommended security and privacy advice", are much more susceptible to security and privacy behaviour change, than people with high security behaviour intention [24]. Combining these latter findings, it means that people that are not or less invested and motivated in behaving securely, i.e. following expert recommendations, are especially susceptible for social triggers.

5.4.2 Ability

Ability is about simplification through six aspects, as seen in Figure 5.20, namely: time, money, (physical or mental) effort, brain cycles, social deviance and routine. Remediation generally does not cost money, unless you pay someone else to perform the remediation. The ability to remediate comes mostly down to effort, time and possibly brain cycles needed to figure out what to do. In a rare instance money is the obstacle to remediate the infection, as shown by the survey (see Figure 5.9).

5.4.3 Prompt/trigger

As seen in Figure 2.5, prompts or triggers only work once the activation threshold has been crossed. The prompts are perceived as annoying or distracting if the motivation is too low, even if the ability is high. If the ability is too low, even with a high motivation, the prompts are perceived as frustrating [32]. Therefore, to enact or to stimulate end-users to remediate a smishing-based malware infection it is important to keep the remediation as simple as possible (i.e. high ability), the motivation high enough; and the trigger should be timed once these latter two aspects have been met. Otherwise, warnings (or other prompts) could be seen as annoying or even frustrating. This might lead to end-users becoming more hesitant to read and follow other warnings, impacting warnings and remediation processes for other security issues too.

In the case of Flubot and similar smishing-based malware infections, a typical prompt is the email notification a victim receives that would inform the victim of having an infected device as a result of Shadowserver tracking a connection that was made with an infected C&C server (see the notification in Figure A). In the case of KPN,

another prompt would be getting a notification that the cellular connection is blocked in combination with the cellular service stopping to work as a consequence of an unusually high amount of SMS texts being sent, i.e. the SMS auto block notification. A more indirect prompt is finding out, either by being informed (e.g. by other end-users having received a malicious SMS from the infected phone) or by noticing it themselves (e.g. that the phone bill has skyrocketed for no apparent reason). Depending on the timing, a general warning sent out by government institutions or telecom providers, could be a prompt too. Such a warning only triggers behaviour change when a smartphone user has an infection and realizes they may have clicked on a malicious link, or when a warning might lead to the end-user becoming more careful with opening SMS texts, including the link.

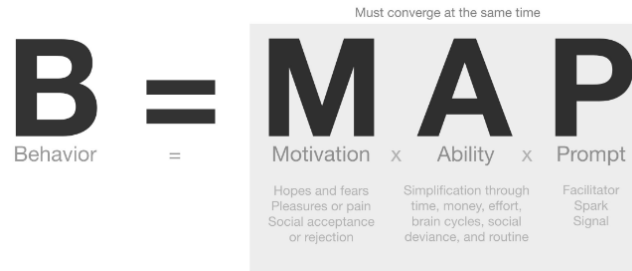


Figure 5.20: The criteria, including underlying principles that lead to behaviour change, according to the Fogg Behavior Model [102]

5.4.4 For prevention

The Fogg Behavior Model could also be applied in the context of prevention, in this case to prevent an end-user from clicking on a malicious link or to prevent the malicious malware from being downloaded [32]. By making downloading an external application very hard, an end-user would only succeed with sufficiently high motivation and it being not hard enough, which is unlikely. Measures could be applied to allow certain prompts (i.e. SMS texts) to be shown only when it is known that there is low motivation or the steps are made very hard for an end-user. In that scenario the end-user is not refused any texts, letting the end-user decide for himself whether to click on or download anything. Instead of having a measure that makes a decision for the end-user, running the risk of blocking non-malicious texts, applications or links.

Das et al. have found that people with high security behaviour intention, are more likely to follow proactive security and privacy behaviours [24]. This means that the preventive usage of the Fogg Behavior Model applies better to the more securely behaving end-users.

The application of the Fogg Behavior Model regarding the remediation and preventive steps is shown in Figure 5.21, the three target groups including their reactive and preventive measures are also shown in the Fogg Behavior activation graph in Figure 5.22.

Target group	Reactive / proactive measures	Motivation and ability	Trigger	Security behavior change examples
older people and people more likely to follow experts' recommendation	Proactive	The motivation of this group is generally higher, which makes them more suitable for proactive measures. If the measures are deemed not too hard, then they might lead to proactive security behavior changes. (S1: too hard to do and S2: easy to do)	Contacting (i.e. phone, mail or email) about preventive measures (i.e. SMS-filtering applications, or just not clicking on links in texts from unknown senders), the ease of the measure dictates whether S1 or S2	Incorporating SMS-filtering, or becoming more cautious about clicking on unknown links
younger people and people less likely to follow experts' recommendation	Reactive	Generally, the motivation to improve security behavior is relatively low, and sometimes it is deemed too hard or to take too much time. However, in the case of informing about an infection the motivation is often significantly higher. Then it still depends on the assessment of the end-user whether it is deemed feasible. (S3: too hard to do and S4: easy to do)	Contacting (i.e. phone, mail or email) about reactive measures (i.e. resetting phone), the ease of the measure dictates whether S3 or S4	Resetting phone
younger people and people less likely to follow experts' recommendation	Proactive	Social influences are effective for enacting security behavior change. This means that the motivation is increased, and if the end-user deems himself capable of improving (not too hard to do), then security behavior change might be enacted. (S4: enough motivation and S5: not enough motivation)	Facilitating social discourse about security behavior changes (i.e. creating an environment for it or incentivising end-users to share their behavior change), the social discourse experienced with a specific social trigger dictates whether S4 or S5	Incorporating SMS-filtering, or becoming more cautious about clicking on unknown links

Figure 5.21: Fogg Behavior Model applied to three end-user target groups

The survey including the correlations between different aspects, the interview including the descriptive statistics of the remaining cases, the desk research and the application of the Fogg Behavior Model provide insights and results are to be put in the appropriate context. This makes it possible to understand how applicable the results are and what they actually mean, which is discussed in the next chapter.

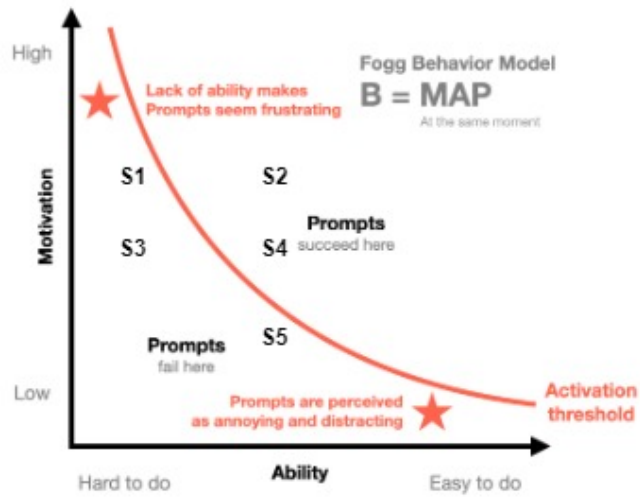


Figure 5.22: Three target groups of Fig 5.21 applied in the activation graph

Chapter 6

Discussion

The results and findings found and provided in the last chapter, are discussed in this chapter in their appropriate context and supplemented with or contradicted with relevant (academic) findings. The characteristics of the sample and the answers provided are compared to other research and used to check how representative the sample is. The division of the different subchapters is based on the correlations found in the previous chapter.

One of the reasons smishing-based malware is such a big threat, is because SMS is a trusted means of communication, as email used to be in the earlier days [43]. This vulnerability in trust has been exploited in email phishing and after years of receiving spam and phishing, in combination with notifications about getting phished, the sentiment towards email has changed completely. The average success rate of email phishing campaigns was as low as 1% by 2018, compared to the significantly higher success rate of smishing campaigns (tens of times higher) [43]. This can partly be attributed to the filters that have been employed to filter out phishing and spam mail, which has lessened the impact of phishing. If the success of smishing-based malware will go through a similar evolution, it will likely mean that people will be impacted badly as SMS texts still seem trustworthy, leading to the decline of the trustworthiness of SMS, if enough people will be impacted negatively and enough coverage will be given on this topic, a natural breaking mechanism of sorts. However, with the knowledge of phishing and the harm smishing-based malware can inflict, it is better to prevent such a cycle, or at least the harm that comes with a large number of smishing-based malware infections.

6.1 Notification

Notifying consumers and end-users through email has been proven to be effective in studies, inside KPN it has not been studied, but as the measure has worked well in limiting Flubot peaks before November 2021, it can be assumed it works well in general [95]. Stock et al. concluded that a notification system based on email has technical (i.e. the email getting flagged as spam) and non-technical drawbacks (i.e. the receiver distrusting the email), logically, KPN has experienced some of these issues. Notifications, especially warnings of infections, tend to not be trusted and, therefore, judged to be spam by the end-users themselves. Rodriguez et al. and Stock et al. found that distrust negatively impacts the end-users in triggering them to act on notifications including a warning or security issue [86, 95]. Not trusting a notification can partly be explained because of the unexpected timing of the warning. Flubot is a notoriously hard to detect type of malware as it does not show anything suspicious. The only ways of noticing is through an increased phone bill or sudden transactions, the phone being blocked, random SMS texts from other victims that your phone has forwarded malicious texts to or, incidentally, a notification from the telecom provider. Therefore, it is unlikely a phone user notices any of these aspects and most likely does not expect a notification about an infection and that influences the judgment to judge the notification to be spam. Wash et al. concluded that the unexpected timing of a notification is a key aspect for considering an email to be fishing, i.e. not taking the notification serious [107]. Given the Fogg Behavior Model, if a notification is considered spam then it will not function as a prompt for behaviour change for remediation.

Furthermore, of the 1684 victims contacted for the survey, 43 resulted in a no-reply. This means that 2.5% of the victims have by now a non-functioning email for contact information. Depending on how generalizable this is for the whole customer base of KPN, this would add up to a significant number of customers being unreachable through email. Furthermore, as the one interview has shown and if that interview can be considered indicative, there is also a portion of customers that have an outdated email, which is not unlikely as Return Path's report has shown that 9% of email addresses are completely unused [111]. Radicati's report in 2018 has shown that the

average user has 1.8 personal email accounts, combined with Return Path's finding that secondary accounts are 14 times less likely to lead to responses than primary accounts, meaning that if end-users provide a secondary email-address as contact information it is highly unlikely that the email notification is going to be read, and even less likely that the victim remediates the infection [80]. These outdated and/or secondary email addresses lower the effectiveness of the IP-CC notification system used to curb the spread of Flubot. The findings of the survey, see Figure 5.9, further confirm that even though the same email address was used both initially for informing the end-users and later for requesting to participate in the survey, 11 respondents (12.6% of the sample) gave being "unaware" of an infection as answer on the question why the infection had not been remediated. It is unlikely these respondents have been notified often as that would mean that it would have been very unlikely that they would have seen the survey request.

It can be assumed that between 65.7% and 50.6% of the respondents have become aware of the infection through the notification. The higher percentage is based on the fact that 23 respondents have stated to have experienced the harm after being notified, meaning that the notification was the first thing that made them aware of the infection. The difference between number of remediations and number of respondents having experienced harm is 21, i.e. the respondents that had been notified but did not experience harm, can be added to the 23 prior respondents, totalling 41 respondents. Then, assuming only respondents that remediated the infection had an infection, that leads to a group of 44 respondents out of 67, i.e. 65.7%. The lower percentage is based on the assumption that all respondents at some point had an infection, even if no remediation took place, leading to a group of 44 respondents out of the total 87 respondents, i.e. 50.6%.

Another finding is that it is very unlikely that a respondent will answer to the survey if the respondent has received more than two notifications about Flubot, as discussed in subchapter 2.4. Of the 152 surveys sent out to victims (Group 2) that received three or more notifications, none responded. The group (Group 1) of victims that only received one or two notifications responded more often with 88 times out of 1.532 surveys (5.7%). Putting this finding in a different context: that if an end-user has not remediated after two notifications, it might be very unlikely that the respondent will remediate at all. Rodriguez et al. had a similar finding that "many participants acted on or close to the first notification they received" [86], however the findings in this research are more extreme where no one responded if notifications had been sent previously at least three times. By determining at what point there is no use in notifying a consumer through email anymore might save resources and can lead to adaptive or changing notification mediums, to ensure everyone does get notified.

The data subject that participated in the interview had been notified 126 times in a span of 7 months, which is just higher than the average 103.3 times in 7.6 months for the totalling 14 remaining active cases of Flubot recorded, as seen in Appendix J. The assumption that respondents are unlikely to remediate after being notified a handful number of times, would apply to all remaining active cases (recorded on the 22nd of June), as the lowest amount of notifications (i.e. events in Appendix J) is 40. This would further imply to keep sending these cases emails would not impact them remediating the infection, and that if remediation is the goal different means of notifying are needed.

6.2 Age

The sample is relatively old, with only two participants under the age of 40 (see Figure 5.1). It is not unlikely to find an older sample as older people are more vulnerable and more likely to become cyber victims. When victimized, older people tend to be impacted more severely, they tend to lose more money compared to younger victims and find it harder to bounce back as their sources of income are more limited, impacting their health and well being too [67]. Older people are especially more vulnerable to spam, as they have less knowledge of security threats and they are more likely to trust those encountered in digital transactions [66]. That trust older people have more of towards spam could also be the reason for responding relatively more often to the survey, which, as a possible explanation for the older sample population, should not be ignored.

Paradoxically to being more vulnerable and impacted more heavily, older people are more risk averse as they think more about the threats, i.e. a higher perception of security threats [66]. An explanation for these opposite effects is that older people have a lower awareness of being susceptible to threats. This means that they underestimate how susceptible they are to threats, leading them to take risks that make them more vulnerable in the end. If older people would have estimated their susceptibility more accurately, such as the general population, then their risk adverseness would have led them to become less vulnerable to cyber threats and spam [66]. Wash and Rader had a similar finding, that older people tend to take more protective measures than

younger people if they are scared, but they generally do not respond well to teaching protective measures as older people generally do not believe that they are vulnerable [108].

6.3 Profession and perceived skill level

Unlike participants in similar studies, i.e. Rodriguez et al., where on average more technically skilled data subjects participated [86], this sample is not particularly tech-savvy or invested in cybersecurity or technology in general. On average the sample considers themselves just a bit more experienced than would be considered moderate or medium. Kumar et al., found in their study that people that are more familiar with security measures tend to show more secure behaviour [54], with this sample that would imply that the participants should engage less in (based on profession) or moderate (based on skill level) security behaviour. Depending on how accurate the perceived skill levels of the respondents align with the actual skills, which do not necessarily have to align, according to Forget et al. [33].

Perceived skill level has been shown, through the correlation analysis seen in Figure 5.17 and Figure 5.18, to have a strong statistically significant correlation with the satisfaction regarding the information provided ($r=0.324$, $p=0.002$) and a less strong and less statistically significant correlation with the satisfaction regarding the provided support ($r=0.221$, $p=0.040$). This implies that rating themselves higher on technical skill is exhibited in this sample with higher satisfaction scores. It could be that more skilled users need less of the information and support and therefore are more easily satisfied with the information and support they received. The reverse would imply that end-users that rate themselves less skilled experience less satisfaction because they might need more information and support. As both more-skilled and less-skilled get the same information and the support in general, especially if no additional support is looked for, regardless of the skill level.

6.4 Prior knowledge and cause infection

Prior to this research, around half of the respondents (48.3%) had already heard of Flubot, mostly through the news (71.4% of respondents that had heard of Flubot), then social media (42.9%), friends (38.1%), the telecom providers coming fourth and family fifth, as seen in Figure 5.4. However, having heard about Flubot does not necessarily mean that it is correct what one might have heard, as will be discussed in the next paragraph. It is unlikely that the telecom provider or the news will inform end-users incorrectly, so the inaccurate mouth-to-mouth communication (i.e. friends, family) is most-likely the cause of sharing incorrect information between end-users. Therefore, it is important to reach more end-users when smishing campaigns are running rampant again.

In the absence of correct information end-users will either fill in the blanks themselves and, often, incorrectly or have no clue at all. The majority of respondents has either no idea what could have caused the infection (47.1%) or has a wrong idea (10.3%, including answers: "Hack", "Called back to unknown number" and "Malicious (DHL) email (about parcel)"), as seen in Figure 5.6. This is an alarming number as that implies that a future infection is likely to happen to these respondents if faced with a similar malicious text again.

Furthermore, timing can influence a subject into judging a notification to be either spam (when unexpected) or serious (when expected) [107]. The opposite of an end-user not expecting a notification that informs of an infection and judging the notification to be spam, happens when an end-user does expect a parcel and receives a text about a parcel, including a link and how to track it, and judges the notification or text to be serious and not spam. This means that smishing-based campaigns that use parcel texts are more effective and dangerous in periods (for example before Christmas in most of Europe or during pandemics) and areas where ordering parcels happens more frequently [92]. The prediction that the global parcel shipping will double from 2020 to 2026 makes only for a more vulnerable population, with current measures and smishing-based malware making use of parcel texts [27]. At least 11.5% of respondents, that accurately pinpointed that to be the cause of the infection and specifically mentioned the parcel to be expected, have been tricked into downloading Flubot this way and it is likely the percentage is higher as some respondents have probably skipped some aspect of their idea of what the infection caused and 57.4% does either not know what the cause is or has a wrong idea of what could have caused the infection, see Figure 5.6.

Targeted campaigns A future risk of these campaigns is that smishing-based malware starts adapting campaigns based on the most popular parcel service per country or region. The parcel texts, currently, seem to

only impersonate DHL and UPS, however regional differences most likely influence the effectiveness as DHL and UPS are not the biggest parcel services everywhere. Anatsa, a similar smishing-based malware that is currently active, uses DHL, UPS and DHL impersonations for instance [87]. It might be useful for other popular parcel services to prepare for smishing-based malware to impersonate its services [92]. Furthermore, as some campaigns adapted Adobe updates as malicious texts, it is likely that smishing-based campaigns are going to branch out to impersonate other services, that are likely to be using SMS, as well, such developments would make smishing-based campaigns harder to detect and to inform end-users on. With previous campaigns, warning users was relatively easy because of most of the smishing texts impersonating DHL 5.6 [62, 103].

6.5 SMS texts received and likelihood of clicking on a text from an unknown sender

Intuitively, if end-users receive on average more SMS texts from unknown senders, the likelihood of clicking on a hidden malicious text is going to be higher, as the receiver is less likely to find receiving a text from an unknown sender to be odd. This is confirmed through the strong significant correlation ($r=0.402$, $p=0.000$), shown in Figure 5.17. It should be noted that a correlation does not mean causation, and that it could mean that they are caused by something else but move at the same time. Furthermore, because the smishing-based malware requires the end-user to download something external after clicking on the link, it does not necessarily mean that an end-user that receives more texts from unknown senders will get infected, that group does have to be more wary of such smishing-based malware. A counter argument could be made that when people do get more texts from unknown senders, by having to make judgment calls on the maliciousness of SMS texts more often, they might have trained themselves to be better at discerning genuine SMS texts from malicious ones.

Furthermore, a very significant correlation has been found between clicking on a link inside a text from an unknown sender and reputational harm, and a less significant correlation between clicking and psychological and societal harm have been found through the correlation analysis, see Figure 5.17 and Figure 5.18. Of the latter two correlations, the psychological harm has a stronger correlation and significance, meaning that an increased likelihood of clicking on a link from an unknown sender makes it likely to experience societal harm ($r=0.299$), more likely to experience psychological ($r=0.348$) and the most likely to experience reputational harm ($r=0.444$). The reputational correlation is least likely to be caused by chance, as it has the highest significance (0.000) with the same number of different values, then the psychological correlation (0.015) and then the societal correlation (0.039). In general these correlations mean that end-users most likely to click on a link from an unknown sender have experienced more reputational, psychological and societal harm (impacts ranked in that order), or, the opposite, that end-users least likely to click on a link from an unknown sender have experienced the least reputational, psychological and societal harm (impacts ranked in that order).

6.6 Suspicion and remediation

40.2% of the respondents suspected something that happened with their smartphone, prior to being notified and 77% remediated the infection, leaving a difference of 36.8% of respondents that suspected nothing but did remediate the infection after being notified, regardless of having read the notification. Assuming all suspicions were sound, as no elaboration given in Figure 5.5 can be deemed completely incorrect, the notification might have been enough of a trigger for these respondents to remediate the issues. It is possible too for these respondents that they would have remediated the infection anyhow, most likely both apply for these respondents but based on the questions asked no further detail can be given. Furthermore, of all the respondents that were notified and did not remediate (23% of the sample), only 11 respondents did not remediate because of not having read the notification or "unaware" (55% of non-remediated cases) and 2 respondents "did not know how to" and therefore did not remediate the infection, which implies that either no sense of urgency was felt or no way of fixing could be thought of, or both. In this case, using the Fogg Behavior Model, it seemed too hard for the respondents that even with motivation and a prompt no behaviour change was triggered. In such cases, a notification (i.e. prompt) can seem annoying and distracting (see Figure 2.5). For these two respondents a lack of urgency might have resulted in not sufficient motivation too, most likely it was a combination of seeming very hard and not enough motivation to look further or ask someone to remediate the infection. The respondent that deemed the remediation, or fixing the issue, to be too expensive might have assumed it or been informed by a third party of potential costs for letting someone else do it for them. This is an unfortunate perception, as the remediation, in theory, is easy and free. This could have been resolved if the respondent had contacted KPN Abuse, which was probably not clear enough for the person as the answer seems to suggest that the

infection would otherwise have been remediated. 2 respondents gave an "unused phone" as the reason for not remediating, which is a valid argument if nothing of value is on the phone and there is no chance of them being turned on again, however, it is hard to determine with the given answers how certain the unusability of the phone is and how exactly that relates to the infection.

