Teaching Empirical Social-Science Research to Cybersecurity Students The Case of "Thinking Like a Thief"

Barth, Susanne; Hartel, Pieter; Junger, Marianne; Montoya, Lorena

DOI
10.1109/MSEC.2018.2888781

Publication date
2019

Document Version
Accepted author manuscript

Published in
IEEE Security & Privacy Magazine: building confidence in a networked world

Education

Teaching empirical social science research to cyber security students. The case of "Thinking like a thief"

Susanne Barth, University of Twente

Pieter Hartel, Delft University of Technology and University of Twente

Marianne Junger, University of Twente

Lorena Montoya, University of Twente

We report on an educational experiment where computer science students perform empirical research into the human factor in cyber security. Most courses restrict students to work in a lab environment, but we encouraged our students to conduct a realistic experiment with real-world subjects. The students wrote a research proposal that had to be approved by the IRB. They then executed the proposal, collecting and analysing the data. Finally the students wrote and presented a paper a student conference. The main method of assessment is by peer-review. After teaching the course for six years, we report on the exciting ideas our students came up with, and on the lessons we learned in teaching the course. The main conclusions are (a) offering complete freedom to choose research topics inspires students to design creative projects, (b) working with real subjects creates a stimulating learning experience, and (c) peer-review is a useful assessment tool.

K.3 COMPUTERS AND EDUCATION, K.4.1 Public Policy Issues (Abuse and crime involving computers), K.6.5 Security and Protection.

Background

Cyber security is a multidisciplinary field straddling the technical and the social sciences[9]. Accordingly, cyber security students learn about the role the human factor plays in cyber security[11]. For the cyber security program of the 4TU, the federation of the four Dutch technical universities (see https://www.4tu.nl/cybsec/), we developed and taught a course on the human factor in cyber security. We based the content of the course on the principles of crime science. The main reason for that choice is the focus of crime science on empirical research into countering crime[5]. We believe that an emphasis on empirical social science research will be particularly fruitful for students' future cyber security careers.

Crime science and cyber security have in common that "thinking like a thief" often leads to insights. In the computing literature, this is called adversarial thinking. It is the offender who is looking for ways to misuse a design; hence the prudent designer is well advised also to think like a thief. An illustration of what this might entail is the ordinary beer glass, which, when broken, becomes a lethal weapon. Hence, a designer who has been thinking like a thief uses laminated glass that does not break[7]. This example highlights not only the approach shift but also the multi-disciplinary approach that crime science involves.

Cyber security curricula across the world offer a variety of courses on adversarial thinking[3]. However, the majority of cyber security courses focus on the technical aspects of adversarial thinking, for example cryptanalysis (mathematics), kernel hacking (systems), and red-blue teaming (networks)[1]. In almost all courses that take the human factor into account the students are either pitted against each other, or work in a laboratory setting. We believe that a realistic setting would significantly improve the learning experience. There is, of course, a good reason to make student work in a lab setting: the ethical and legal issues of real research are thorny and time consuming[2].

The students of our course are asked to conduct and document a real experiment in the real world. This requires our students to seek approval for their research proposal from the Institutional Review Board (IRB). Students acquire valuable experience by going through the process of interacting with the IRB. We have not found reports in the computing literature on courses that also provide student with first-hand experience of working with an IRB.

Performing realistic empirical social science research with high quality results gives the students the best possible learning experience. However, if the results are disappointing, the learning experience will be poor. Therefore we set out to investigate -- and if possible to control -- factors influencing the quality of the student work.

The quality influencing factors that we considered were (1) the amount of time available for the course, (2) factors that the teachers control, (3) factors that the students control, and (4) factors that neither control.

The indicators of the quality of the student works that we considered were (a) random allocation of subjects, (b) statistically significant results, and (c) publication quality of the papers. More specifically, we were interested in the following questions:

(1) Is a *learning by doing course*, in the form of an experimental design with high quality results manageable within 5 EC (= 140 student hours)?
(2) How do factors that the teachers control, such as *improvements to the course content over the years*, influence the quality of the results?
(3) How do factors that the students control, such as *choice of research method, and choice of topic* influence the quality of the results?
(4) How do factors that neither the teachers nor the students control, such as *group diversity* influence the quality of the results?