The lack of feedback when removing malware has been shown, by Bouwmeester et al., to lead to despair and uncertainty regarding the success of the remediation [11]. This lack of feedback is an issue for the Flubot remediation too, as there is no notification or prompt that is shown to end-users when remediating Flubot. Furthermore, it is also not addressed in the notification taking away some uncertainty, as it could be mentioned in the notification that if the respondent does not receive any more notifications the remediation has been conducted successfully. This might be the cause of two respondents answering with "no way of knowing" on why the respondent did not remediate the infection, assuming it means that the respondent found no way of determining whether the remediation was successful. However, it could also imply that the respondent found no way of knowing whether an infection had occurred in the first place. On the other hand, some respondents might incorrectly have assumed to have remediated the infection, which would lead to more frustration with KPN due to their informational provision and support, if harm would have been experienced afterwards due to the infection. This explains some answers (i.e. "no (or very little) support from KPN (even after calling)" and "took long to get clarification") given regarding the remediation experience, see Figure 5.15.

From the elaborations a perception arises that only three respondents deemed themselves to be unable to perform a remediation (i.e. found it too hard according to Fogg's behaviour Model), and two found it not necessary (i.e. not having enough motivation) given that the phone is not used. All other respondents either remediated the infection (77.0%), were not aware of the infection and that has stopped them from remediating (14.9%), had an unusable phone anyway, or the phone was not theirs, when the notification was received. This implies that the trigger (i.e. the notification), if received and with a functioning phone, did manage to trigger the respondents into performing the remediation (i.e. behaviour change). This means that the notification does work, when received.

6.7 Harm

The sample is almost evenly spread between respondents having experienced harm and not having experienced harm, unlike the expectation of the sample consisting of victims being impacted by harm and therefore wanting to share their experience. Only respondents having experienced physical/digital and economic harm are skewed towards the extremes (i.e. the majority rating their harm a four or five out of five, see Figure 5.12). This is shown in the average ratings, scoring a 3.2 and 3.45, respectfully, with psychological harm averaging very moderately at 3.0. The latter harm type and physical/digital harm have been experienced the most often too, by 42.5% and 43.7% of the respondents, respectively. The elaborations, see Figure 5.11, on the harm experienced back this up, as most answers are about costs, stress, lost data or discomfort. The most shocking elaborations are about respondents having received aggressive and even threatening texts and, consequently, feeling unsafe. This has only happened to victims that were unaware of the infection, and not expecting anything at all. This might be explained by the fact that if an end-user is aware of the infection, aggressive texts do not impact the end-user that much or are not memorable because the cause for these texts is clear and such alarming threats can be neglected, another explanation could be that unaware victims let the malware send out more texts and are therefore more likely to receive extreme reactions back.

Experienced harm is often a very strong prompt, especially harm with a high impact such as financial loss or receiving aggressive texts, which is often accompanied with a strong motivation that the victim realises just then. This leads then to the victims remediating the infection eventually, even if they initially deem the remediation to be too hard, finding some way to perform the remediation. As experienced pains (i.e. losing money or being threatened) have a very big impact, larger than experienced pleasures.

The expected harm to older people has been shown, according to Nicholson et al., to experience more gravely is not shown in the data gained from the survey [67]. No significant correlations have been found between age and any type of harm. It is possible that the sample is not large enough to find statistically significant correlations between age, harm types and the severity of the harm experienced. The sample is on average already relatively old (i.e. averaging 63), with 79 respondents being in between 51 and 81, making it harder to find a significantly strong correlation than if it were an evenly spread sample starting at 31 and ending at 81. However, this is not very likely as the correlations found are relatively low with the highest

correlation being 0.157 with economical harm, and there even being a negative correlation between age and physical/digital harm, -0.089, and the statistical significance for both correlations being very high, 0.550 and 0.288 respectfully (see Figure I.1). Another possible explanation for the discrepancy between Nicholson et al. findings and these results is that the elderly might be less aware of any harm [67]. This correlation cannot be checked, as the question 3_HarmWhen, on whether harm has been experienced and whether it was before or after being notified, produces nominal variables (i.e. 0, 1 and 2) and not ordinal variables, which are needed for the analysis of the correlations. Therefore, only the 46 respondents that were aware of having experienced any harm were included in the 'harm type' questions and consequently in the correlation analysis of the harm types.

6.7.1 Types of harm linked

Five correlations have been found, of the statistically most significant correlations between types of harm, as seen in Figure 5.17. The strongest correlation is between societal and reputational harm, which are also very close to each other when looking at the scores given (see Figure 5.12), including the average scores (see Figure 5.13). This strong correlation can be explained by the similar definitions used for reputational harm (i.e. "harm pertaining to the general opinion held about an entity"); and social and societal harm ("i.e., a capture of harms that may result in a societal context or society more broadly") as phrased by Agrafiotis et al. and used in this research too [1]. Both Reputational and Societal harm are correlated with Psychological and Economic harm, all with similar correlations around the 0.5, which are all strong correlations. This implies that a victim that experiences either economic or psychological harm, is very likely to also experience reputational and societal harm, and vice versa.

Even so, the correlation between psychological and economical harm itself is less strong and less statistically significant, albeit still statistically significant ($p=0.341$, $r=0.018$, see Figure 5.18). This in combination with the occurrence of psychological and economical harm implies that if harm is experienced it is likely to have been either economical, psychological or physical/data harm, and when it is economical or psychological harm, it is also likely to experience reputational and societal harm. These implications make it possible to create more targeted indirect detection systems for smishing-based malware and warning systems that, once one of these harm types have been established by and for a victim, the victim should also watch out for the other types of harm, as mentioned previously.

6.8 Satisfaction with the information and support provision

In general the remediation advice provided in the notification has been experienced as positive when looking at the elaborations given (15 respondents said either "easy", "notification was clear" or "mail correspondence helped", compared to 7 respondents saying either "took long to get clarification" or "no (or very little) support from KPN (even after calling)", see Figure 5.15). However, when looking at the ratings, the information provided scored only a moderate 3.14 out of five, which paints a different picture that there is a quite a bit of room to improve. Both ratings of satisfaction (i.e. information and support provision) are strongly correlated ($p=0.620$) to each other, the correlation is statistically significant. This implies that if a customer is satisfied with the information provided, then most likely satisfied with the support provided as well, and vice versa. The ratings for both satisfaction aspects are relatively evenly spread and not really skewed towards one side, this implies that the sample is not specifically unsatisfied with the remediation process and therefore is venting their frustrations through this survey, nor the opposite, where the customers are very satisfied and therefore willing to share their experience.

The abuse team, which is responsible for helping victims once they have been notified and need more information, is only available during working hours, which one customer has stated to be an issue, meaning that they had to wait for help, see Figure 5.15. Two others raised a similar issue that it took a long time to get clarification on the issue that they had been informed about. Looking at the remediation time, 68.7% (46 respondents) of the victims had remediated the infection within two days, of which 47.8% (32 respondents) on the first day, as seen in Figure 5.10. Assuming that the 67 respondents that did remediate the infection are the only end-users that actually have had a Flubot infection and the other respondents have only had an occasional infected device connect to their KPN broadband connection, it is likely that the victims that experienced some type of harm were the ones that remediated the infection as quickly as possible as they had more motivation to lessen the harm. This group would account for 68.7% (or 46 of the 67 cases), which accounts for all quick remediations (68.7%), realistically speaking it is somewhere in between 68.7% and 52.9% (assuming

all respondents were infected, i.e. 46 out of 87 respondents). Then, as a victim, having to wait a day can seem very long and frustrating. It is understandable for them to feel frustrated (according to the Fogg Behavior Model discussed in Chapter 3 and shown in Figure 2.5) if they have been triggered (by a notification of an infection and some type of harm experienced) and are motivated (to remediate the infection and prevent any further harm) but are not able to perform the remediation, because they feel like they need help [102]. This applies especially to the group that experienced the harm after being notified (34.3%, or 23 respondents out of 67), as for that group it is easier to pinpoint why the harm is experienced and thus more frustrating to be unable to do anything about it and this group is most likely to see KPN as culprit for the frustration, which will be reflected in the customer satisfaction and possibly in customer retention (i.e. the ability to keep a customer over time). Furthermore, as seen in Figure A.1, the victim is asked in the notification to follow the steps as soon as possible, ideally the same day, to remediate the infection but there is no mention of the victim turning on flight or safe mode in the meantime. 52.2% of the infections get remediated two days or more after being notified, which can leave the malware unobstructed in their malicious functioning, further spreading the virus and possibly inflicting (more) financial, psychological, data, reputational and societal harm on the victim. By putting the phone on flight or safe mode, the malware will not inflict more harm on the victim itself and the overall population, until the malware infection is remediated.

The elaboration on the measures being too rigorous, as seen in Figure 5.15, hints at measures employed by different KPN systems, most likely SMS auto block or another system employed by KPN for an unrelated type of issue or malware. Because the survey has been sent to victims that have been detected through the IP-CC connection, no actual measures have been taken except for notifying the victim of an infected device through this system. The same applies to the respondents answering that it either took too long to block or to unblock the phone. The responses make sense if the respondents are talking about the SMS auto block measure as it essentially blocks the cellular and internet connection of the phone. The rigorosity of the measure has also been criticised on the KPN forum, as seen in Figure K.1. There are customers that do send out large numbers of SMS texts each day, which is a reason to get an unlimited bundle from KPN, and apparently these customers feel deceived if, because of the SMS auto block measure, they cannot in fact send a huge, almost unlimited, number of SMS texts. It is said these customers get blocked when they do send such large numbers of texts, and that it can happen repeatedly, without it being possible to get an exemption from the SMS auto block function.

The SMS auto block measure has only become more rigorous, as KPN experts have determined that the SMS-threshold for the SMS auto block measures has been lowered to combat the lower and less-detectable number of SMS texts sent by Flubot. This arms race between Flubot and the SMS auto block measure will reach a point where it will be very hard to distinguish 'excessive' amounts of SMS texts from usual amounts. This will then only lead to more opposition and negative feedback from customers, and more customers feeling deceived with having purchased an unlimited bundle, lowering the customer satisfaction, even though the measures are taken to protect the customers. It would then require a more nuanced approach, not only looking at the absolute numbers of texts sent but also at the spreading of the texts and to which numbers the texts are sent. Due to the secrecy of correspondence legislation it is illegal to look inside the texts by telecom providers, therefore the SMS auto block measure is limited to indirect information about the texts [38, 73]. It might be useful to look at the length of the SMS texts sent to determine whether it is likely to have been spam or personal messages. Furthermore, it is possible and likely that consumers use SMS texts to spread information or for marketing purposes, which would have to be accounted for to make sure that it stays possible when using a more nuanced SMS auto block function.

The IP-CC detection system that only informs victims, of there being an infection, is a very unobtrusive measure that might need to be backed up with more active measures, as nine respondents stated to have had "No idea" of the infection when asked about the satisfaction and five respondents felt like there was little to no support from KPN, as seen in Figure 5.15.

Furthermore, the remediation advice that is included in the notification that victims receive is considered clear and easy to understand, see Figure 5.15. However, 10 respondents still needed someone else to remediate the infection, which means that the notification did not manage to trigger and help the receiver enough to remediate it themselves but it did manage to accomplish indirectly what was intended, to remediate the infection but by someone else. 2 respondents, unfortunately, have not remediated the infection after having received the notification because they did not know how to, see Figure 5.9. For such cases it is important to determine what was missing in the notification or what was not clear enough, to be able to better help victims by making use of

the measures already in place, it must be admitted that there is no one-size-fits-all notification that could help everyone completely. Further assistance is then needed, which five respondents answered to have experienced insufficient of.

6.9 Changed phone interaction

The survey results show that even end-users who have not experienced harm due to the Flubot infection, have been impacted in such a way that it has changed their smartphone interaction, as 52.9% of the respondents experienced harm and 62.1% of the respondents have changed how they interact with their phone. Unfortunately, it is significantly lower than 77.0% of respondents that have remediated the infection. The difference becomes even larger if the two respondents (that answered with: "not answering the phone for unknown numbers" and "not using financial applications anymore") are excluded that have changed how they interact in such a way that does not make it less likely to have a further infection. The latter answer is more damage control than prevention. Furthermore, some respondents seem to be under the impression that an email might have caused the Flubot malware infection (see Figure 5.6 and 5.16, which helps with preventing falling for phishing emails but still leaves them open to a future smishing-based malware infection, unfortunately. These misunderstandings have a positive impact on the spreading and the global impact of Flubot and other smishing-based malware, which should be clarified to be able to tackle future successful smishing-based malware campaigns. The answer "more careful" is too vague to determine how well it helps in preventing further infections, just like "installing anti-virus" might help in the overall cyber security of the respondents, but does not necessarily have to help in preventing a future smishing-based malware.

6.10 (Incorrect) malware conclusions

The open answers provided throughout the survey give an indication of how well Flubot is understood by victims, and possibly non-victims (i.e. KPN broadband users that had an infected device of someone else connected to their connection once or twice). The initial notification(s) about a Flubot infection, (in some cases) the followup or other KPN correspondence and possibly the survey (including the sms-related questions and Flubot being mentioned often) have still left a significant portion of the sample without a correct understanding of Flubot, or more importantly of what is the cause of Flubot and similar smishing-based malware. Looking at the causes respondents gave for the Flubot infection, ranging from calling "foreign number through WiFi" or "calling back to an unknown number" to malicious emails, in combination with the 41 respondents that admitted having no idea what could have caused the infection, it shows that a clear understanding is missing for maybe even half of the respondents. The elaborations given on how the respondents have changed how they interact with their phone, as discussed in the previous paragraph, further confirm this finding. This is an important issue in future smishing-based malware campaigns, because unlike biological viruses, where victims build up a natural defense against a future infection which hampers the further spread of the virus, for digital viruses, such as Flubot, this has been shown not to necessarily be the case. Victims, when experiencing a pain and understanding it correctly, should never have to fall for any similar social-engineering tricks, thereby preventing any future smishing-based malware infections and ideally also informing others correctly. In the current situation, a significant portion of the respondents is still at risk for future infections and might inform others incorrectly, making a future smishing-based malware campaign more likely to succeed in spreading.

Examining the notification, there is nothing that indicates the infection could have been caused by clicking on a link in a SMS text and downloading malicious software, or any mention of SMS texts or downloading external software for that matter. It is possible that the victims received the notification and followed the instructions, without looking for the reason or just assumed to know what caused the infection. Furthermore, looking at how some respondents said to have asked others to remediate the infection, it begs the question whether it was then communicated with the victims properly how it was caused and how to prevent a future infection by the person that helped the victim, assuming the helper did know what caused the infection which does not have to be the case if the helper followed the instructions in the notification without looking further.

6.11 Limitations of the conducted research

The research performed has largely been based on KPN and its measures, policies, processes and customers. KPN is the largest telecom provider, together with Ziggo, in the Netherlands accounting for 40% of the market share. This shows to some extent how the findings can be generalized for the larger end-user population.

However, because no other large telecom provider has been included, despite attempts to include them (Ziggo specifically) in the study, there is no comparison. Therefore, it is hard to determine exactly how generalizable the data from this study is for the whole telecom market in the Netherlands. The sample itself is relatively old, which limits the generalizability of the sample on the overall population. It is important to note that the survey results are based on end-users that are (most-likely) Flubot victims, no baseline group was reached for comparison. This means that the results apply to Flubot victims and are generalizable for the victim population, the results can only function as an indicator for the overall population. The approach that was chosen to make use of the KPN forum for looking for aware uninfected end-users and to not make use of other platforms as well, has resulted in too few results. The number of members found that seemed suitable to be interviewed was too small. This resulted in zero interviews and no information gained from that target group. Getting results from that target group would have given additional insights and shown major differences between end-users that do and do not get tricked, creating a more complete picture of the smishing-based malware context. Furthermore, because the survey generally provides the perception of the respondents, as the submitted data is not coupled with objective data, the accuracy of the answers is hard to determine. It might be possible that remediation took much longer, for instance, or the victims might be under the incorrect impression that the infection has been remediated at all. Some answers indicated that the respondents might be talking about different malware infections.

The setup of using anonymous surveys naturally means that no questions can be asked about the answers given by the respondents, which can partly be resolved by asking for elaborations. However, as the elaborations have shown in this survey, the elaborations can still be vague and very short and, therefore, of no to little value for the analysis. This has been the case for some elaboration answers. A way of combating vague and short answers is to ask for specific aspects in their elaboration, however it was decided to not steer participants into any direction and to prevent respondents from getting overwhelmed by the survey, the minimal number of questions was asked with the shortest formulation and easiest ways of answering. Running the risk of getting the unusable answers, which sometimes happened. It became clear, by analysing the survey answers, that the reputational and societal harm distinction might not have been clear enough and some elaboration questions should have been more clear on what the respondent should elaborate on. Precautions were taken by consulting the supervisors, other researchers and KPN specialists to make sure a clear and comprehensive survey was drafted and sent out. The lack of time made it impossible to use test groups to determine how well the survey was formulated. This has resulted in the analyses of the harm types and its impact to be not as valuable as it could have been, just as with the elaborations being of no to little value.

Furthermore, it became clear, after analysing the answers, that some respondents still do not know what Flubot is or have a wrong idea of what Flubot is. This puts these respondents at risk for smishing-based malware. Because it was assumed that all respondents would know of Flubot or at least have a vague, but correct, idea of how it works and what to do against it, no message at the end was included to correctly inform the incorrectly informed and the ones that had no knowledge of Flubot.

The qualitative addition of incorporating an interview of an active case was helpful, however as it is a single interview it can only be used as an indication. This insight can be researched later on, however the findings of the interview cannot be generalized. Interviewing multiple data subjects would make generalizing this insight possible, however due to Flubot being taken down the remaining population is extremely small.

The nature and novelty of Flubot creates a situation where a balance has to be found and adhered to regarding how much to report and publish about, to prevent informing and nudging the malware threat actors on how to better improve the malware. However, findings need to be published and addressed to improve the telecom providers' and end-users' capabilities for defending against and dealing with such malware. Furthermore, as KPN has cooperated very generously and shared a significant volume of data for this research, it is also important to adhere to their policies as to what is considered sensitive information. These reasons have led to a measure against Flubot not being reported or mentioned, however the impact of that measure was researched. Furthermore, details on measures have been left out on purpose, not to inform malware threat actors too much with, possibly, dangerous information. The aspects and measures that have been left out would have contributed to the future research suggestions. However, leaving out certain aspects in the publishing of this paper does not change the (applicability of the) findings in this paper.

The limitations of the performed research and the discussion regarding the findings, lead to a comprehensive overview of the subject of this paper. This overview creates the basis for answering the research questions,

which is performed in the next chapter.

Chapter 7

Conclusion

This chapter starts with the main research question and then the sub research questions are addressed, including how the knowledge gaps are filled, in Subchapters 7.1 to 7.6. In Subchapters 7.7 and 7.8, the academic relevance and societal contribution are reflected upon. Then, based on the answers provided in the first six subchapters, recommendations are provided for the industry, other companies affected by smishing-based malware, and governmental institutions involved the smishing-based malware landscape, in Subchapter 7.9. The remaining knowledge gaps, that have not been addressed by this research but have been identified for future research, are mentioned in Subchapter 7.10.

It has to be mentioned that Flubot itself currently does not pose any active threat, therefore, addressing how well the detection and notification approach align with end-user's awareness is based on how it was perceived before June 2022. The necessity to understand how well these aspects are aligned is still very crucial and relevant, as similar malware is roaming the internet and experts agree on there being a high risk of Flubot returning, as it was very successful, or a copycat version. Restarting Flubot and its network would not take very much effort and cooperation between different malware threat actors is not unlikely. It is crucial for future campaigns to address and detect the malware better than in the last months of Flubot's life cycle. The quantitative study in combination with the desk research have led to findings to answer the main research question, by answering the sub research questions.

7.1 How has Flubot impacted consumers, of a Dutch ISP and telecom provider, with an infected mobile phone?

As with the arms race, once one side develops new techniques the other hand responds to counter them, this back-and-forth tends to keep going, until one side is completely defeated. In this analogy, it can be stated that Flubot has been defeated. However, in the greater context of smishing-based malware, it is more accurate to state that this battle has been won (against Flubot), but the war (against smishing-based malware) is not over. If anything, the next battle will most likely be lost. End-user remediation (advice), as provided by KPN, has impacted Flubot victims positively by helping them to remediate the infections. If the victims were reached, it generally led to the remediation of the malware infection, decreasing the spread of the malware campaign. This has led to the malware designers combining forces and further improving the malware, which it continuously did. Flubot became successful in spreading without being detected, leading to a consensus that the spread of Flubot had been curbed and that it therefore was no longer a serious threat. A negative effect was that there were no incentives for institutional and industrial organizations to improve the measures equipped to detect and combat Flubot. Which then led to Flubot going completely undetected, whilst still doing harm, up until it had been taken down by the international police cooperation. It is possible that the awareness of the current detection methods being unable to curb Flubot, might have been the reason for J-CAT to target Flubot, however this has not been confirmed.

In the later stages victims would have been exposed to harm and solving the issue would have been a guessing game at most, as it was assumed Flubot was not likely to be the cause. There is no clear picture of how many victims there have been in the Netherlands in 2022, however the rise in cases in April and March 2022 in Europe indicates that there must also have been a large number, which have gone undetected with the current detection methods.

For the few that did suspect an infection, the accessible information on Flubot is not of much added value either, as available advice often does not tell enough to determine whether an infection has occurred and how to properly deal with an infection. Furthermore, in most notifications and reports found on Flubot, only financial and data harm is mentioned. The prioritization to address the most common and most impactful harm is a rational decision, especially if informational provision is bounded by policies regarding simplicity (i.e. short and simple notifications). However, not addressing the potential of societal, reputational and psychological harm (especially the latter harm type because of its high impact and its high occurrence) might leave disproportional and lasting impacts on victims, as some have voiced. This might lead to digitally vulnerable end-users stopping to participate in the cyber environments, and, worst case scenario, getting left out of much of the digitalised services. This further exacerbates the impact of Flubot on victims.

Though Flubot has been taken down, the threat of smishing-based malware is lingering. We, with current detection methods and accessible information, are completely unequipped to deal with future campaigns. The urgency to combat future campaigns seems nowhere to be found, as we won the last battle. This puts smartphone users at further risk for future smishing-based malware campaigns.

7.2 SRQ 1: Are mobile end-users aware of being infected by Flubot?

Flubot is notoriously hard to detect, once it has infected a smartphone. The only victims that are aware of an infection by themselves, before any harm is experienced, are the ones that found downloading an external application to be fishy and could not find an application to delete, which alerted them of something being wrong. However, this group seems to be very small and only represents 2.3% of the sample. Other ways of finding out about an infection are either by becoming aware of harm caused, which still does not mean an end-users will be able to accurately determine that it is in fact Flubot, or by being alerted by others (e.g. telecom provider or a recipient of a malicious SMS text). Examples regarding finding out about an infection, range from increased phone bills because of a surge of SMS texts being sent, to other financial losses due to the financial applications being taken over, to the infected phone being disconnected from the cellular connection (which is accompanied with a notification on why the connection has been cut), to receiving aggressive texts from others.

Being informed by another party is the most common way of finding out about a Flubot infection. These notifications are either from other (potential) victims (ranging from just asking whether the sending infected smartphone is infected to aggressive reactions) or the telecom provider (e.g. KPN), informing a broadband connection owner by email that an infected device has made connection with their broadband connection.

The survey has shown that a significant portion of the end-users does not know what caused the infection, including a portion of end-users not having a clear picture of what caused the infection and what Flubot is. This indicates that in the larger population it is likely to be an issue as well. Up until the end of 2021, Flubot victims were generally aware of a Flubot infection, even though they were not always correctly informed. Since 2022, the share of Flubot victims being aware of an infection has dropped, as the detection systems have become less effective. It is likely that, in the last months of Flubot, the Flubot victims were, at least for some time, completely unaware of an infection and if they found out it is likely because of some harm they experienced.

7.3 SRQ 2: How have end-users acted on the Flubot infection?

End-users behave differently when it comes to remediating the issue they think has arisen. The remediation of Flubot is a relatively easy process of (putting the phone first in flight or safe mode, especially if the remediation is not conducted immediately) backing up any data that might be lost, performing a factory reset and then loading a backup of the data and the settings. However, because of the nature of Flubot, it is hard to determine which Android phone needs to be remediated and whether the remediation was successful (as there is no direct feedback loop in the remediation process).

Informed victims do not always directly remediate the infection, as a significant portion of respondents experienced harm after being informed and the majority of the informed victims mentioned to have conducted the remediation after one day. Around half of the remediation processes lasted between two and seven days. Furthermore, a quarter of the respondents had not remediated at all, because the victims did not trust the notification, did not know how to remediate and did not read the notification. According to the majority of the

respondents the instructions are clear, however to some the instructions are too difficult and that is the reason third parties are often asked to perform the remediation. If the end-user is aware of the infection and willing to remediate the infection, then, most of times, it is done correctly. Few victims buy a new phone, completely circumventing the remediation process. Other end-users, that are aware, decide not to remediate because they deem it too costly, too hard or irrelevant. The remaining end-users are unaware of the infection and therefore unlikely to remediate the infection coincidentally, i.e. performing a factory reset for another reason.

7.4 SRQ 3: Which types of harm have end-users experienced by Flubot and are there indicators?

Victims have experienced all five types of harm, as phrased by Agrafiotis et al. [1]. The type of harm with the largest impact is economic harm, then physical/digital harm, psychological harm, ending with reputational and societal harm, respectively. Regarding the impact: economic, physical/digital and psychological harm have impacted the victims the most, with reputational and societal harm having a significantly lower impact. Regarding the occurrence of the types of harm, physical/digital and psychological harm are the most common, then economic, and then societal and reputational, respectively. Combining the occurrence and the impact of the types of harm, it is important to focus on physical/digital, economic and psychological harm, and focus on reputational and societal harm less.

The average age of the sample is relatively high, which would corroborate previous findings regarding the influence of age on the severity of the impact, however no influence of age on the impact of the experienced harm has been found and it can therefore not be confirmed with these results. Correlations between types of harm have been found. If a victim experiences economic harm then it is very likely societal and reputational harm will be experienced as well, the same applies to psychological harm likely coinciding with reputational and social harm. Furthermore, when end-users are likely to click on links in SMS texts from unknown senders then it is likely that the end-user will experience reputational harm and it is a bit less likely that the end-user will experience societal and psychological harm. The likelihood of clicking on links from unknown senders, can be used to prevent further harm, or even prevent infections, just as the types of harm can be utilised as indicators to lessen other types of harm.

7.5 SRQ 4: How have end-users perceived the remediation process?

In general, the respondents were moderately satisfied with the information and support provided in the remediation process. The consensus in the survey is that the notification is clear and useful, and the required support is sufficient. However, because the survey only includes end-users that have been reached through the email notification system, a significant number of end-users have not experienced any remediation process at all, or at least not from KPN. The minority found the notification to not be clear enough and the additional support to be insufficient, including how long it took to get additional help. Most of the frustrations are directed towards the support rather than the notification.

The remediation process, in general, had a lasting impact on the end-users. Most of end-users are now more careful with how they interact with their phone, others are specifically more careful with clicking on unknown senders' messages and some are just more careful with downloading external applications. Unfortunately, some have been impacted in such a way that the remediation process has not helped them with how insecure they feel about using their smartphone, and, incidentally, some completely forego financial applications.

7.6 SRQ 5: How do available Flubot detection methods, of a Dutch ISP and telecom provider, align with the end-users' awareness?

Up until November 2021, the Flubot detection systems, especially the SMS auto block measure, were effective and well-equipped to deal with the predominant Flubot versions. The IP-CC detection system did work, however, because no baseline study has been performed it is hard to determine how well it functioned. It has been established that using email is the most efficient way of reaching potential victims, however it is not enough to reach everyone. The system becomes very inefficient in some cases as the likelihood of a potential victim reacting after two emails is already low. Furthermore, the IP-CC detection system is inherent to inaccuracy as it is impossible to pinpoint a specific infected device. Meaning that, even if the owner of the broadband

connection is reached, it does not naturally mean that the end-user is reached. The SMS auto block measure on the other hand, did lead to the end-user noticing the infection quickly, as all cellular connection was lost and a follow-up email was sent with information.

As the malware evolved, especially after October 2021, the detection approaches became more misaligned. The malware kept evolving but the detection measures did not, meaning that older variants of the malware became less prevalent. The newer campaigns integrated newer versions of Flubot, which were able to avoid IP-CC detection. This means that the IP-CC detection method only detected cases of older Flubot versions. End-users that had a newer Flubot malware infection, did not get notified at all, as their infected connections were not detected. Later on, at the end of the first quarter of 2022, the SMS auto block measure became less effective as well, as the malware adapted to sending lower amounts of SMS texts. At that point, victims were completely dependent on themselves to figure out whether an infection had occurred, which is nearly impossible, and how to deal with it, with the trigger generally being some type of harm.

7.7 Contribution to the academic knowledge

Knowledge gap 1: Lack of research on the efficacy of remediation for smishing-based malware victims Earlier versions of smishing-based malware have only existed since 2017, and this particular malware only since 2020, therefore the academic and industrial knowledge and literature is limited. When looking at the user remediation for smishing-based malware, there is no academic literature available and only a limited amount of accessible industrial knowledge regarding the impact of Flubot (and similar smishing-based malware) on the victims and the remediation thereof. This research has found issues in the complex environment of smishing-based malware that had not been identified before, like, the current overall inability to detect and tackle future smishing campaigns similar to Flubot and the overall information provision being insufficient.

Knowledge gap 2: Lack of policy for smishing-based malware for end-users and customers of telecom providers The research has found that the policies regarding smishing-based malware for end-users and consumers has been insufficient. This can be attributed to the most threatening malware having been taken down. This research has shown that the threat level was lowered much earlier than was appropriate, the only excuse for such a government decision would be to tackle the malware secretly, however this has not been confirmed. Furthermore, both government and telecom providers have employed warnings and notifications that lack important aspects, that otherwise could improve the end-user's ability to remediate the infection and prevent future infections.

Knowledge gap 3: Lack of research on the influence of technical skill and profession on security behaviour The study has not found any impact of technical skill and profession on the remediation process, the second identified knowledge gap. That is based on there not being a statistically significant correlation between the technical skill and other indicators, especially between how long it took to remediate the infection and the technical skill. To improve the understanding of a possible correlation between technical skill and the remediation process, specific cases with higher technical skill should be analysed more in-depth and the direct correlation between remediation and technical skill should be analysed, which has not been done in this paper.

7.8 Societal contribution

The findings of this research provide actionable improvements for the notifications and the notification system used by the largest telecom provider in the Netherlands, the stakeholder best equipped to enact an improved cybersecurity environment for smartphone users. The findings show an inability to curb any future smishing-based campaign, similar to Flubot, showing the need for improving detection and notification systems. These findings potentially can improve the smartphone cybersecurity environment, lowering the impact of future smishing-based malware campaigns. Furthermore, some of the findings can be extrapolated to other malware, and not just smishing-based malware, extending the potential for societal contribution. Addressing the types of harm in the remediation process and including help for future victims, can lead to helping the technologically less able and preventing them from completely foregoing digitalised services.

The research does not include analysing and researching ways of making the current detection methods, that have been proven to be ineffective, effective again. This is because of the limited resources (i.e. time and expertise). The research is targeted towards the less technical side of the remediation process and Flubot's impact on end-users. The findings and research are geared towards improving the notification system and the notifications to better help victims, assuming that the actual detection methods are going to improve at some point. Otherwise these findings and recommendations will only be applicable to the remediation process of similar smartphone malware, not future Flubot campaigns.

The recommendations are mostly made for KPN, not because KPN is obligated to do these tasks or because they have dealt with Flubot badly, but because KPN, as both a telecom provider and an ISP, has such an opportunity to enact improvements regarding the cybersecurity for smartphone users. This is because of the unique positioning they in this complex (cyber) system, by being able to reach a large share of Dutch smartphone users; having access to the cellular data and the internet connections. This provides KPN, which has curbed Flubot considerably in the Netherlands, given the constraints they operate under, in a unique position to further improve the (cyber)security of smartphone users. In general, the urgency to further the remediation process, especially regarding Flubot infections, might reasonably be low, however with these findings the impact of Flubot, if it or something similar returns, can be lowered. With the customer satisfaction and security in mind, it is reasonable and practical to further improve the measures against Flubot and similar malware. This applies to other involved parties, as well, such as the companies that have been imitated or that are likely to be imitated.

7.9 Recommendations

7.9.1 Companies imitated by smishing-based malware (e.g. DHL, UPS and Adobe) and companies likely to be imitated by smishing-based malware

Research in the field of 2FA and the abuse thereof by smishing, has shown that by using disclaimers inside 2FA texts can reduce the likelihood of end-users becoming a victim of social-engineering tactics. The disclaimers include some notion of: "if you did not request a 2FA code, ignore the text and do not share the text with anyone" [43]. In the case of Flubot and similar smishing-based malware it can be useful to include disclaimers inside genuine texts from impersonated services, e.g. parcel services. The disclaimer should include some notion of: "never click on a link inside a text from us, we, the parcel service, do not send links inside SMS texts" before the actual message. This would inform the public on what to believe and not to believe, when they make use of a service that has been impersonated. This improves the end-users' awareness, and minimizes the impact malicious impersonations have on the genuine brand image. If certain services and companies do not use SMS 2FA for customers, but have been imitated by smishing-based malware, it can be useful to include these disclaimers in other means of notification (e.g. mail notifications).

7.9.2 KPN and similar telecom providers

The adaptive notification system The notification system, based on emails and employed for the IP-CC detection, is limited by the KPN broadband connection owners' (i.e. KPN broadband users) usage of the email submitted to KPN. This limitation makes for a notification system that, for specific cases that do not react to the notification, is inefficient and ineffective. Incorporating an adaptive notification approach can help those specific cases and lower the burden on the system, including less emails having to be sent. This adaptive approach uses the same initial setup, where cases that have been identified by Shadowserver are sent a notification email. This is repeated at varying intervals, instead of the current three day interval. If the case is not resolved after five notifications in four weeks, the system highlights the case and different means of notifying are attempted, see Figure 7.1. It starts with looking for an alternative email addresses that might be connected to that specific KPN IP, if one is found then that email will be notified. A period of seven days is given for the victim to remediate the infection. If that does not resolve the IP-CC case, the KPN broadband owner will be contacted by phone or by letter or the broadband connection can be put in walled garden environment (i.e. blocking most internet traffic) as the next step, depending on which step is deemed more suitable for the infection at hand. This adaptive approach might be a heavier burden on the employees for it requires manual tasks, however, it will result in less ongoing cases and it is suitable for other cybersecurity issues and malware too. Figure 7.1 shows a diagram of the suggested adaptive notification system.

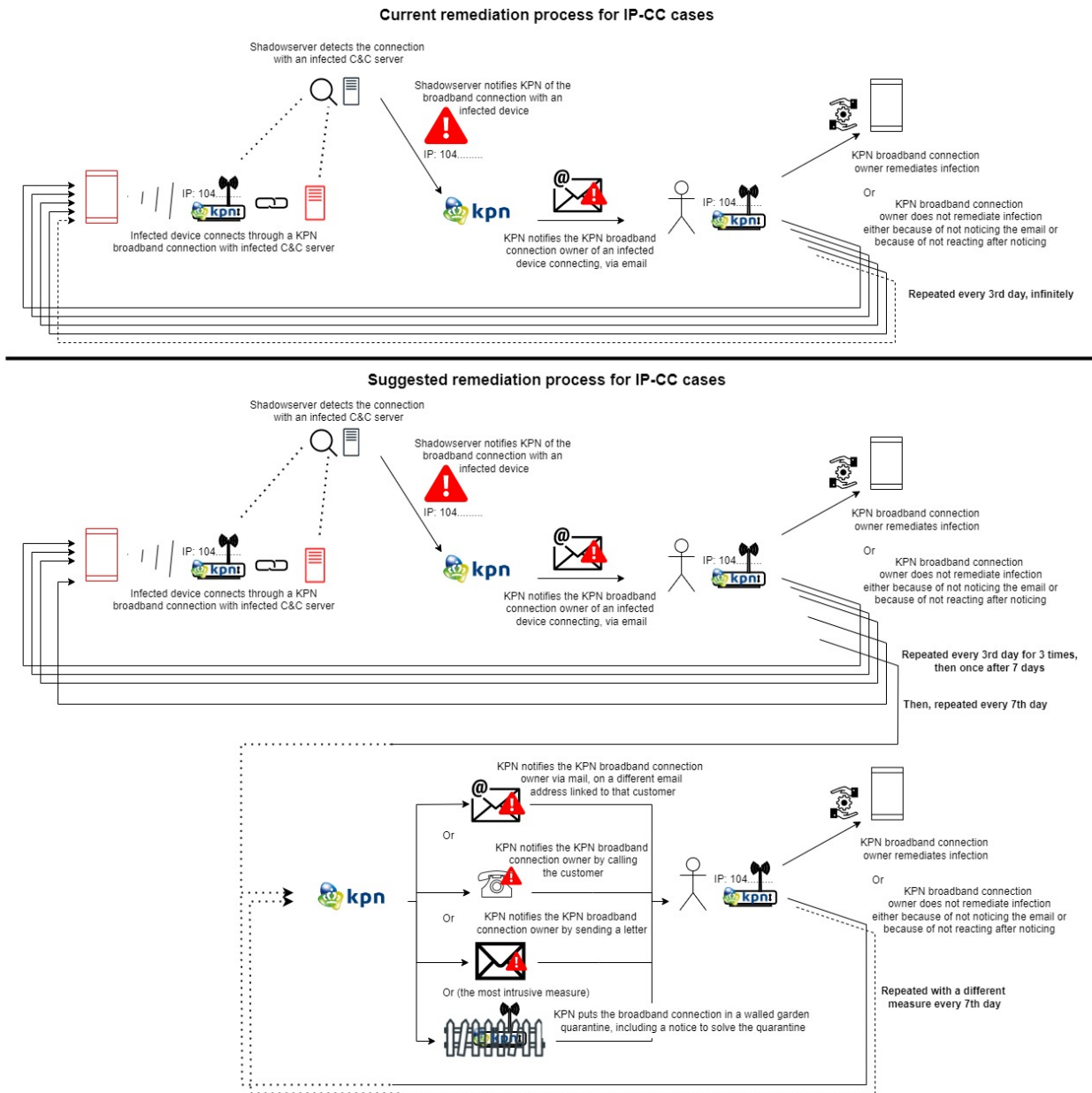


Figure 7.1: The current and recommended adaptive IP-CC notification process

The notification The notification sent by KPN due to the IP-CC detection and notification system, does mention the most important aspects, i.e. that an infection has been detected and that the end-user should make a back-up of their data before performing a factory reset. However, three important aspects are missing. The first aspect, that is missing in the notification, is a guideline for suspected victims to determine whether an infection occurred on an Android smartphone. By adding an instruction that combines the different guidelines from several accessible sources, the end-user should be better equipped for determining which Android smartphone might be infected. This is especially applicable to cases that have been detected by the IP-CC method. The added instruction should include three signs to look for on the Android smartphone. It should be noted, that, especially, the first two signs do not conclusively mean that the smartphone has been infected by Flubot. These signs should rather be considered as possible indicators that help with determining which smartphone is infected. An example of the instruction is:

"These are signs that an application may be Flubot malware:

- if your Android smartphone has a Voicemail application with a blue cassette in a yellow envelope as its logo. Also check for delivery service apps, like FedEx or DHL.
- if you tap an app, and it does not open.

- if you try to uninstall an app, and are instead shown an error message.

The first two signs, separately, do not automatically mean that the application is Flubot malware."

The second aspect, that should be included in the notification, is the cause of the Flubot infection. Two sentences about the end-user having clicked on a link inside a SMS text and having downloaded an application that contains malware, would be sufficient. This could help with determining which phone was infected. By informing the victims of the cause of the infection, they are also better equipped to prevent future infections and they might warn others, which is needed. Flubot, and similar malware, is still unknown to a large number of end-users, or at least potential victims. An example is:

"The infection was caused by clicking on a URL link inside a SMS text and downloading an application from outside the Google App Store. The SMS text might have seemed to be from UPS, DHL, Acrobat Reader, or another service."

The third aspect is about the usage of safe or flight mode and the potential risks of (not remediating) the infection. This might help the end-user with determining whether any harm has been experienced, and possibly persuade the end-user to take action sooner. Furthermore, by putting the smartphone in flight or safe mode, the malware cannot spread further and no additional data will get stolen, providing the end-user with time to make an informed decision and, possibly, perform a data back-up. An example of this addition is:

"The Flubot malware can gain access to your financial applications and send SMS texts without it being observable to you, possibly, leading to financial harm. By putting your Android smartphone in safe and flight mode, the malware cannot send anymore SMS texts and no additional (financial) data can be stolen, giving you some time to remediate the Flubot infection."

The additional information web page The information included on the web page, that can be accessed with the link inside the email notification sent by KPN, should offer both crucial and non-crucial information on the Flubot infection at hand. This includes the first aspect mentioned regarding the notification additions, as the web page should provide all needed information for the remediation. Furthermore, to improve the remediation process and lessen the impact of smishing-based malware infections in the short and long term, the web page should provide help with how to best cope with the infection. The additional information should address what to do when having experienced economical loss as a result of the infection or what to do when having experienced psychological harm. The likelihood of the victim becoming insecure about how they use their phone, will decrease if they can properly address the issue and any possible consequences. A short and simple addition providing some links for additional support, improves the resilience of the end-users and networks. The correlations between types of harm have shown that it is likely to experience different types at the same time, therefore it is important to include links that cover financial, psychological, data, societal and reputational harm. The latter two types of harm have less of an impact and are therefore the least important to include.

KPN Veilig Currently, KPN Veilig (i.e. the application KPN recommends to improve the cybersecurity of smartphone users) does not include a function to perform SMS filtering. KPN cannot perform SMS filtering on the SMS traffic, therefore including it in the KPN Veilig applications is of added value. If incorporating SMS filtering in KPN Veilig is deemed too costly, external applications that perform this function should be suggested to customers for improving their cybersecurity and lowering the impact of smishing-based malware.

7.10 Future research

Das et al. found that people with low-to-medium security behavioural intention are most likely to be triggered through social triggers [24]. Incentivising people to share their security behaviours in their social environments should, according to Das et al. findings, trigger further sharing of security behaviours. By providing a platform or environment for end-users, the sharing of security behaviour might get a kick-start. This could lead to a cycle of end-users noticing someone in their environment mentioning certain security behaviour, then doing it themselves and then sharing their security behaviour. This could lead to a self-sustaining cycle that most likely would need some readjusting and monitoring to make sure no incorrect security behaviour would become popular. Creating an environment where end-users can share their security behaviour and read about others' security behaviour, ideally, inside or in combination with an already existing and popular environment, such as social media or other media platform, might lead to the self-sustaining cycle of security behaviour improvements. Research on the feasibility and effectiveness of including or creating such a social security environment, should provide an insight into the possibilities of using social triggers and social environments for the improvement of

cybersecurity. This could potentially improve the security behaviours of end-users that tend to be reached the least, improving overall cybersecurity, not just regarding smishing-based malware.

By including other telecom providers in the Netherlands, findings can be made based on the larger telecom industry instead of just this specific telecom provider, creating a more encompassing smishing-based malware landscape inside, and possibly outside, the Netherlands.

The second knowledge gap, identified in Subchapter 3.2, regarding the influence of technical skill and profession on the remediation process ought to be looked into further. Enlarging the scope to not just technical skill and profession but also Security Behavior Intention would provide a more comprehensive understanding of the impact of Flubot on different groups, providing a better understanding on how to appropriately notify and support these different groups. Furthermore, a direct correlation between these factors and the remediation would contribute to the remaining knowledge gap surrounding this topic.

The research is based on the IP-CC detection and notification system, however that is just part of the whole Flubot landscape. Researching the SMS auto block detection system more in-depth and using the end-users that are detected through that system creates a more complete picture of how Flubot impacts end-users in the ever-adapting environment. The SMS auto block group is impacted more heavily by the measures as they lose all network connections with their telecom provider, meaning their phone essentially only connects through WiFi and nothing more. Compared to the IP-CC cases, this group generally does notice the infection. It is useful to determine whether this group experiences more harm because of the large volume of texts sent or less harm because, once the phone gets blocked, no further harm can be done. Furthermore, researching the SMS auto block group provides information on how to best notify and support this group.

By analysing and including the end-users that saw a smishing text and handled effectively to avoid harm, the understanding of end-users in the smishing-based malware landscape can be improved. Further expanding the target groups, by researching and analysing the overall smartphone user population would create a baseline of what is normal in security behaviour regarding smishing and what sets secure end-users apart from smishing victims. These insights would make it possible to create more effective, possibly targeted, information campaigns and further improve the information provided in any notifications.

To improve the efficiency of email notification systems, it is useful to determine at which notification it is statistically useless to keep sending new ones. This would lower email traffic and energy needed to keep sending notifications, whilst maintaining the effectiveness of the email notification system. This insight could be used for notification systems for other types of malware as well, not just Flubot or smishing-based malware. Research has been performed on which email contacts and messages work best for alerting domains of an issue [95]. However, no such research has been conducted in the field of end-user remediation for smartphone malware. This could potentially improve remediation processes for other malware too. The findings can then be incorporated in the improvement of the adaptive notification system described in the previous subchapter.

In the context of smishing-based malware and the remediation thereof, future research on adaptive SMS auto blocking could potentially be very useful, by researching the appropriate limits for thresholds and what kind of factors might influence the threshold (e.g. what the influence is of texts being sent in batches, texts being the same length, there being a pattern in sending the texts, and the time of day the texts are sent). This could provide essential information on how to curb other smishing-based malware and improve the detection and remediation of the malware, based solely on SMS traffic.

Bibliography

- [1] Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *OUP Journal of Cybersecurity*. <http://kar.kent.ac.uk/69076/>
- [2] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3. <https://doi.org/10.3389/fcomp.2021.563060>
- [3] Amin, A., ul Haq, I., & Nazir, M. (2017). International journal of computer science and mobile computing two factor authentication. *International Journal of Computer Science and Mobile Computing*, 6, 5–8. <https://www.ijscmc.com/docs/papers/July2017/V6I7201707.pdf>
- [4] Anderson, R., Barton, C., Boehme, R., Clayton, R., Ganan, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019). Measuring the changing cost of cybercrime. *The 18th Annual Workshop on the Economics of Information Security*. <https://doi.org/10.17863/CAM.41598>
- [5] Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. *The Economics of Information Security and Privacy*, 265–300. https://doi.org/10.1007/978-3-642-39498-0_12/TABLES/1
- [6] AppAnnie. (2021). *State of mobile 2021*. <https://www.data.ai/en/go/state-of-mobile-2021/>
- [7] Atanassov, N., & Chowdhury, M. (2021). Mobile device threat: Malware. *2021 IEEE International Conference on Electro Information Technology (EIT)*, 007–013. <https://doi.org/10.1109/EIT51626.2021.9491845>
- [8] Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, 23, 4–17. <https://doi.org/10.1016/J.INTCOM.2010.07.003>
- [9] Bitdefender. (2022). *New flubot and teabot global malware campaigns discovered*. <https://www.bitdefender.com/blog/labs/new-flubot-and-teabot-global-malware-campaigns-discovered>
- [10] Bosamia, M., Patel, D., Chandaben, S., & Patel, M. (2019). Wallet payments recent potential threats and vulnerabilities with its possible security measures. *International Journal of Computer Sciences and Engineering Open Access Review Paper*. <https://doi.org/10.26438/ijcse/v7i1.810817>
- [11] Bouwmeester, A. ; Rodriguez, B. T., Gañán, E. R., Eeten, C. ; V., & Parkin, M. ; (2021). "the thing doesn't have a name" learning from emergent real-world interventions in smart home security (SOUPS 2021), 493–512. www.usenix.org/conference/soups2021/presentation/bouwmeester
- [12] Bowen, M. (2017). *Mobile malware: Introducing a new era of cyber threats - intelligent cio middle east*. <https://www.intelligentcio.com/me/2017/12/18/mobile-malware-introducing-a-new-era-of-cyber-threats/#>
- [13] Bubukayr, M. A. S., & Almaiah, M. A. (2021). Cybersecurity concerns in smart-phones and applications: A survey. *2021 International Conference on Information Technology (ICIT)*, 725–731. <https://doi.org/10.1109/ICIT52682.2021.9491691>
- [14] centraal bureau statistiek. (2021). *Households today*. <https://www.cbs.nl/en-gb/visualisations/dashboard-population/households/households-today>
- [15] Cetin, O., Ganan, C., Altena, L., Kasama, T., Inoue, D., Tamiya, K., Tie, Y., Yoshioka, K., & van Eeten, M. (2019). Cleaning up the internet of evil things: Real-world evidence on isp and consumer efforts to remove mirai. *Proceedings 2019 Network and Distributed System Security Symposium*. <https://doi.org/10.14722/ndss.2019.23438>
- [16] Chawdhry, M. (2022). *What is flubot malware? how to detect, remove, and prevent it*. <https://vpnoverview.com/internet-safety/malware/flubot/>
- [17] Childers, D. (2021). *State of the auth experiences and perceptions of multi-factor authentication*. Cisco Systems, Inc. <https://duo.com/assets/ebooks/state-of-the-auth-2021.pdf>
- [18] Chorghé, S. P., & Shekoker, N. (2016). A survey on anti-phishing techniques in mobile phones. *2016 International Conference on Inventive Computation Technologies (ICICT)*, 1–5. <https://doi.org/10.1109/INVENTIVE.2016.7824819>

- [19] Choudhury, R., Luo, Z., & Nguyen, K. A. (2022). Malware in motion (G. Balint, B. Antala, C. Carty, J.-M. A. Mabieme, I. B. Amar, & A. Kaplanova, Eds.). *Uniwersytet śląski*, 85. <https://doi.org/10.2/JQUERY.MIN.JS>
- [20] Choueiry, G. (n.d.). *Statistical software popularity in 40,582 research papers*. <https://quantifyinghealth.com/statistical-software-popularity-in-research/>
- [21] cleafy labs. (2021a). *Oscorp evolves into ubel: An android malware spreading across the globe*. <https://www.cleafy.com/cleafy-labs/ubel-oscosp-evolution>
- [22] cleafy labs. (2021b). *Teabot, a new android malware targeting banks in europe*. <https://www.cleafy.com/cleafy-labs/teabot>
- [23] Crahmaliuc, R. (2021). *What is flubot and why you need to start taking it seriously right now*. <https://www.bitdefender.com/blog/hotforsecurity/what-is-flubot-and-why-you-need-to-start-taking-it-seriously-right-now/>
- [24] Das, S., Dabbish, L. A., & Hong, J. I. (2019). A typology of perceived triggers for end-user security and privacy behaviors. *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*. <https://www.usenix.org/conference/soups2019/presentation/das>
- [25] Das, S., Kim, T. H.-J., Dabbish, L. A., & Hong, J. I. (2014). The effect of social influence on security sensitivity. *USENIX Association Tenth Symposium On Usable Privacy and Security 143 The Effect of Social Influence on Security Sensitivity*. <https://www.usenix.org/system/files/conference/soups2014/soups14-paper-das.pdf>
- [26] department of homeland security. (2012). *The menlo report: Ethical principles guiding information and communication technology research*. Directorate of Science and Technology. https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf
- [27] Dies, J. (2021). *A rapid rise in global parcel volumes shows no signs of slowing*. ParcelIndustry.com. Pitney Bowes Sending Technology Solutions. <https://www.pitneybowes.com/us/shipping-index.html>
- [28] Eshmawi, A., & Nair, S. (2019). The roving proxy framewrok for sms spam and phishing detection. *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019*. <https://doi.org/10.1109/CAIS.2019.8769562>
- [29] Europol. (2022a). *Joint cybercrime action taskforce (j-cat): Fighting cybercrime around the world*. <https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce>
- [30] Europol. (2022b). *Takedown of sms-based flubot spyware infecting android phones | europol*. <https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones>
- [31] Fagan, M., Maifi, M., & Khan, H. (2016). Why do they do what they do?: A study of what motivates users to (not) follow computer security advice why do they do what they do? a study of what motivates users to (not) follow computer security advice. *e Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*., 59. <https://www.usenix.org/conference/soups2016/technical-sessions/presentation/fagan>
- [32] Fogg, B. (2009). A behavior model for persuasive design. *ACM International Conference Proceeding Series*, 350. <https://doi.org/10.1145/1541948.1541999>
- [33] Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L. F., Egelman, S., Harbach, M., & Telang, R. (2016). Do or do not, there is no try: User engagement may not improve security outcomes. *Proceedings of the Twelfth Symposium on Usable Privacy and Security*. <https://www.usenix.org/conference/soups2016/technical-sessions/presentation/forget>
- [34] FraudWatch. (n.d.). *Flubot malware: How it spreads and how to remove it*. <https://fraudwatch.com/flubot-malware-how-it-spreads-and-how-to-remove-it/>
- [35] Fruchter, N. H. (2019). *Enhancing isp-consumer security notifications*. MASSACHUSETTS INSTITUTE OF TECHNOLOGY. <https://dspace.mit.edu/bitstream/handle/1721.1/122916/1126790910-MIT.pdf?sequence=1&isAllowed=y>
- [36] Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers Security*, 73, 519–544. <https://doi.org/10.1016/j.cose.2017.12.006>
- [37] Gruber, A., & Ségur-Cabanac, N. (2021). Necessary or premature? the nis 2 directive from the perspective of the telecommunications sector. *International Cybersecurity Law Review 2021 2:2*, 2, 233–243. <https://doi.org/10.1365/S43439-021-00035-6>
- [38] Hartholt, S. (2017). *Kamer akkoord met briefgeheim e-mail en sms*. <https://www.binnenlandsbestuur.nl/digitaal/kamer-akkoord-met-briefgeheim-e-mail-en-sms>

- [39] Herald, N. (2022). *Flubot: Nasty phone virus sends spam messages that can cost you thousands - nz herald*. <https://www.nzherald.co.nz/business/flubot-nasty-phone-virus-sends-spam-messages-that-can-cost-you-thousands/63SINI7ODSIZLKFEGUTMMZZLVA/>
- [40] Herley, C. (2014). More is not the answer. *IEEE Security and Privacy*, 12, 14–19. <https://doi.org/10.1109/MSP.2013.134>
- [41] Hoeffnagel, W. (2021). *Politie waarschuwt voor android-malware verstoep in track and trace-apps*. <https://dutchitchannel.nl/674090/android-malware-verstoep-in-track-and-trace-apps-maakt-slachtoffers-in-nederland.html>
- [42] Howler, L. (2021). *Ubel – the successor of oscorp android credential stealing malware*. <https://howtoremove.guide/ubel-oscorp-android-malware/>
- [43] Jakobsson, M. (2018). Two-factor inauthentication – the rise in sms phishing attacks. *Computer Fraud Security*, 2018. [https://doi.org/10.1016/S1361-3723\(18\)30052-6](https://doi.org/10.1016/S1361-3723(18)30052-6)
- [44] Jean, E. (2021). *How to check if you're infected by flubot; ways to remove and prevent malware*. <https://www.itechpost.com/articles/107235/20211005/check-youre-infected-flubot-x-ways-remove-prevent-malware.htm>
- [45] Jones, W. S. (2021). *Choose your own compromise: Attackers use similar lures to deliver both smishing and malware attacks | proofpoint us*. <https://www.proofpoint.com/us/blog/email-and-cloud-threats/choose-your-own-compromise-attackers-use-similar-lures-deliver-both>
- [46] Jörgensson, A. (2018). *Bachelor's programme in it-forensics and information security, 180 credits malware in mobile devices*. Halmstad University. <http://hh.diva-portal.org/smash/get/diva2:1248547/FULLTEXT01.pdf>
- [47] Kadir, A. F. A., Stakhanova, N., & Ghorbani, A. A. (2018). Understanding android financial malware attacks: taxonomy, characterization, and challenges. *Journal of Cyber Security and Mobility*, 7, 1–52. <https://doi.org/10.13052/jcsm2245-1439.732>
- [48] Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *The Economic Society*, 47. <http://www.jstor.org/stable/1914185>
- [49] Kemp, S. (2021). *Digital 2021: Global overview report*. Datareportal. <https://datareportal.com/reports/digital-2021-global-overview-report>
- [50] KPN. (2021). *Kpn integrated annual report 2021: Connecting everyone in the netherlands to a sustainable future contents contents*. <https://annualreport2021.kpn/>
- [51] kpn forum blog. (2022). *Flubot malware blokkade na het versturen van veel sms'jes. let op: Sms-verbruik hoger dan normaal*. <https://forum.kpn.com/mobiel-15/flubot-malware-blokkade-na-het-versturen-van-veel-sms-jes-let-op-sms-verbruik-hoger-dan-normaal-556707>
- [52] kpn phone abuse department (employee). (2022).
- [53] Kshetri, N., & Sharma, A. (2021). A review and analysis of online crime in pre and post covid scenario with respective counter measures and security strategies. *Journal of engineering, computing architecture*, 11, 13–33. <http://www.journaleca.com/>
- [54] Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems*, 46, 254–264. <https://doi.org/10.1016/J.DSS.2008.06.010>
- [55] Laudon, M. (2020). *Security brief: Mobile phishing increases more than 300 per cent as 2020 chaos continues*. <https://www.proofpoint.com/us/blog/threat-protection/mobile-phishing-increases-more-300-2020-chaos-continues>
- [56] McAfee. (2019). *The cerberus banking trojan: 3 tips to secure your financial data*. <https://www.mcafee.com/blogs/privacy-identity-protection/cerberus-banking-trojan/>
- [57] McKinsey. (2020). *Covid-19 digital transformation technology*. McKinsey Company. <https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever>
- [58] Merriam-Webster. (n.d.). *Malware definition meaning*. <https://www.merriam-webster.com/dictionary/malware>
- [59] Meskauskas, T. (2022a). *Anatsa trojan (android) - malware removal instructions (updated)*. <https://www.pcrisk.com/removal-guides/23778-anatsa-trojan-android>
- [60] Meskauskas, T. (2022b). *Ermac 2.0 trojan (android) - malware removal instructions (updated)*. <https://www.pcrisk.com/removal-guides/23920-ermac-20-trojan-android>
- [61] Meskauskas, T. (2022c). *Smscontrollo malware (android) - malware removal instructions*. <https://www.pcrisk.com/removal-guides/23607-smscontrollo-malware-android>
- [62] Meskauskas, T. (2022d). *Flubot malware (android) - malware removal instructions (updated)*. <https://www.pcrisk.com/removal-guides/20475-flubot-malware-android>

- [63] Morgan, S. (2020). *Cybercrime to cost the world \$10.5 trillion annually by 2025*. <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
- [64] national cyber security center (employee). (2022).
- [65] Newcombe, G. (2021). *Commissioner's blog: Don't get infected by flubot*. <https://www.commerce.wa.gov.au/announcements/commissioners-blog-dont-get-infected-flubot>
- [66] Nicholson, J., Coventry, L., & Briggs, P. (2019). "if it's important it will be a headline": Cybersecurity information seeking in older adults. *CHI*. <https://doi.org/10.1145/3290605.3300579>
- [67] Nicholson, J., Morrison, B., Dixon, M., Holt, J., Coventry, L., & McGlasson, J. (2021). Training and embedding cybersecurity guardians in older communities. *Association for Computing Machinery*, 86. <https://doi.org/10.1145/3411764.3445078>
- [68] Nizar, D., & Moshailov, R. (2022). *Flubot's authors employ creative and sophisticated techniques to achieve their goals in version 5.0 and beyond | f5 labs*. <https://www.f5.com/labs/articles/threat-intelligence/flubots-authors-employ-creative-and-sophisticated-techniques-to-achieve-their-goals-in-version-50-and-beyond>
- [69] Norton. (2021). *2021 norton cyber safety insights report global results*. NortonLifeLock Inc.
- [70] Paganini, P. (2022). *Flubot malware continues to evolve. what's new in ver 5.0 and beyond?* <https://securityaffairs.co/wordpress/126451/malware/flubot-ver-5-0-improvements.html>
- [71] Parkin, S. (2022).
- [72] Parkin, S., Redmiles, E. M., Coventry, L., & Sasse, M. A. (2019). Security when it is welcome: Exploring device purchase as an opportune moment for security behavior change. <https://doi.org/10.14722/usec.2019.23024>
- [73] parlementaire monitor. (n.d.). *Onschendbaarheid brief-, telefoon- en telegraafgeheim*. <https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vkfmwfhkpixv>
- [74] Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. *IFIP Advances in Information and Communication Technology*, 405, 366–378. https://doi.org/10.1007/978-3-642-39218-4_27/COVER
- [75] Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2016). The information security awareness of bank employees. *Proceedings of the Tenth International Symposium on Human Aspects of Information Security Assurance (HAISA 2016)*. <https://www.semanticscholar.org/paper/The-Information-Security-Awareness-of-Bank-Pattinson-Butavicius/ac9cbe032650de41d33a6fd9eb2d5f2f4045d4a4>
- [76] Politie. (2022). *Politie stopt internationaal verspreiding flubot malware | politie.nl*. <https://www.politie.nl/nieuws/2022/juni/1/02-politie-stopt-internationaal-verspreiding-flubot-malware.html>
- [77] Potter, K. (2018). Increased use of two-factor authentication force new social engineering tactics. *Utica CollegeProQuest Dissertations Publishing*. <http://160.75.22.2/dissertations-theses/increased-use-two-factor-authentication-force-new/docview/2037183631/se-2?accountid=11638>
- [78] Proofpoint. (2020). *State of the phish: An in-depth look at user awareness, vulnerability and resilience*. proofpoint.com.
- [79] Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy amp; future directions. *Future Generation Computer Systems*, 97, 887–909. <https://doi.org/10.1016/j.future.2019.03.007>
- [80] Radicati, S. (2018). *Email statistics report, 2014-2018*. THE RADICATI GROUP, INC. <http://www.radicati.comhttp://www.radicati.com>
- [81] Ralston, N. (2021). *Flubot threat bulletin – allot blocks over 140m cc connection attempts - security boulevard*. <https://securityboulevard.com/2021/05/flubot-threat-bulletin-allot-blocks-100m-cc-connection-attempts/>
- [82] redactie beleef knp. (2021). *Pas op voor flubot malware*. <https://www.knp.com/beleef/blog/flubot-malware-android.htm>
- [83] Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue: 11. <https://doi.org/10.1177/21582440211000049>
- [84] Rijksoverheid. (n.d.). *Aow-leeftijd stijgt minder snel*. <https://www.rijksoverheid.nl/onderwerpen/pensioen/toekomst-pensioenstelsel/aow-leeftijd-stijgt-minder-snel>
- [85] risk frontiers. (2018). *Fs-isac 2018 cybersecurity trends*. <https://riskfrontiers.com/insights/fs-isac-2018-cybersecurity-trends/>
- [86] Rodríguez, E., Fukkink, M., Parkin, S., Eeten, M. V., & Gañán, C. (2022). Difficult for thee, but not for me: Measuring the difficulty and user experience of remediating persistent iot malware. <https://doi.org/10.1109/EuroSP53844.2022.00032>
- [87] Ruik. (2021). *Anatsa android malware uses fake delivery notifications to infect victims*. <https://www.cyclonis.com/anatsa-android-malware-uses-fake-delivery-notifications-to-infect-victims/>

- [88] Schless, H. (2021). *Flubot: Malware as a service meets mobile phishing*. <https://resources.lookout.com/blog/flubot-malware-as-a-service-meets-mobile-phishing>
- [89] Segura, A., & Govers, R. (2022). *Flubot: The evolution of a notorious android banking malware – fox-it international blog*. <https://blog.fox-it.com/2022/06/29/flubot-the-evolution-of-a-notorious-android-banking-malware/amp/>
- [90] Siadati, H., Nguyen, T., Gupta, P., Jakobsson, M., & Memon, N. (2017). Mind your smses: Mitigating social engineering in second factor authentication. *Computers Security*, 65. <https://doi.org/10.1016/j.cose.2016.09.009>
- [91] Sikder, R., Khan, S., Hossain, S., & Khan, W. Z. (2020). A survey on android security: Development and deployment hindrance and best practices reliable wireless sensing and internet of things based monitoring and surveillance in oil and gas fields view project. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, 18, 485–499. <https://doi.org/10.12928/TELKOMNIKA.v18i1.13288>
- [92] Speelman, S. (2021). *Acm: Parcel delivery market grows even faster as a result of the pandemic | acm.nl*. <https://www.acm.nl/en/publications/acm-parcel-delivery-market-grows-even-faster-result-pandemic>
- [93] Statcounter. (2022a). *Mobile operating system market share netherlands | statcounter global stats*. <https://gs.statcounter.com/os-market-share/mobile/netherlands>
- [94] Statcounter. (2022b). *Mobile operating system market share worldwide | statcounter global stats*. <https://gs.statcounter.com/os-market-share/mobile/worldwide>
- [95] Stock, B., Pellegrino, G., Li, F., Backes, M., & Rossow, C. (2018). Didn't you hear me?-towards more successful web vulnerability notifications. *Network and Distributed Systems Security (NDSS) Symposium 2018*. <https://doi.org/10.14722/ndss.2018.23171>
- [96] Tavares, A. (2022). *Flubot malware persists: Most prevalent in germany and spain*. <https://www.bitsight.com/blog/flubot-malware-persists-most-prevalent-germany-and-spain>
- [97] techtarget contributor. (n.d.). *What is command-and-control server (cc server)?* <https://www.techtarget.com/whatis/definition/command-and-control-server-CC-server>
- [98] Telecompaper. (2021). *Kpn waarschuwt voor smishingmalware flubot*. <https://www.telecompaper.com/news/kpn-waarschuwt-voor-smishingmalware-flubot--1384249>
- [99] Teunissen, R. (2022).
- [100] the shadowserver foundation. (n.d.). *What we do*. <https://www.shadowserver.org/what-we-do/>
- [101] Toulas, B. (2021). *Anubis android malware returns to target 394 financial apps*. <https://www.bleepingcomputer.com/news/security/anubis-android-malware-returns-to-target-394-financial-apps/>
- [102] Toxboe, A. (2019). *Making the fogg behavior model actionable*. <https://ui-patterns.com/blog/making-the-fogg-behavior-model-actionable>
- [103] Truta, F. (2022). *Rejuvenated flubot campaign moves to finland; iphone users also targeted*. <https://www.bitdefender.com/blog/hotforsecurity/rejuvenated-flubot-campaign-moves-to-finland-iphone-users-also-targeted-2/>
- [104] Tuli, S. (2020). *Developing an accessibility service for android*. <https://codelabs.developers.google.com/codelabs/developing-android-a11y-service#0>
- [105] Varadaraj, V. (2021). *Beware of brata: How to avoid android malware attack*. <https://www.mcafee.com/blogs/mobile-security/beware-of-brata-how-to-avoid-android-malware-attack/>
- [106] Veiliginternetten.nl. (2021). *Flubot - een sms-bericht dat malware plaatst op je (android) smartphone*. <https://veiliginternetten.nl/nieuws/flubot/>
- [107] Wash, R., Nthala, N., & Rader, E. (2021). Knowledge and capabilities that non-expert users bring to phishing detection. *Proceedings of the Seventeenth Symposium on Usable Privacy and Security*. www.usenix.org/conference/soups2021/presentation/wash
- [108] Wash, R., & Rader, E. (2015). Too much knowledge? security beliefs and protective behaviors among united states internet users. *Symposium on Usable Privacy and Security (SOUPS) 2015*. <https://bitlab.cas.msu.edu/papers/security-survey.pdf>
- [109] Yao, M.-L., Chuang, M.-C., & Hsu, C.-C. (2018). Research on the user attitudes and behaviors of mobile security and antivirus. *International Journal of Liberal Arts and Social Science*, 6. www.ijlass.org
- [110] Yeboah-Boateng, E. O., & Boaten, F. E. (2016). Bring-your-own-device (byod): An evaluation of associated risks to corporate information security. *International Serial Directories International Journal in IT and Engineering*, 4. <https://doi.org/10.48550/arxiv.1609.01821>
- [111] Zettasphere. (n.d.). *The number of email addresses people use [survey data]*. <https://www.zettasphere.com/how-many-email-addresses-people-typically-use/>

Appendix A

Notification of Flubot infection

The figures, including a translated summary.



Beste meneer Test Test,

Veilig internet is voor iedereen belangrijk. Daarom houden we samen onze internetverbindingen zo veilig mogelijk. We hebben hierbij uw hulp nodig, omdat we een veiligheidsprobleem hebben ontdekt op uw internetverbinding. Doorloop alstublieft de stappen hieronder vandaag nog.

Waarom moet ik iets doen?

We lossen de meeste veiligheidsproblemen op afstand op. Maar soms hebben we de hulp van onze klanten nodig. Het is voor u en andere klanten belangrijk dat u helpt, ook als u zelf niets merkt van het veiligheidsprobleem.

Wat is er aan de hand en hoe kan ik dit oplossen?

Een Android apparaat dat besmet is/was met FluBot-malware heeft uw internet- of wifiverbinding gebruikt. Waarschijnlijk gaat het om één van uw eigen telefoons of tablets. Maar het kan ook een Android toestel van een gast geweest zijn dat tijdelijk met uw wifi verbonden was.

1

Figure A.1: The notification customers receive when an infected smartphone has been detected to their KPN broadband connection, part 1

Safe internet is important for everyone. That is why we are trying to keep our internet connections as safe as possible together. We need your help for this, as we have detected a safety issue concerning your internet connection. Please, go through the steps below today.

Why should I do something? We solve most security problems remotely. But sometimes we need the help of our customers. It is important for you and other customers that you help, even if you don't notice the security problem yourself.

What's going on and how can I fix it? An android device infected with FluBot-malware has been using your internet- or WIFI connection. It is probably one of your own phones or tablets. But it could also have been a guest's Android device that was temporarily connected to your Wi-Fi.

Probeer te achterhalen welke Android toestellen er verbonden zijn (geweest) met uw internetverbinding. Breng eerst alle bestanden zoals foto's en contactgegevens in veiligheid. Zet daarna de toestellen terug naar de fabrieksinstellingen. Doe dit zo snel mogelijk. Kijk voor meer informatie op kpn.com/service/internet/veilig-internetten/gevaar-en-fraude.htm

Let op! Met het terugzetten naar de fabrieksinstellingen wist u alle gegevens op het toestel.

Wat gebeurt er als ik niets doe?

Als u de stappen niet of niet goed uitvoert, dan blokkeren wij tijdelijk uw internetverbinding. Dit doen we om uw persoonlijke gegevens te beschermen. Voer de stappen daarom vandaag nog uit. En bevestig dat u ze hebt uitgevoerd door een e-mail te sturen naar abuse@kpn.com.

De afdeling Abuse

De afdeling Abuse handelt veiligheidsincidenten af voor KPN.

Meer informatie

Hebt u nog vragen?

U kunt uw vragen stellen via e-mail op abuse@kpn.com.

Met vriendelijke groet,

KPN Abuse Team

Wat vindt u van deze e-mail?

[Heel goed](#)

[Kan beter](#)

Figure A.2: The notification customers receive when an infected smartphone has been detected to their KPN broadband connection, part 2

Try to find out which android devices have been connected to your internet connection. First, secure all files such as photos and contact information. Then reset the devices to the factory settings. Do this as soon as possible. For more information, see kpn.com/service/internet/veilig-internetten/danger-en-fraude.htm (Link of kpn.com concerning internet safety)

NB! Factory reset erases all data on the device.

What happens if I don't do anything? If you do not perform the steps or do not perform them correctly, we will temporarily block your internet connection. We do this to protect your personal information. Therefore, complete the steps today. And confirm that you have conducted them by sending an email to abuse@kpn.com.

The department Abuse resolves safety incidents for KPN. For more information contact through e-mail abuse@kpn.com.

With Kind Regards

KPN Abuse Team.

Appendix B

Notification on KPN forum to participate in interview

The figure, including a translated summary.


[Research] Have you received a false SMS text?

Have you received a suspicious text in the last six months, that included a link, and that you did not click on? Currently, a research is conducted regarding smishing (SMS-phishing) and Flubot. Flubot is a virus that spreads on Android smartphones. [A link with information on Flubot]

If you've had experienced with this malware, than you're kindly requested to participate in the research and answer some questions. Your information will be processed anonymously. If you want to participate, send me a private message, including your phone number.

30-06-2022 10:34 [Onderzoek] Heb jij wel eens een valse SMS gehad? | KPN Community

Aanbod Service MijnKPN

 Webmail

Naar Zakelijk


Zoeken...

Menu


< Online veiligheid


[Onderzoek] Heb jij wel eens een valse SMS gehad?

22 dagen geleden · 0 reacties



Valse sms: smishing



 Raymondt

Heb jij in het laatste halfjaar een (verdacht) sms bericht ontvangen waar een link in stond en waar je niet, om wat voor reden ook, op hebt gedrukt?

Op dit moment loopt een onderzoeker van de TU Delft stage bij mij. Hij doet onderzoek naar smishing (phishing via sms) en Flubot. Flubot is een virus voor Android telefoons die via sms binnenkomt. Meer over Flubot [lees je hier](#).

Mocht je hier persoonlijke ervaring mee hebben (waarbij het niet uitmaakt of je nu een mobiel abonnement hebt bij KPN, of bij een van de concullega's), dan zou mijn stagiair je graag wat vragen willen stellen voor zijn onderzoek (waarin de gegevens uiteraard anoniem verwerkt worden). Mocht je het leuk vinden om hieraan mee te werken, dan verzoek ik je mij [een privébericht te sturen](#) waarin je aangeeft hier aan mee te willen werken, en daarin je telefoonnummer vermeldt. We maken dan een afspraak over wanneer mijn stagiair je zou kunnen bellen om zijn vragen te stellen.

Je zou ons hier enorm mee helpen. Alvast bedankt!

<https://forum.kpn.com/online-veiligheid-25/onderzoek-heb-jij-wel-eens-een-valse-sms-gehad-566514> 1/3

Figure B.1: Notification in Dutch posted on KPN forum to participate in an interview on why end-users did not click the malicious link inside a suspicious text

Appendix C

Additional information provided by KPN on Flubot

The figure, including a translated summary.



Figure C.1: The additional information customers and potential victims are directed to, about Flubot and how it works

Internet crime and telephone fraud.

To be able to use the internet safely, it is important that you know what the risks are. You can also be confronted with fraud by telephone. Below you will find the most common and current risks.

A new type of malware is spreading for Android smartphones, called Flubot. An application is installed and it will send SMS texts from your phone. The SMS texts include a link and if someone clicks on those links, they might get infected too. You might experience some costs through KPN, or other installed applications.

Rest your phone to factory settings, the only way of remediating the infection. If you do not know how, use this link [A link is provided for smartphone help].

[Then an example of a Flubot text is shown]

Appendix D

Email notifications and the survey pre-participating notification

Figures, including a translated summary.

A reminder of a previous security problem that hasn't been resolved and is still present on one of the devices connected to the user's internet connection. In collaboration with the TU Delft research is conducted, to improve KPN's service and help contribute to scientific research. Within 5 working days, the researcher (Artur Geers) will contact the user and help resolve the issue and in addition would like to ask a few questions regarding the research. The research is anonymous and voluntary.

The user has received this e-mail, since their Android smartphones has dealt with security issues in the past six months. Therefore, we would like to invite you to complete a short survey, regarding your experience with Flubot infections and resolving these issues. By completing the survey, KPN can improve their service and help contribute to scientific research. The research is anonymous.

Thank you for participating in our research. We will ask you about your experiences and insights regarding the Flubot infection.

Participation is voluntary and with it we can help our customers better to remediate infections, like Flubot. You are contributing to scientific research regarding a safer and more accessible virtual environment. Your answers will stay anonymous and are not coupled to your email or other customer information. The answers, after anonymising, will be published. You're free to leave at any moment. And if you have any question, you can pose them to [provided email].

Geers, Artur

Van: KPN Abuseteam <abuse@kpn.com>
Verzonden: vrijdag 17 juni 2022 15:29
Aan: Geers, Artur
Onderwerp: Onderzoek online veiligheid



Onderzoek online veiligheid

Geachte **heer/mevrouw**,

U ontvangt deze e-mail omdat wij u onlangs hebben geïnformeerd over een beveiligingsprobleem op een van de apparaten op uw internetverbinding. Uit de meldingen die we zien blijkt dat het probleem nog steeds aanwezig is.

In samenwerking met de TU Delft voeren wij momenteel een onderzoek uit naar mensen die besmet zijn (geweest) met dit specifieke virus. Door onderzoek te doen kan KPN haar dienstverlening naar klanten verbeteren, en dragen we bij aan wetenschappelijk onderzoek.

Binnen 5 werkdagen zal de onderzoeker in kwestie (Artur Geers) telefonisch contact met u opnemen om u te helpen het probleem op te lossen, en zou hij u graag voor het onderzoek een aantal vragen willen stellen. Het staat u uiteraard vrij om aan te geven dat u hieraan geen medewerking wenst te verlenen.

Deelname aan het onderzoek is anoniem. De antwoorden op de vragen die opgeslagen worden, worden niet gekoppeld aan uw naam, e-mailadres of andere persoonsgegevens. Mocht u hierover nog verdere vragen hebben, dan kunt u dit aan de onderzoeker kenbaar maken, of ons hierover een e-mail sturen. U kunt per e-mail contact opnemen met de onderzoeker.

De afdeling Abuse

De afdeling Abuse van KPN handelt veiligheidsincidenten af voor KPN.

Meer informatie

Hebt u nog vragen?

U kunt contact opnemen met de hoofdonderzoeker via: artur.geers@kpn.com of met de KPN AbuseDesk, via: abuse@kpn.com

Figure D.1: The email that was sent to, still active, cases to participate in the interview, regarding being contacted by telephone by KPN, i.e. the researcher

Geers, Artur

Van: KPN Abuse team <abuse@kpn.com>
Verzonden: maandag 13 juni 2022 13:49
Aan: Geers, Artur
Onderwerp: Onderzoek online veiligheid

You don't often get email from abuse@kpn.com. [Learn why this is important](#)



Onderzoek online veiligheid

Geachte **heer/mevrouw**,

U ontvangt deze mail omdat u recentelijk, in de laatste zes maanden, een beveiligingsprobleem heeft gehad met een van uw internet verbonden android smartphones. In het kader van een onderzoek naar de ervaring van Flubot infecties en het verhelpen ervan, willen wij u uitnodigen om een korte enquête in te vullen. Dit duurt ongeveer 5 minuten.

U kunt de enquête vinden via de onderstaande link:

<https://www.kpn.com/tu-delft-onderzoek>

Met uw antwoorden kan KPN haar dienstverlening beter laten aansluiten op de wensen van haar klanten, en draagt u bij aan wetenschappelijk onderzoek. Uw deelname is anoniem; uw antwoorden zijn niet gekoppeld aan een emailadres of andere klantgegevens.

De afdeling Abuse

De afdeling Abuse van KPN handelt veiligheidsincidenten af voor KPN.

Meer informatie

Hebt u nog vragen?

U kunt contact opnemen met de hoofdonderzoeker via: artur.geers@kpn.com of met de KPN AbuseDesk, via: abuse@kpn.com

Figure D.2: The email older cases were sent to participate in the survey

24-08-2022 15:46

TUDelft Onderzoek

TUDelft Onderzoek

Bedankt voor het willen meewerken aan ons onderzoek wat in samenwerking met de TU Delft uitgevoerd wordt. We vragen om uw ervaringen en inzichten over de Flubot infectie.

Deelname is vrijwillig en met uw deelname kunnen wij onze klanten beter helpen met infecties, zoals Flubot, en draagt u bij aan wetenschappelijk onderzoek naar een veiligere en toegankelijke virtuele omgeving. Uw antwoorden blijven anoniem en zijn niet gekoppeld aan een emailadres of andere klantgegevens. De resultaten afkomstig van de geanonimiseerde antwoorden zullen gepubliceerd worden.

Indien u nog vragen heeft, kunt u contact opnemen met de hoofdonderzoeker via: artur.geers@kpn.com of met de KPN AbuseDesk, via: abuse@kpn.com.

Naar het onderzoek

Mobiele telefoons	▼
Internet en TV	▼
KPN Hussel	▼
Service & Contact	▼
MijnKPN	▼
Over ons	▼

[Alle voorwaarden](#) |
 [Missie en privacy statement](#) |
 [Security](#) |
 [Report Vulnerability](#) |
 [Beveiligingslek melden](#) |
 [Over KPN](#)

<https://www.kpn.com/service/Internet/veilig-Internetten/abuse/tudelft-onderzoek.htm>

1/2

Figure D.3: The notification older cases were shown before participating in the survey

Appendix E

Set of (follow-up) questions for the semi-structured interview

Figures, including a translated summary.

Interview by Artur Geers on behalf of KPN.

A week and a half ago you received an email from KPN about a virus infection in your android phone. The e-mail stated that we would contact you and that is why I called you.

First to check, is it correct that the email address is yours? It is the e-mail address registered with KPN and linked to this number.

- If yes; that's great, are you available for this call to solve the problem and at the same time answer a number of questions for me for a study that is being conducted by me in collaboration with KPN and TU Delft?

o If no: when can you be reached to call you back?

o I would like to thank you for your time and I will call you back on

- If no; Is the person available that this email address and number belongs to?

o If no: when can you be reached to call you back?

o I would like to thank you for your time and I will call you back on

Did you receive the email?

- If no; I can send the e-mail to a different email address, can you read it now? At KPN we notice that these types of infections can take a long time, as stated in the mail we send you, we have tried to warn regularly but according to our system nothing has changed. I call you to solve the infection, to improve your cyber security and to conduct research on how customers respond and experiencing the current process of resolving mobile infections, Flubot in this case. The interview will be recorded and transcribed as part of the research. Before the examination, in addition to Flubot related questions, I will also ask a number of questions about yourself. The conversation will be stored anonymously and to be examined later, no personal data will be used, so the answers will not be traceable. The results of the study will be published later, and the conversations will be deleted one month after the study. If you still have any questions, you can ask me at the end of this conversation and it's also possible afterwards via mail, artur.geers@kpn.com. I will repeat the email address again later. This interview is voluntary and you do not need to answer, if something is not clear, please let me know. There are also no wrong answers. This is purely to get a clear image of how customers and end users are using the currently experiencing the process.

Will you give me permission to continue this conversation and record it?

SQ 1:

Have you read the emails that KPN has sent about the infection?

IF no: How come?

If not received: is the email address correct?

IF incorrect e-mail address: what is your e-mail address then I will send the e-mail to this address.

IF yes, why didn't you act on it?

SQ2:

IF mail not read: Could you read that mail for me and share your thoughts out loud, pretend I'm not on the phone. This is to get an idea of how an end user experiences this notification and possibly what question you would have with the information and / or instructions in the email. I stay on the line but try as much as possible to tell me your thoughts and steps. Tell me every thought and / or ideas, there is no right or wrong in this regard.

Do you plan to deal with the infection?

IF yes: how do you plan to do that?

IF no: why not?

I recommend that you change the e-mail address of your WIFI connection at KPN, so that the warnings could be read. If you receive another email entitled "abuse of your internet connection" at the new email address, then you probably have the wrong phone(s) and the infected phone has not yet been addressed.

SQ3:

Before this conversation and the warning from KPN about an infection, did you already hear about Flubot?

IF yes, what have you heard and from whom?

IF no: What do you think is the cause of this Flubot infection?

IF no idea: Have you received suspicious text messages?

If correct Idea: Why do you think you clicked on this link at the time?

If dealing with a lot of text messages: if you should make an estimate of how many messages you received at the time, how much would that have been on average per week?

SQ4:

How did you experience the information in the email about fixing the Flubot infection?

Even before I thank you and say goodbye.

What is your age? Your profession? And how experienced are you in using and recovering your smartphone, give an estimate from very inexperienced (1) to very experienced (5)?

Then I would like to thank you for your time. If you have any questions about the research, I would be happy to help you.

via artur.geers@kpn.com

IF: LARGE IF:

Do you own an android phone?

IF yes: Is this the only android phone that regularly uses your home wifi?

IF no: Is there a single android phone that regularly uses your home wifi or are there several?

IF single: Could you connect me to the one, that phone is most likely infected?

IF no: Can you give me the phone number of that person and do you have any idea when I might be able to contact that person?

Then I'll thank you for your time and call ... back. If you have any questions about the research. I would love to contact you through artur.geers@kpn.com

IF multiple: to be able to find out the infected phone and its user, I know for sure, that the phone was still connected to your wifi on June 15th. Is it then clear which phone it is?

IF yes: Can you tell me the phone number of that person and do you have any idea when I might be able to contact that person?

Then I'll thank you for your time and call ... back. If you have any questions about the research. I would love to contact you through artur.geers@kpn.com.

IF no, then I cannot help you, since I have not more data to trace the phone.

If correct email: then you should search the email titled "abuse of your internet connection" and follow the steps for the android phones that you think might be infected. If you receive the same email in the next few days, then you probably chose the wrong phone. To reassure you, Flubot is no longer harmful except for the fact that it takes up unnecessary battery and storage use on your phone, which in the long run is a waste of your phone.

Then I thank you for your time. If you have any questions about the research. I would love to contact you through artur.geers@kpn.com

IF incorrect email: then you must change the email address from your WIFI connection at KPN, where you receive the alerts on. You will then get another email if the infected android phone is connected with your wifi. The email is titled "abuse of your internet connection", in the meanwhile I'll send you the same email: what is your email address? Follow the steps in the email for the android phone (s) you are using that you think may have been infected. If you receive the same e-mail again in the next few days at the modified e-mail address, then you probably picked the wrong phones. To reassure you Flubot is no longer harmful except for the fact that it uses unnecessary battery and storage on your phone, which is a waste of your phone.

I would like to thank you for your time. If you have any questions about the research, I would love to contact you through artur.geers@kpn.com

Goedenmorgen/-middag, mijn naam is Artur Geers en ik bel namens KPN.

Anderhalve week terug heeft u een email ontvangen van het Abuse Team van KPN over een virus infectie in uw android telefoon. In de mail stond dat we contact met u zouden opzoeken en daarom bel ik u.

Ten eerste om te checken, klopt het dat het mailadres .. van u is? Dat is namelijk het mailadres dat ingeschreven staat bij KPN en aan dit nummer is gekoppeld.

- IF ja: dat is mooi, bel ik gelegen om het probleem op te lossen en tegelijkertijd een aantal vragen voor me te beantwoorden voor een onderzoek dat verricht wordt door mij in samenwerking met KPN en de TU Delft?
 - IF no: Wanneer zou het gelegen zijn om u terug te bellen?

Dan bedank ik u voor u tijd en bel ik .. terug.

- IF no: Is diegene van wie dit nummer en emailadres zijn, nu beschikbaar?
 - IF no: Wanneer zou het gelegen zijn om terug te bellen?

Dan bedank ik u voor u tijd en bel ik .. terug.

Heeft u de mail ontvangen?

- IF no: Ik kan de mail naar een ander mailadres doorsturen, dan kunt u die nu lezen?

Bij KPN merken we dat dit soort infecties lang kunnen duren, zoals in de mail staat hebben we u regelmatig proberen te waarschuwen maar is er volgens ons systeem niks veranderd. Ik bel u om de infectie op te lossen, om uw cyber security te verbeteren en om onderzoek te doen naar hoe klanten reageren en het huidige proces ondervinden van het verhelpen van mobile infecties, Flubot in dit geval. Het gesprek zal opgenomen en getranscribeerd worden als onderdeel van het onderzoek. Ik zal voor het onderzoek behalve Flubot gerelateerde vragen, ook een aantal vragen stellen over uzelf. Het gesprek zal geanonimiseerd opgeslagen worden om later onderzocht te kunnen worden maar er zullen geen persoonsgegevens aan te pas komen, dus de antwoorden zullen niet te herleiden zijn naar u. De resultaten van het onderzoek zullen later gepubliceerd en de gesprekken worden een maand na het publiceren van het onderzoek verwijderd. Als u nog eventuele vragen heeft, dan kan die u aan mij stellen aan het einde van dit gesprek en eventueel ook nog achteraf via de mail, artur.geers@kpn.com, het mailadres zal ik later nog een keer herhalen. Dit gesprek is vrijwillig en u hoeft niet te antwoorden, als iets niet duidelijk is, laat het me vooral weten. Ook zijn er geen foute antwoorden. Dit is puur om een beeld te krijgen van hoe klanten en eindgebruikers het huidige proces ondervinden.

Geeft u mij toestemming om dit gesprek voort te zetten en het op te nemen?

SQ 1:

Heeft u de mailtjes die KPN heeft gestuurd over de infectie gelezen?

IF no: Hoe komt dat?

IF niet ontvangen: Klopt het e-mail adres?

Figure E.1: The prepared set of questions for the semi-structured interview, conducted in Dutch and therefore prepared in Dutch, page 1

IF incorrect e-mail adres: wat is uw e-mail adres dan stuur ik de e-mail naar dit adres.

IF yes: Hoezo heeft u er niet op gehandeld?

SQ2:

IF mail niet gelezen: Zou u die mail voor mij kunnen lezen en uw gedachten hardop kunnen delen, doe maar alsof ik niet aan de telefoon hang. Dit is om een beeld te krijgen van hoe een eindgebruiker deze notificatie ervaart en eventueel welke vraagtekens u zou hebben bij de informatie en/of instructies in de e-mail. Ik blijf aan de lijn maar probeer zoveel mogelijk van uw gedachten en stappen aan mij te vertellen. Vertel me elke gedachte en/of ideeën, er is geen goed of fout wat dit betreft.

Bent u van plan de infectie aan te pakken?

IF yes: Hoe bent u dat van plan te doen?

IF no: Waarom niet?

Ik raad u aan om bij KPN het e-mail adres aan te passen van uw WIFI connectie, zodat u de waarschuwingen wel zou kunnen lezen. Als u dan weer een e-mail getiteld "Misbruik van uw internetverbinding" ontvangt op het aangepaste emailadres, dan heeft u waarschijnlijk de verkeerde telefoon(s) gekozen en is de geïnfecteerde telefoon dus nog niet aangepakt.

SQ1:

Had u voor dit gesprek en de eventuele waarschuwing van KPN over een infectie, al van Flubot gehoord?

IF ja: wat heeft u gehoord en van wie?

IF nee: Wat denkt u dat de oorzaak is van deze Flubot infectie?

IF geen idee: Heeft u verdachte sms-berichten ontvangen?

IF correct idee: Hoezo denkt u dat u toch op de link hebt geklikt?

IF te maken met veel smsjes: Als u een schatting zou moeten doen van hoeveel berichten u toentertijd krijg, hoeveel zouden dat er dan gemiddeld zijn geweest per week?

SQ4:

Hoe heeft u de informatievoorziening in de e-mail over het verhelpen van de Flubot infectie ondervonden?

Nog voordat ik u bedank en gedag zeg,

Wat is uw leeftijd? Uw beroep? En hoe ervaren bent u in het gebruiken en herstellen van uw smartphone, geef een schatting van heel onervaren (1) tot heel ervaren (5)?

Dan bedank ik u voor u tijd. Als u nog vragen heeft over het onderzoek dan zie ik die graag tegemoet via artur.geers@kpn.com

Figure E.2: The prepared set of questions for the semi-structured interview, conducted in Dutch and therefore prepared in Dutch, page 2

IF: GROTE IF:

Bent u eigenaar van een android telefoon?

IF yes: Is dit de enige android telefoon die regelmatig gebruikmaakt van uw wifi thuis?

IF no: Is er een enkele android telefoon die regelmatig gebruikt van uw wifi thuis of zijn er meerdere?

IF enkele: Zou u mij met diegene kunnen verbinden, die telefoon is hoogstwaarschijnlijk geïnfecteerd?

IF no: Kunt u mij het telefoonnummer van diegene vertellen en heeft u een idee wanneer ik diegene gelegen zou kunnen contacteren?

Dan bedank ik u voor u tijd en bel ik .. terug. Als u nog vragen heeft over het onderzoek dan zie ik die graag tegemoet via artur.geers@kpn.com

IF meerdere: Om de telefoon en de gebruiker ervan te kunnen achterhalen, weet ik zeker dat de telefoon op 15 juni nog connectie heeft gemaakt met uw wifi. Is het dan wel duidelijk welke telefoon het is?

IF yes: Kunt u mij het telefoonnummer van diegene vertellen en heeft u een idee wanneer ik diegene gelegen zou kunnen contacteren?

Dan bedank ik u voor u tijd en bel ik .. terug. Als u nog vragen heeft over het onderzoek dan zie ik die graag tegemoet via artur.geers@kpn.com

IF no: Dan kan ik van mijn zijde niet veel voor u doen, ik heb namelijk niet meer data om de telefoon te herleiden.

IF correct email: Dan moet u de e-mail zoeken getiteld "Misbruik van uw internetverbinding" en de stappen volgen voor de android telefoons waarvan u denk dat die mogelijk geïnfecteerd zijn. Als u in de komende dagen weer eenzelfde mail binnenkrijgt op dat emailadres, dan heeft u waarschijnlijk de verkeerde telefoons gekozen. Om u gerust te stellen, Flubot is tegenwoordig niet meer schadelijk behalve het feit dat het onnodig veel batterij en opslag op uw telefoon gebruikt, wat op den duur zonde is van uw telefoon.

Dan bedank ik u voor u tijd. Als u nog vragen heeft over het onderzoek dan zie ik die graag tegemoet via artur.geers@kpn.com

IF incorrect email: Dan moet u bij KPN het e-mail adres aanpassen van uw WIFI connectie, dus waar u de waarschuwingen op ontvangt. Dan krijgt weer een e-mail als de geïnfecteerde android telefoon weer met uw wifi is verbonden. De e-mail is getiteld "Misbruik van uw internetverbinding", ik zal u in de tussentijd diezelfde mail doorsturen: wat is uw e-mailadres?

Figure E.3: The prepared set of questions for the semi-structured interview, conducted in Dutch and therefore prepared in Dutch, page 3

Volg de stappen in de mail voor de android telefoon(s) waarvan u denkt dat ze mogelijk geïnfecteerd zijn. Als u in de komende dagen weer eenzelfde mail binnenkrijgt op het aangepaste emailadres, dan heeft u waarschijnlijk de verkeerde telefoons gekozen. Om u gerust te stellen, Flubot is tegenwoordig niet meer schadelijk behalve het feit dat het onnodig veel batterij en opslag op uw telefoon gebruikt, wat op den duur zonde is van uw telefoon.

Dan bedank ik u voor u tijd. Als u nog vragen heeft over het onderzoek dan zie ik die graag tegemoet via artur.geers@kpn.com

Figure E.4: The prepared set of questions for the semi-structured interview, conducted in Dutch and therefore prepared in Dutch, page 4

Appendix F

Survey

The survey, including a translation afterwards.

1. Enter your age.
 2. Enter your profession
 3. How experienced are you in using and restoring your smartphone? Give an estimation of hardly any experience (1) to expert (5).
 4. Before you were informed by KPN, did you have any experience with sms-phishing malware, like Flubot. [Yes or No]
 5. How did you learn about sms-phishing malware, like Flubot? (multiple answers possible) [work, family, friends, news, government, telecom provider, social media, previous infection, other]
 6. Before you were informed, did you experience something different or suspicious on your phone. [Yes or No]
 7. Explain what you noticed.
 8. Do you have an idea what caused the infection. [Yes or No]
 9. What do you think caused the infection?
 10. How often do you receive SMS messages on average per week? Without counting friends and family.
 11. How likely are you to click on a URL link in a text message that is not from friends or family? Give an estimate from very unlikely (1) to very likely (5).
 12. Did you fix the Flubot infection? [Yes or No]
 13. how many days did it take you to clear up the Flubot infection after you were informed?
 14. Explain why not.
 15. Different types of suffering:
 1. Physical or digital suffering:
 2. Economic suffering:
 3. Psychological suffering:
 4. Reputational suffering:
 5. Social suffering:
- Given the types of distress, have you experienced any distress as a result of the Flubot infection? [Yes, before I was informed; Yes, after I was informed; No.]
16. What type of suffering have you experienced as a result of the Flubot infection? Please estimate the impact the suffering has had on you, from low impact (1) to high impact (5) or “No impact” if that type is not applicable.
 17. Explain what kind of suffering you have experienced (including the seriousness of the suffering you have experienced).
 18. On a scale from very bad (1) to very good (5), how did you experience the Flubot infection and its resolution, regarding:
[The information in the original email about how to resolve the Flubot infection; The available support and resources provided by KPN]
 19. Explain your experience.
 20. Since the Flubot infection, has it changed how you use your smartphone? [Yes or No]
 21. Explain the change in use of your smartphone

09-08-2022 13:14

De ervaring van een Flubot infectie en het verhelpen ervan 1.1

De ervaring van een Flubot infectie en het verhelpen ervan 1.1

Dit betreft de infectie op uw android smartphone die er recentelijk toe heeft geleid dat u e-mails heeft ontvangen van KPN over misbruik van uw internetverbinding.

* Required

Demografie

1. Vult uw leeftijd in *

2. Vult uw beroep in *

3. Hoe ervaren bent u in het gebruiken en herstellen van uw smartphone? Geef een schatting van heel onervaren (1) tot heel ervaren (5): *

1	2	3	4	5
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

<https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&Id=SQV51zWM6kCtdZV/Kw-hr6KFGJEGKtO1Glr5...> 1/8

Figure F.1: The survey the respondents were shown regarding the first aspect, demographics

09-08-2022 13:14

De ervaring van een Flubot infectie en het verhelpen ervan 1.1

Oorzaak

4. Voordat u was ingelicht door KPN, had u al eerder van sms-phishing malware, bijvoorbeeld Flubot, gehoord? *

- Ja
 Nee

5. Hoe bent u over sms-phishing malware, bijvoorbeeld Flubot, te weten gekomen? (Meerdere antwoorden mogelijk) *

- Werkgever
 Familie
 Vrienden
 Nieuws
 Overheid
 Telecom provider
 Sociale media
 Voorgaande infectie
 Other

6. Voordat u was ingelicht, merkte u iets anders of verdachts aan uw telefoon? *

- Ja
 Nee

<https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&Id=SQV51zWM6kCtdZV/Kw-hr6KFGJEGKtO1Glr5...> 2/8

Figure F.2: The survey the respondents were shown regarding the second aspect, cause, part 1

09-08-2022 13:14

De ervaring van een Flubot infectie en het verhelpen ervan 1.1

7. Licht toe wat u merkte. *

8. Heeft u een idee wat de oorzaak had kunnen zijn van de infectie? *

- Ja
 Nee

9. Wat denkt u dat de oorzaak was? *

10. Hoe vaak ontvangt u gemiddeld per week SMS berichten? Zonder vrienden en familie mee te rekenen *

11. Hoe waarschijnlijk is het dat u op een URL link klikt in een SMS bericht dat niet afkomstig is van vrienden of familie? Geef een schatting van heel onwaarschijnlijk (1) tot heel waarschijnlijk (5): *

- 1 2 3 4 5
-

<https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&Id=SQV51zWM6kCtdZV/Kw-hr6KFGJEGKt01Glr5...> 3/8

Figure F.3: The survey the respondents were shown regarding the second aspect, cause, part 2

09-08-2022 13:14

De ervaring van een Flubot infectie en het verholpen ervan 1.1

Verholpen

12. Heeft u de Flubot infectie verholpen? *

- Ja
 Nee

13. Hoeveel dagen duurde het voordat u de Flubot infectie had verholpen, nadat u op de hoogte was? *

14. Licht toe waarom niet *

<https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&Id=SQV51zWM6kCtdZV/Kw-hr6KFGJEGKtO1Glr5...> 4/8

Figure F.4: The survey the respondents were shown regarding the third aspect, remediation

09-08-2022 13:14

De ervaring van een Flubot infectie en het verhelpen ervan 1.1

Leed

Voor de volgende vragen is het nodig om de types leed door te nemen.

Leed types:

- 1) fysiek of digitaal leed: een fysiek of digitaal negatief effect op iemand of iets (bijvoorbeeld het verliezen van je telefoon of data, of fysiek gekwetst raken).
- 2) economisch leed: negatieve financiële of economische consequenties.
- 3) psychologisch leed: een negatief effect op de mentale welzijn.
- 4) reputatieleed: een negatief effect op de algemene opinie over iemand of iets.
- 5) sociaal en maatschappelijk leed: een negatief effect in een sociaal of maatschappelijk context.

15. Gegeven de types leed, heeft u leed ondervonden als gevolg van de Flubot infectie? *

- Ja, voordat ik op de hoogte was gebracht
- Ja, nadat ik op de hoogte was gebracht
- Nee

16. Wat voor type leed heeft u ondervonden als gevolg van de Flubot infectie? Geef een schatting van de impact die het leed heeft gehad op u, van weinig impact (1) tot veel impact (5) of "Geen leed" als dat type niet van toepassing is. *

	Geen leed	1	2	3	4	5
Fysiek of digitaal	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Economisch	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Psychologisch	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reputatie	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sociaal of maatschappelijk	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

<https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&Id=SQV51zWM6kCtdZV/Kw-hr6KFGJEGKtO1Glr5...> 5/8

Figure F.5: The survey the respondents were shown regarding the fourth aspect, harm, part 1

09-08-2022 13:14

De ervaring van een Flubot infectie en het verhelpen ervan 1.1

17. Licht toe wat voor leed u ondervonden heeft (inclusief de ernst het leed dat u heeft ondervonden).

<https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&Id=SQV51zWM6kCtdZV/Kw-hr6KFGJEGKtO1Glr5...> 6/8

Figure F.6: The survey the respondents were shown regarding the fourth aspect, harm, part 2

09-08-2022 13:14

De ervaring van een Flubot infectie en het verhelpen ervan 1.1

Ervaring

18. Op een schaal van heel slecht (1) tot heel goed (5), hoe heeft u de Flubot infectie en het verhelpen ervan ondervonden, betreffende: *

	1	2	3	4	5
de informatie in de oorspronkelijke e-mail over het verhelpen van de Flubot infectie	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
de beschikbare ondersteuning en middelen voorzien door KPN	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

19. Licht uw ervaring toe.

20. Sinds de Flubot infectie, is het veranderd hoe u met uw smartphone omgaat? *

- Ja
 Nee

<https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&Id=SQV51zWM6kCtdZV/Kw-hr6KFGJEGKtO1Glr5...> 7/8

Figure F.7: The survey the respondents were shown regarding the fourth aspect, harm, part 1

09-08-2022 13:14

De ervaring van een Flubot infectie en het verhelpen ervan 1.1

21. Licht de veranderde omgang met uw smartphone toe. *

This content is neither created nor endorsed by Microsoft. The data you submit will be sent to the form owner.

 Microsoft Forms

<https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&Id=SQV51zWM6kCtdZV/Kw-hr6KFGJEGKtO1Glr5...> 8/8

Figure F.8: The survey the respondents were shown regarding the fourth aspect, harm, part 2

Appendix G

Survey answers: Profession

The complete list of professions that the respondents provided, with unemployed-related answers grouped as one group because that group is irrelevant for further analysis.

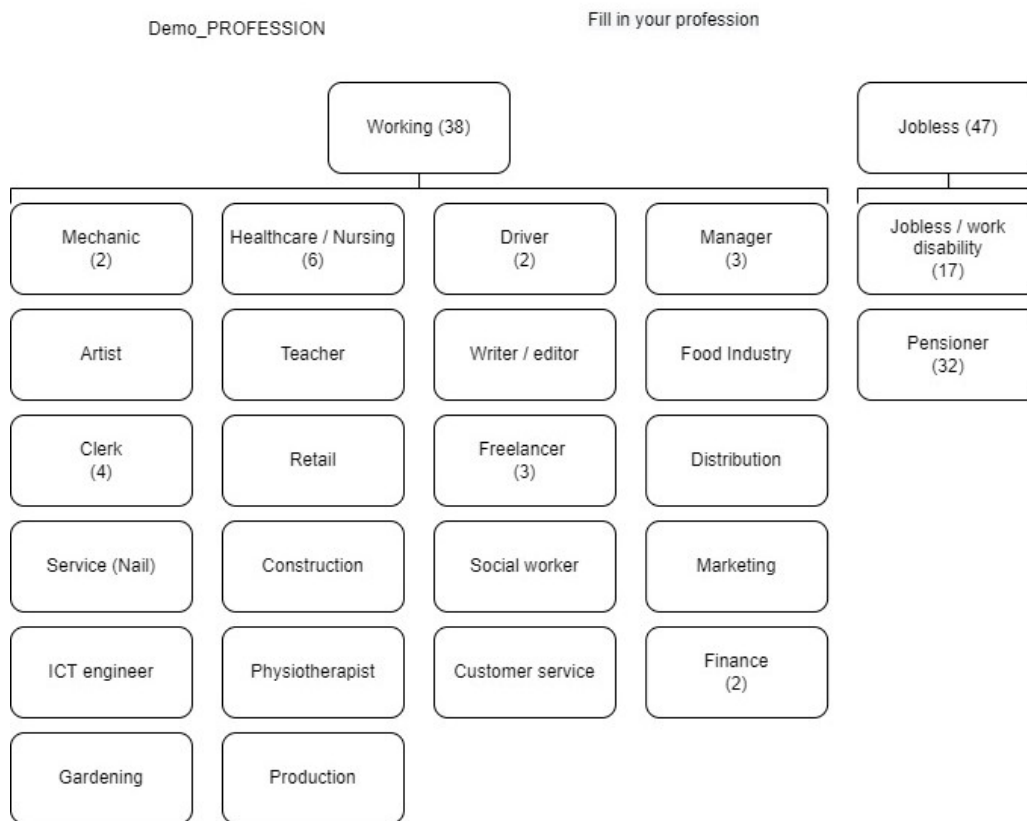


Figure G.1: All professions submitted grouped into two categories, namely: working and unemployed

Appendix H

Summarised interview transcript

The summarised transcript of the interview conducted with an unaware victim of Flubot, found with the IP-CC detection method. The personally identifiable information has been left out to ensure anonymity.

R = Researcher (i.e. Artur Geers), S = Subject

- R: Good afternoon, My name is Artur Geers and I'm calling on behalf of KPN. Am I speaking to ..?
- S: Yes that is correct.
- R: One and a half week ago we, KPN Abuse, sent you an email about an Android infection and in that email it was stated that we would contact you and that is why I am calling. To check, is it correct that your email address is?
- S: No I did not read that mail. We use a different email now.
- R: That makes sense. Do you have a different email address I can send the notification to?
- S: Yes, it is
- R: Okay then I will send the email to you now. I am calling you now to fix the infection and to ask some additional questions for further research. Because our system shows that you repeatedly have been sent an email about the infection at hand, however that is the older email then. This is to improve the cyber security of you and others and to improve our customer service. Am I calling you on a convenient moment?
- S: yeah, this is convenient.
- R: Well in the email you've received by now, it is stated that an Android phone has been infected with Flubot. Have you heard of Flubot before?
- S: No.
- R: Okay well, it is a fast spreading virus that has infected a lot of phones throughout the Netherlands and globally too. It specifically affects Android phones, do you own an Android?
- S: Yes, I own one.
- R: Then there's a chance it is your phone. For us it is impossible to determine which phone it is exactly. We only know that the phone regularly connects to your Wifi connection at home, which is a KPN broadband connection if I'm correct?
- S: Yes that is right.
- R: Well that is how we can detect these infections. Have you had the chance to read the email by now?
- S: I am currently not at home, so it will have to wait.
- R: To be clear, I cannot change the email you have submitted as contact information for KPN. So when you have time, I strongly recommend you change it to the correct email address so that you can be contacted in time, if something like this happens again or even a different infection or risk. Have you noticed anything on your phone that could've been caused by a smartphone infection?

- S: I have not noticed anything.
- R: Good to know. This is part of improving the customer service, your and others' cybersecurity and to perform research. Is it okay if this conversation is recorded and the answers will be used for further research, that might get published?
- S: Yeah go ahead.
- R: Well thank you. When you get home are you planning on remediating the infection?
- S: Yeah I will take a look at it.
- R: So there's a chance that, if multiple Android phones regularly connect to your Wifi network at home, it is not the correct phone you will have to perform the reset on. Then you will receive continuous email notifications, on that updated email address. If that is the case, then you most likely have performed the reset on an Android that was not infected, and you will have to perform it on another Android, the most likely one to be infected. If the email warnings completely stop, then it is likely that you have remediated the issue.
- S: Okay I have to go now.
- R: Okay, with this I hope to have informed you enough to remediate the infection. Then I hope this has helped you and thank you for your time.

Appendix I

Spearman's Correlation on survey result variables

		Correlations					
			Demo_AGE	Demo_Skill LevelSmart phone	1_Average WeeklySMS	1_LikelihoodClickingUnknownSender	2_DaysTakenRemediation
Spearman's rho	Demo_AGE	Correlation Coefficient	1.000	.110	.204	.002	.182
		Sig. (2-tailed)	.	.311	.059	.988	.140
		N	87	87	87	87	67
Demo_Skill LevelSmart phone		Correlation Coefficient	.110	1.000	.082	-.057	-.164
		Sig. (2-tailed)	.311	.	.448	.600	.184
		N	87	87	87	87	67
1_Average WeeklySMS		Correlation Coefficient	.204	.082	1.000	.402**	.115
		Sig. (2-tailed)	.059	.448	.	.000	.352
		N	87	87	87	87	67
1_Likelihood ClickingUnknownSender		Correlation Coefficient	.002	-.057	.402**	1.000	-.228
		Sig. (2-tailed)	.988	.600	.000	.	.064
		N	87	87	87	87	67
2_Days Taken Remediation		Correlation Coefficient	.182	-.164	.115	-.228	1.000
		Sig. (2-tailed)	.140	.184	.352	.064	.
		N	67	67	67	67	67
3_Harm Physical Digital		Correlation Coefficient	-.089	-.061	-.155	-.279	.189
		Sig. (2-tailed)	.550	.681	.294	.055	.225
		N	48	48	48	48	43
3_Harm Economic		Correlation Coefficient	.157	.059	-.088	.083	-.248
		Sig. (2-tailed)	.288	.689	.553	.576	.110
		N	48	48	48	48	43
3_Harm Psychological		Correlation Coefficient	.162	.016	.119	.348*	.044
		Sig. (2-tailed)	.273	.912	.421	.015	.779
		N	48	48	48	48	43
3_Harm Reputational		Correlation Coefficient	-.023	.048	.256	.444**	.009
		Sig. (2-tailed)	.879	.748	.079	.002	.955
		N	48	48	48	48	43
3_Harm Social		Correlation Coefficient	.034	.071	.198	.299*	.044
		Sig. (2-tailed)	.818	.633	.176	.039	.780
		N	48	48	48	48	43

Figure I.1: Correlations, significance and N per variable correlation in SPSS for all ordinal and ratio variables, page 1

			Correlations				
			3_HarmPhy sicalDigital	3_HarmEco nomic	3_HarmPsy chological	3_HarmRe putational	3_HarmSoci etal
Spearman's rho	Demo_AGE	Correlation Coefficient	-.089	.157	.162	-.023	.034
		Sig. (2-tailed)	.550	.288	.273	.879	.818
		N	48	48	48	48	48
	Demo_SkillLevelSmartphone	Correlation Coefficient	-.061	.059	.016	.048	.071
		Sig. (2-tailed)	.681	.689	.912	.748	.633
		N	48	48	48	48	48
	1_AverageWeeklySMS	Correlation Coefficient	-.155	-.088	.119	.256	.198
		Sig. (2-tailed)	.294	.553	.421	.079	.176
		N	48	48	48	48	48
	1_LikelihoodClickingUnknownSender	Correlation Coefficient	-.279	.083	.348*	.444**	.299*
		Sig. (2-tailed)	.055	.576	.015	.002	.039
		N	48	48	48	48	48
	2_DaysTakenRemediation	Correlation Coefficient	.189	-.248	.044	.009	.044
		Sig. (2-tailed)	.225	.110	.779	.955	.780
		N	43	43	43	43	43
	3_HarmPhysicalDigital	Correlation Coefficient	1.000	.056	.190	.086	.141
		Sig. (2-tailed)	.	.706	.195	.563	.340
		N	48	48	48	48	48
	3_HarmEconomic	Correlation Coefficient	.056	1.000	.341*	.434**	.492**
		Sig. (2-tailed)	.706	.	.018	.002	.000
		N	48	48	48	48	48
	3_HarmPsychological	Correlation Coefficient	.190	.341*	1.000	.517**	.538**
		Sig. (2-tailed)	.195	.018	.	.000	.000
		N	48	48	48	48	48
	3_HarmReputational	Correlation Coefficient	.086	.434**	.517**	1.000	.879**
		Sig. (2-tailed)	.563	.002	.000	.	.000
		N	48	48	48	48	48
	3_HarmSocial	Correlation Coefficient	.141	.492**	.538**	.879**	1.000
		Sig. (2-tailed)	.340	.000	.000	.000	.
		N	48	48	48	48	48

Figure I.2: Correlations, significance and N per variable correlation in SPSS for all ordinal and ratio variables, page 2

Correlations				
			4_Satisfacti onInformati onProvision	4_Satisfacti onSupport
Spearman's rho	Demo_AGE	Correlation Coefficient	-.033	-.059
		Sig. (2-tailed)	.763	.589
N		87	87	
Demo_SkillL evelSmartph one	Correlation Coefficient	.324**	.221*	
	Sig. (2-tailed)	.002	.040	
	N	87	87	
1_AverageW eeklySMS	Correlation Coefficient	.060	-.069	
	Sig. (2-tailed)	.581	.523	
	N	87	87	
1_Likelihood ClickingUnkn ownSender	Correlation Coefficient	-.003	.003	
	Sig. (2-tailed)	.981	.980	
	N	87	87	
2_DaysTake nRemediatio n	Correlation Coefficient	-.022	-.130	
	Sig. (2-tailed)	.858	.294	
	N	67	67	
3_HamPhys icalDigital	Correlation Coefficient	-.098	-.089	
	Sig. (2-tailed)	.506	.549	
	N	48	48	
3_HamEcon omic	Correlation Coefficient	-.158	-.015	
	Sig. (2-tailed)	.283	.917	
	N	48	48	
3_HamPsc hological	Correlation Coefficient	-.036	.001	
	Sig. (2-tailed)	.806	.997	
	N	48	48	
3_HamRepu tational	Correlation Coefficient	.116	-.028	
	Sig. (2-tailed)	.434	.853	
	N	48	48	
3_HamSoci etal	Correlation Coefficient	.124	-.066	
	Sig. (2-tailed)	.400	.656	
	N	48	48	

Figure I.3: Correlations, significance and N per variable correlation in SPSS for all ordinal and ratio variables, page 3

Correlations

		Demo_AGE	Demo_Skill LevelSmart phone	1_Average WeeklySMS	1_LikelihoodClickingUnknownSender	2_DaysTakenRemediation
4_SatisfactionInformation Provision	Correlation Coefficient	-.033	.324**	.060	-.003	-.022
	Sig. (2-tailed)	.763	.002	.581	.981	.858
	N	87	87	87	87	67
4_SatisfactionSupport	Correlation Coefficient	-.059	.221*	-.069	.003	-.130
	Sig. (2-tailed)	.589	.040	.523	.980	.294
	N	87	87	87	87	67

Correlations

		3_HarmPhysicalDigital	3_HarmEconomic	3_HarmPsychological	3_HarmReputational	3_HarmSocietal
4_SatisfactionInformation Provision	Correlation Coefficient	-.098	-.158	-.036	.116	.124
	Sig. (2-tailed)	.506	.283	.806	.434	.400
	N	48	48	48	48	48
4_SatisfactionSupport	Correlation Coefficient	-.089	-.015	.001	-.028	-.066
	Sig. (2-tailed)	.549	.917	.997	.853	.656
	N	48	48	48	48	48

Correlations

		4_SatisfactionInformationProvision	4_SatisfactionSupport
4_SatisfactionInformation Provision	Correlation Coefficient	1.000	.620**
	Sig. (2-tailed)	.	.000
	N	87	87
4_SatisfactionSupport	Correlation Coefficient	.620**	1.000
	Sig. (2-tailed)	.000	.
	N	87	87

** . Correlation is significant at the 0.01 level (2-tailed).

* . Correlation is significant at the 0.05 level (2-tailed).

Figure I.4: Correlations, significance and N per variable correlation in SPSS for all ordinal and ratio variables, page 4

Appendix J

Active cases descriptive statistics

The remaining 14 active cases have shown, of which one subject has performed the interview (i.e. data subject 11), that Flubot infections can last very long if not treated properly (or at all). All the active cases have been analysed to get an insight into how long these cases have lasted for and how often these cases have been detected on separate days (i.e. events).

Data subject	Sum of events (days an infection was detected)	Length in months	Number of cases (different periods)
1	154	10	10
2	76	10	15
3	63	7	10
4	83	7	10
5	90	7	7
6	137	9	2
7	125	7	4
8	40	4	3
9	156	10	4
10	79	9	4
11	126	7	4
12	135	7	3
13	107	7	5
14	75	5	4
Average	103.3	7.6	6.1

Table J.1: Data subjects, the amount of times that an infected device has connected (i.e. events), the amount of months it has lasted for and in how many periods (i.e. cases), including the averages of the sample

Appendix K

Forum customer feedback on rigorousness of SMS auto block

The customer in the figures below has a discussion with a moderator about the limitless bundle not being limitless and getting blocked every time he sends a large amount of texts. He argues that the policies and rules made up by KPN do not constitute for the measures applied and would like an exemption to the current blockades he keeps experiencing [51]. This forum discussion is publicly accessible, therefore it is not considered secret information, however, out of respect for the moderator and the users, their usernames, including pictures have been removed from the screenshots.

A forum where a user writes the following;

The user purchased a bundle with unlimited calls and text, however after sending a 1000 texts the user got blocked. The user got suspected of being the victim of Flubot Malware, which wasn't the case. After reaching out to customer service, the user was unblocked. However, the user asked to disable the block if he sends a lot of text, which isn't possible due to the Fair Use policy of KPN when using an unlimited bundle.

The forum moderator reacts by highlighting section 7.2 of the terms and conditions.

In summary states that sending around 1000 texts in a short period, is not normal and reasonable use of the bundle and can be seen as a potential Flubot Malware infection. Where in a short period of time a lot of texts are sent to quickly spread the malware. The reason for not disabling the blockade is due to the user still being vulnerable to Flubot Malware.

The user states that with his order the terms and conditions of 2020 and 2018 are included. In the terms and conditions of 2018, fair use policy is stated and linked to a website where their explained. However, on the website the fair use policy isn't specified.

The forum moderator responds; by highlighting chapter 7.2 of the terms and conditions where is specified that customers must follow a code of conduct. The forum moderator states that there isn't a fair use policy, however there is a code of conduct which states that a customer must use their bundle for, personal, reasonable and normal use. In addition, if the user doesn't follow the code of conduct, he will get blocked again for their own safety and other users against a Flubot Malware infection.

The user writes that he ordered an unlimited text and call bundle, however in reality there is a limit. In addition, he complains about the problems and time it takes to unblock him. After 6 phone calls that didn't result in anything he got forwarded to the complaint department. Which will take between 1 to 3 days and he is currently waiting for that.

The forum moderator responds; Nowadays, customers mostly use Whatsapp, Facebook Messenger or Telegram for sending messages. And sending a large amount of text in a short period is seen as suspicious behaviour. This behaviour results in an automatic process to block a user and the department Credit Risk will determine if a user needs to be unblocked.

User writes that after a discussion with an unknown department (he thinks Credit Risk Department), he got unblocked however not permanently.

The forum moderator recommends using a business bundle, since there are different terms and conditions. And sending a lot of texts in a short period does not fall in the code of conduct of personal, reasonable and normal use.

8/16/22, 3:42 PM

Flubot Malware blokkade na het versturen van veel sms'jes. Let op: SMS-verbruik hoger dan normaal | KPN Community

Aanbod Service MijnKPN

Webmail

Naar Zakelijk

Zoeken...

Menu

BEANTWOORD

Flubot Malware blokkade na het versturen van veel sms'jes. Let op: SMS-verbruik hoger dan normaal

7 maanden geleden • 6 reacties • 208 keer bekeken

Afgelopen week heb ik bij KPN een bundel aangeschaft met onbeperkt bellen / sms'en, juist omdat ik erg veel sms en op de website overduidelijk staat vermeld dat er geen fair use is, en onbeperkt dus ook écht onbeperkt is.

Echter, de eerste dag dat ik er gebruik van heb gemaakt ben ik na het versturen van zo'n 1000 sms'jes geblokkeerd.

In de mail die ik erover heb gekregen staat iets over een Flubot Malware, wat het in dit geval dus niet is, maar er staat niet hoe je de blokkade kan weghalen.

Toen heb ik maar contact opgenomen met de klantenservice; deze heeft me gelukkig kunnen deblokkeren, maar toen ik vroeg of de check niet permanent uitgeschakeld kan worden zei degene met wie ik sprak dat dit niet kon, omdat er een Fair Use policy is...

Had toen alleen de verkeerde pagina voor me staan, waar het erover ging dat er bij Roaming geen Fair Use is.

Vervolgens heb ik de juiste pagina weer gevonden waar stond dat er überhaupt geen Fair Use policy is, en nog een keer teruggebeld naar de klantenservice. Dit keer kwam ik aan de lijn met iemand anders; ik legde de hele situatie uit, dus dat er gezegd is dat er een Fair Use policy is en wordt gehandhaafd, terwijl op de website overduidelijk staat van niet.

Ze ging overleggen met een andere afdeling, en toen ze terugkwam zei ze dat er inderdaad een Fair Use policy is, en deze in de Algemene voorwaarden te vinden is.

In de algemene voorwaarden staat echter niks over een Fair Use policy, alleen iets over gedragsregels. Aan deze gedragsregels hou ik mij gewoon, en bovendien staat er niks over te veel bellen of sms'en.

Bovendien staat er op de website dus nog steeds overduidelijk dat er géén Fair Use policy is.

Veel verder dan dat kwam ik met haar niet, ook omdat ze puur als tussenpersoon functioneerde. Uiteindelijk zei ze dat ik het beste een klacht in kon dienen.

Een klacht gaat alleen weer via de klantenservice van jullie zelf, of het moet via de geschillencommissie maar dit kost me weer een hoop geld.

Daarom besloten dit topic te openen.

Ik voel mij enorm om te tuin geleid: eerst krijg ik een SMS waarin staat dat de dienst op mijn verzoek is geblokkeerd. Dit heb ik nooit verzocht...

Vervolgens krijg ik een mailtje met daarin iets over een Flubot Malware (met daarin ook niks over een Fair Use policy), maar aan de telefoon wordt er gezegd dat ik geblokkeerd ben door het overtreden van de Fair Use policy.

Nogmaals: op de website staat dat er geen Fair Use is, en ook in de algemene voorwaarden staat hier niks over. Ik heb ook andere topics op dit forum bekeken, en daar zie ik tevens bevestigd dat er géén Fair Use policy is.

Jullie handhaven dus een niet-bestaande Fair Use policy, maar laten het lijken alsof het is door die Flubot. Als het echt ter bescherming voor de Flubot zou zijn, waarom kan deze check dan niet worden uitgeschakeld op mijn verzoek als ik aangeef het zelf te zijn?

Hier staat aangegeven dat er geen fair use is, of dat onbeperkt écht onbeperkt is:

<https://www.kpn.com/mobiel-abonnement/sim-only.htm> --> "Veelgestelde vragen" --> "Is er een fair use policy voor onbeperkt bellen bij mijn Sim Only abonnement?":

<https://forum.kpn.com/mobiel-15/flubot-malware-blokkade-na-het-versturen-van-veel-sms-jes-let-op-sms-verbruik-hoger-dan-normaal-556707>

1/7

Figure K.1: Criticism on the rigorousness of the SMS auto block in the KPN forum, page 1

8/16/22, 3:42 PM Flubot Malware blokkade na het versturen van veel sms'sjes. Let op: SMS-verbruik hoger dan normaal | KPN Community

"nee, die is er niet. Onbeperkt bellen is ook echt onbeperkt bellen. En als je sms's op zijn r ijan verlagen we je alleen je sneineid, maar brengen we geen extra kosten in rekening."

<https://www.kpn.com/shop/mobiel/sim-only> --> "meer weten?" --> "Over je abonnement" --> "Voorwaarden en tarieven":

"Onbeperkt bellen bij een telefoonabonnement is ook echt onbeperkt bellen. Met uitzondering van nummers buiten de EU en de informatiekosten van betaalde servicenummers. Denk bijvoorbeeld aan 0900-nummers."

[redacted] welkom op het KPN forum. Goed dat je ons gevonden hebt, ik kan me namelijk voorstellen dat je hier meer duidelijkheid over wilt. Wanneer je een abonnement bij ons afsluit, zijn er een aantal gedragsregels waar je je aan dient te houden. Dit is wat hierover in de algemene voorwaarden staat:

7.2 Gedragsregels waar u zich aan moet houden
Het is belangrijk dat u zich aan de volgende regels houdt:

- *Onze diensten zijn bestemd voor eigen, redelijk en normaal gebruik. Daarmee bedoelen we persoonlijk gebruik voor privédoeleinden. Of als het diensten zijn die gericht zijn op zakelijke klanten: voor gewoon zakelijk gebruik. We vertrouwen erop dat u onze diensten alleen op die manier gebruikt*
- *U mag alleen apparaten aansluiten die voldoen aan de wettelijke vereisten die voor apparaten gelden. Bijvoorbeeld eisen op het gebied van veiligheid. Zo brengt u de werking van ons netwerk niet in gevaar.*
- *We vertrouwen erop dat u en onze medewerkers elkaar altijd met respect behandelen*
- *We vertrouwen erop dat u de dienst niet gebruikt op een manier die strafbaar is of onrechtmatig tegenover ons en/of een andere persoon of ander bedrijf.*

Strafbaar en/of onrechtmatig gebruik zijn in ieder geval:

- *Versturen van spam*
- *Openbaar maken of verspreiden van kinderporno of andere strafbare porno*
- *Verspreiden van (computer)virusen of andere bestanden die de (goede) werking van onze software of die van anderen kunnen beschadigen*
- *Bedreigen van personen*
- *Illegaal downloaden*
- *Zonder toestemming het adres van iemand gebruiken waardoor het lijkt alsof u de afzender van een bepaald bericht bent*
- *Iemand anders lastigvalven of inbreuk maken op de rechten en het persoonlijk leven van iemand anders*
- *Storingen of overlast veroorzaken*
- *Hacken*
- *Inbreuk maken op intellectuele eigendomsrechten van ons en/of derden*
- *Uw nummer gebruiken op een manier die in strijd is met de wettelijke regels die voor het gebruik van nummers gelden*

Houdt u zich niet aan deze gedragsregels? Dan kunnen we maatregelen treffen. Bijvoorbeeld het tijdelijk stopzetten van de dienst of het beëindigen van de overeenkomst.

Er wordt in de algemene voorwaarden niet gesproken over een fair use policy, maar er wordt wel gesproken over eigen, redelijk en normaal gebruik. Wanneer je 1000 sms'sjes in korte tijd verstuurd, wordt dit niet meer gezien als normaal en redelijk gebruik. Dit doet denken aan een mogelijke besmetting met **Flubot malware**, waarbij in korte tijd veel sms'sjes worden verstuurd om de malware zo verder te verspreiden. Hoewel je hier als gebruiker misschien niet direct iets aan kunt doen als je slachtoffer bent geworden, is dit wel in strijd met onze algemene voorwaarden. Om jouzelf en anderen te beschermen, kan je daarom geblokkeerd worden zo gauw we constateren dat je hier slachtoffer van bent geworden. Dit doen we door te monitoren op onredelijk sms gebruik. Hoe weet je of dit voor jou van toepassing is?

- Je kunt ineens niet meer bellen/SMS'en/internetten
- Je ontvangt rare SMS'sjes van mensen die je niet kent, waar in staat dat je hén berichten zou hebben gestuurd, maar je weet nergens van

Kun je niet meer sms'en, dan ben je dus geblokkeerd. Je kunt ons dan bellen om de blokkade op te heffen. Het is alleen niet mogelijk om een permanente deblokkade in te stellen. Je zou namelijk in de toekomst alsnog slachtoffer kunnen worden van Flubot, dus blijven wij monitoren op normaal en redelijk gebruik. Zien wij weer abnormaal verbruik, dan zullen wij de blokkade opnieuw instellen om jou en anderen te beschermen. Het beste dat je dan kunt doen, is opnieuw telefonisch contact met ons opnemen om de blokkade op te heffen.

[Bekijk origineel](#)

probleem sms sms-diensten misleiding algemene voorwaarden

Like Quote Topic volgen Share

<https://forum.kpn.com/mobiel-15/flubot-malware-blokkade-na-het-versturen-van-veel-sms-sjes-let-op-sms-verbruik-hoger-dan-normaal-556707>

2/7

Figure K.2: Criticism on the rigorousness of the SMS auto block in the KPN forum, page 2

8/16/22, 3:42 PM Flubot Malware blokkade na het versturen van veel sms'sjes. Let op: SMS-verbruik hoger dan normaal | KPN Community

6 reacties Oudste eerst ▾

[Redacted]

Nog een vreemd dingetje waar ik net achter kom:

In de mail van de bevestiging van de bestelling zijn de Algemene Voorwaarden van 2020 bijgesloten, maar in de mail waarin ook het contract staat, zijn nog de oude voorwaarden, van 2018, bijgesloten.

Nou staat er in de voorwaarden van 2018 (artikel 7) het volgende:

"Houdt u zich niet aan deze regels voor redelijk gebruik van uw dienst? Dan kunnen we maatregelen treffen. Bijvoorbeeld het tijdelijk stopzetten van de dienst of het opzeggen van de overeenkomst. Op onze website (onder fair use) leest u wat niet redelijk gebruik is en wat we kunnen doen."

Hier staat dat er wél een fair use policy is, en op de website zou staan wat die inhoud. Op de website staat alleen juist weer dat er géén fair use policy is (zie vorige post).

En überhaupt gelden voor mij neem ik aan de voorwaarden van 2020, niet die van 2018, aangezien ik het abonnement pas net heb aangeschaft?

👍 Like 🗨️ Quote

7 maanden geleden

[Redacted] kpn Moderator • 5178 reacties • ANTWOORD

Welkom op het KPN forum. Goed dat je ons gevonden hebt, ik kan me namelijk voorstellen dat je hier meer duidelijkheid over wilt. Wanneer je een abonnement bij ons afsluit, zijn er een aantal gedragsregels waar je je aan dient te houden. Dit is wat hierover in de algemene voorwaarden staat:

7.2 Gedragsregels waar u zich aan moet houden
Het is belangrijk dat u zich aan de volgende regels houdt:

- *Onze diensten zijn bestemd voor eigen, redelijk en normaal gebruik. Daarmee bedoelen we persoonlijk gebruik voor privédoeleinden. Of als het diensten zijn die gericht zijn op zakelijke klanten: voor gewoon zakelijk gebruik. We vertrouwen erop dat u onze diensten alleen op die manier gebruikt*
- *U mag alleen apparaten aansluiten die voldoen aan de wettelijke vereisten die voor apparaten gelden. Bijvoorbeeld elsen op het gebied van veiligheid. Zo brengt u de werking van ons netwerk niet in gevaar.*
- *We vertrouwen erop dat u en onze medewerkers elkaar altijd met respect behandelen*
- *We vertrouwen erop dat u de dienst niet gebruikt op een manier die strafbaar is of onrechtmatig tegenover ons en/of een andere persoon of ander bedrijf.*

Strafbaar en/of onrechtmatig gebruik zijn in ieder geval:

- *Versturen van spam*
- *Openbaar maken of verspreiden van kinderporno of andere strafbare porno*
- *Verspreiden van (computer)virussen of andere bestanden die de (goede) werking van onze software of die van anderen kunnen beschadigen*
- *Bedreigen van personen*
- *illegaal downloaden*
- *Zonder toestemming het adres van iemand gebruiken waaraan het lijkt alsof u de afzender van een bepaald bericht bent*
- *Iemand anders lastigvallen of inbreuk maken op de rechten en het persoonlijk leven van iemand anders*
- *Storingen of overlast veroorzaken*
- *Hacken*
- *Inbreuk maken op intellectuele eigendomsrechten van ons en/of derden*
- *Uw nummer gebruiken op een manier die in strijd is met de wettelijke regels die voor het gebruik van nummers gelden*

Houdt u zich niet aan deze gedragsregels? Dan kunnen we maatregelen treffen. Bijvoorbeeld het tijdelijk stopzetten van de dienst of het beëindigen van de overeenkomst.

Er wordt in de algemene voorwaarden niet gesproken over een fair use policy, maar er wordt wel gesproken over eigen, redelijk en normaal gebruik. Wanneer je 1000 sms'sjes in korte tijd verstuurd, wordt dit niet meer gezien als normaal en redelijk gebruik. Dit doet denken aan een mogelijke besmetting met [Flubot malware](#), waarbij in korte tijd veel sms'sjes worden verstuurd om de malware zo verder te verspreiden. Hoewel je hier als gebruiker misschien niet direct iets aan kunt doen als je slachtoffer bent geworden, is dit wel in strijd met onze algemene voorwaarden. Om jouzelf

7 maanden geleden

<https://forum.kpn.com/mobiel-15/flubot-malware-blokkade-na-het-versturen-van-veel-sms-jes-let-op-sms-verbruik-hoger-dan-normaal-556707>

3/7

Figure K.3: Criticism on the rigorosity of the SMS auto block in the KPN forum, page 3

8/16/22, 3:42 PM **Flubot Malware blokkade na het versturen van veel sms'jes. Let op: SMS-verbruik hoger dan normaal | KPN Community**



en anderen te beschermen, kan je daarom geblokkeerd worden zo gauw we constateren dat je hier slachtoffer van bent geworden. Dit doen we door te monitoren op onredelijk sms gebruik. Hoe weet je of dit voor jou van toepassing is?

- Je kunt ineens niet meer bellen/SMS'en/internetten
- Je ontvangt rare SMS'jes van mensen die je niet kent, waar in staat dat je hén berichten zou hebben gestuurd, maar je weet nergens van

Kun je niet meer sms'en, dan ben je dus geblokkeerd. Je kunt ons dan bellen om de blokkade op te heffen. Het is alleen niet mogelijk om een permanente deblokkade in te stellen. Je zou namelijk in de toekomst alsnog slachtoffer kunnen worden van Flubot, dus blijven wij monitoren op normaal en redelijk gebruik. Zien wij weer abnormaal verbruik, dan zullen wij de blokkade opnieuw instellen om jou en anderen te beschermen. Het beste dat je dan kunt doen, is opnieuw telefonisch contact met ons opnemen om de blokkade op te heffen.

—
 "There is a defiance in being a dreamer" — V.E. Schwab, *The Invisible Life of Addie LaRue*

👍 Like 🗨️ Quote

  7 maanden geleden


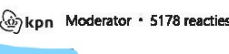
Ik begrijp dat er gedragsregels zijn, maar dan nog zou onbeperkt écht onbeperkt moeten zijn.
 En dat het een mogelijke besmetting is met de Flubot, ja oké, maar die blokkades zorgen er wel voor dat onbeperkt níét echt onbeperkt is.

Wat volgens de voorwaarden bedoeld wordt met eigen, redelijk en normaal gebruik:
 "persoonlijk gebruik voor privédoeleinde"
 Dit betekent dus niet dat er een beperking is van de hoeveelheid SMS die je verstuurd.

Inmiddels was ik 2-3 dagen geleden weer geblokkeerd. Toen ik gisteren belde had ik weer een slechte ervaring (vooral betreft de aparte afdeling):
 Ik heb namelijk 6 keer moeten bellen om iemand aan de lijn te krijgen. Telkens hoorde ik alleen gehijg en/of gemompel, waarna er op werd gehangen. Of ik werd in de wacht gezet (alle medewerkers bezet), daarna werd er opgenomen om direct opgehangen te worden.
 De 6de keer kreeg ik iemand aan de lijn waarvan het klonk alsof ie er totaal geen zin in had. Uiteindelijk zei hij dat hij me door kan verbinden naar de afdeling klachten, en voordat ik daar nog op kon reageren had ie me al doorverbonden.


Diegene zei tenminste wel dat ie me zou helpen. Hij zou erachter gaan om de blokkade permanent eraf te laten halen, dit zou 1-3 dagen duren, daar wacht ik nu nog op.

👍 Like 🗨️ Quote

  kpn Moderator • 5178 reacties 7 maanden geleden

Wat volgens de voorwaarden bedoeld wordt met eigen, redelijk en normaal gebruik:
 "persoonlijk gebruik voor privédoeleinde"
 Dit betekent dus niet dat er een beperking is van de hoeveelheid SMS die je verstuurd.

Ja, dat klopt. Maar vergeet niet dat er tegenwoordig niet zo veel meer van sms gebruik gemaakt wordt. Men gebruikt tegenwoordig veelal Whatsapp, Facebook Messenger of Telegram voor het versturen van berichten. Veel sms'jes versturen in korte tijd wordt daardoor al snel gezien als afwijkend sms gedrag. En afwijkend sms gedrag kan duiden op een geautomatiseerd proces of een besmetting met Flubot malware. En dit is weer in strijd met de gedragsregels, dus wordt je uit voorzorg geblokkeerd. Contact met de afdeling Credit Risk is dan aan de orde om te achterhalen wat het sms gedrag veroorzaakt en om de blokkade op te heffen, natuurlijk.

 *Inmiddels was ik 2-3 dagen geleden weer geblokkeerd. Toen ik gisteren belde had ik weer een slechte ervaring (vooral betreft de aparte afdeling):
 ik heb namelijk 6 keer moeten bellen om iemand aan de lijn te krijgen. Telkens hoorde ik alleen gehijg en/of gemompel, waarna er op werd gehangen. Of ik werd in de wacht gezet (alle medewerkers bezet), daarna werd er opgenomen om direct opgehangen te worden.
 De 6de keer kreeg ik iemand aan de lijn waarvan het klonk alsof ie er totaal geen zin in had. Uiteindelijk zei hij dat hij me door kan verbinden naar de afdeling klachten, en voordat ik daar nog op kon reageren had ie me al doorverbonden.
 Diegene zei tenminste wel dat ie me zou helpen. Hij zou erachter gaan om de blokkade permanent eraf te laten halen, dit zou 1-3 dagen duren, daar wacht ik nu nog op.*

Dit is niet wat je van ons mag verwachten. Mijn excuses voor deze nare ervaring met de telefoonlijn! Ik ben bang dat ik hier weinig aan kan veranderen, maar ik kan wel voor je uitzoeken wanneer je een telefoontje kunt verwachten. Ik heb momenteel alleen nog geen gegevens van je. Zou je kunnen vertellen wat voor OS je hebt gebruikt? En welke telefoonnummer heb je gebruikt? En hoe vaak heb je gebeld?

<https://forum.kpn.com/mobiel-15/flubot-malware-blokkade-na-het-versturen-van-veel-sms-jes-let-op-sms-verbruik-hoger-dan-normaal-556707> 4/7

Figure K.4: Criticism on the rigorousness of the SMS auto block in the KPN forum, page 4

8/16/22, 3:42 PM **Flubot Malware blokkade na het versturen van veel sms'sjes. Let op: SMS-verbruik hoger dan normaal | KPN Community**

je [forumprofiel](#) willen aanvullen met jouw 06-nummer, postcode, huisnummer, geboortedatum en klantnummer? Jouw mobiele nummer kan je invullen onder 'persoonlijke opmerkingen'. De gegevens in jouw profiel zijn alleen zichtbaar voor jou en de moderators. Geef je hier een seintje als je jouw profiel hebt ingevuld?

—

"There is a defiance in being a dreamer" — V.E. Schwab, *The Invisible Life of Addie LaRue*

👍 Like ➦ Quote

 5 maanden geleden


Ten eerste m'n excuses voor de late reactie. Ik had even de tijd nog zin om uren lang te bellen en schrijven hierover.

Na de belofte van de klachtenafdeling op 9 januari om binnen 3 dagen een permanente deblokkade in te stellen, heb ik hier niks meer over gehoord, en ik ben ook niet gedeblokkeerd. Op 26 februari heb ik maar weer eens gebeld hierover (ik weet niet welke afdeling ik aan de lijn had, maar het was via het normale KPN nummer, 0800 0402, en bij het inspreken waar je over belt heb ik gezegd dat het over een klacht ging), en nu kreeg ik weer hetzelfde verhaal als eerst, dat er een fair use policy van toepassing is. Uiteindelijk na een discussie hierover heeft degene waarmee ik beide boos de lijn opgehangen. Ik was nu wel weer gedeblokkeerd, maar niet permanent. (Gezien degene waarmee ik aan de lijn was mij kon deblokken ga ik ervan uit dat dit niet de klachtenafdeling was maar de Credit Risk afdeling)

Om dus even kort samen te vatten:

- De Credit Risk afdeling verwijst mij steeds naar de klachtenafdeling en verbindt mij uiteindelijk door naar die afdeling waarop ik besluit de klacht in te dienen
- De klachtenafdeling gaf mij gelijk en zegt dat er binnen 3 dagen een permanente deblokkade wordt ingesteld
- 48 dagen later heb ik nog niks gehoord dus neem ik zelf weer contact op (onbekend welke afdeling), en hoor ik weer precies hetzelfde als de Credit Risk afdeling mij steeds vertelde. Mijn klacht lijkt compleet genegeerd te zijn.


Vrij absurd als je het mij vraagt..



Ja, dat klopt. Maar vergeet niet dat er tegenwoordig niet zo veel meer van sms gebruik gemaakt wordt. Men gebruikt tegenwoordig veelal Whatsapp, Facebook Messenger of Telegram voor het versturen van berichten. Veel sms'sjes versturen in korte tijd wordt daardoor al snel gezien als afwijkend sms gedrag. En afwijkend sms gedrag kan duiden op een geautomatiseerd proces of een besmetting met Flubot malware. En dit is weer in strijd met de gedragsregels, dus wordt je uit voorzorg geblokkeerd. Contact met de afdeling Credit Risk is dan aan de orde om te achterhalen wat het sms gedrag veroorzaakt en om de blokkade op te heffen, natuurlijk.

Ik kan begrijpen dat ik uit voorzorg voor een flubot malware geblokkeerd word, maar niet dat als ik aangeef dat ik het zelf ben, en niet een malware of geautomatiseerd proces, deze blokkade er niet permanent afgehaald wordt. Om steeds weer contact op te nemen met de Credit Risk afdeling is niet praktisch en kan 's-avonds ook niet (m.u.v. donderdag en vrijdag).

Wat anderen gebruiken voor het versturen van berichten verandert het feit niet dat onbepikt ook écht onbepikt zou moeten zijn volgens de website. Als ik steeds weer moet bellen (wat dus niet altijd kan, en het kost alleen al moeite om überhaupt iemand aan de lijn te krijgen) om weer te kunnen SMS'en is dit níét onbepikt.



Dit is niet wat je van ons mag verwachten. Mijn excuses voor deze rare ervaring met de telefoonlijn! Ik ben bang dat ik hier weinig aan kan veranderen, maar ik kan wel voor je uitzoeken wanneer je een telefoontje kunt verwachten. Ik heb momenteel alleen nog geen gegevens van je. Zou je je [forumprofiel](#) willen aanvullen met jouw 06-nummer, postcode, huisnummer, geboortedatum en klantnummer? Jouw mobiele nummer kan je invullen onder 'persoonlijke opmerkingen'. De gegevens in jouw profiel zijn alleen zichtbaar voor jou en de moderators. Geef je hier een seintje als je jouw profiel hebt ingevuld?

Ik heb de gegevens zojuist in m'n profiel gezet.

👍 Like ➦ Quote

 **KPN Moderator** • 5178 reacties 5 maanden geleden

Bedankt voor jouw gegevens. Ik lees in het systeem dat mijn collega's van credit risk vallen over het hoge aantal sms'sjes in korte tijd. Dit valt volgens hun niet binnen eigen, redelijk en normaal gebruik. Helemaal als je bedankt dat sms tegenwoordig weinig wordt gebruikt. Mag ik vragen waarom jij zoveel sms's? Als het voor zakelijke doeleinden is, dan raad ik je een zakelijk abonnement aan. Daar heb je andere voorwaarden. En zou je dus minder met blokkades te maken moeten hebben.

—

"There is a defiance in being a dreamer" — V.E. Schwab, *The Invisible Life of Addie LaRue*

👍 Like ➦ Quote

<https://forum.kpn.com/mobiel-15/flubot-malware-blokkade-na-het-versturen-van-veel-sms-sjes-let-op-sms-verbruik-hoger-dan-normaal-556707>

5/7

Figure K.5: Criticism on the rigorousness of the SMS auto block in the KPN forum, page 5