To answer these questions we analysed the student papers, we used surveys completed by the students, and we interviewed the students. In the rest of this section we discuss each of the quality influencing factors mentioned above in more detail.

Learning by doing course

Our Cyber-crime science course is a 5 European Credit (= 140 student hour) one-semester course for computer science master students specialising in cyber security. The learning outcomes of the course are:

- A good understanding of the theoretical principles of crime science;
- A good understanding of the psychological issues of cyber security;
- An appreciation of the spectrum of different cyber crimes;
- Skills necessary to research cyber crime prevention measures.

Throughout the course, the students work towards a conference where they present a research paper on a topic of their own choice. Assessment is done entirely by peer-review, moderated by the lecturers.

During the first eight weeks students attend weekly lectures on crime science, cyber crime, and social science research methods. At the same time, teams of normally three students draft a research proposal for a cyber crime prevention project of their choice. Students are completely free to choose a topic for their research. After two rounds of feedback by their peers and the lecturers on the research proposals, the teams submit their projects to the IRB. In cases where deception is involved, the students often have to modify their proposals, and in case the IRB refuses permission, students have to develop alternatives.

Upon approval of the IRB, the students execute their projects. Ultimately, this results in a six-page paper based on the American Psychological Association (APA) guidelines. The papers are presented at a half-day conference at the end of the semester. The students peer-review each other's papers and presentations, moderated by the lecturers. Finally the students complete a questionnaire on their experience. The *first aim* of the present paper is to present a description of students' studies and some global evaluations. In addition, we test some hypotheses, which are developed below.

Improvements to the course contents over the years

During the early years of the course we found that computer science students needed more help to perform social science research than we had anticipated. In subsequent course iterations, we increased the number of lectures devoted to social science research methods and decreased the number of lectures devoted to other topics. We also introduced clinics where students could get advice. Thus we changed from a passive to a more active, trouble-shooting form of social science research methods delivery. Therefore, we were interested in the extent to which our cyber security students apply standard social science research methods[15]. Do students use random selection of subjects for the control group? Do they analyse the data and check for statistically significant results? Our *second aim* is therefore to investigate whether there are differences between the papers of the first three years compared to those of the last three years reflecting the increased focus on the social perspective.

Choice of research method and choice of topic

Since crime science emphasizes experimental work, we encouraged students explicitly to develop their own intervention and to test it in an experiment. The *third aim* is to examine whether the topics chosen by students involved an experiment or a survey.

Group diversity

Group diversity plays an important role in education. Since our students are free to choose their teammates we thought that group diversity might explain some of the performance differences between the teams. Studies have shown that gender stereotypes[8], and national and cultural differences[13] can be an issue for collaborative learning. In this study we assume that gender and nationality are an acceptable proxy for group diversity. There are no significant language differences in the 4TU master program as the teaching language is English in a non-English speaking country. Accordingly, our *final aim* is to investigate differences between homogenous male teams and teams that include at least one female student, as well as differences between homogenous Dutch teams and teams that include at least one international student. The student population of the 4TU master course contains about 30% international students from many countries around the world.

Method

To measure the factors that influence the quality of the student work and the quality of the work itself, we collected three data sets. The first data set consists of the research papers written by student teams. The second data set consists of course evaluation questionnaires completed by students who attended the course. The third data set consists of a small number of structured interviews with students who completed the course.

The IRB of the faculty of electrical engineering, mathematics and computer science at the University of Twente approved the present study under nr Rp-2017-55.

Student papers

The student papers were coded using three independent variables: gender, nationality, and year, and four dependent variables: applied research method, sample randomisation, statistical significance tests, and chosen research topic.

Background of the students:

- Gender was coded as 0 when at least one female participated in the group, and 1 when the group consisted of males only.
- Nationality was coded as 0 when at least one international student participated in the group, and 1 when the group consisted of Dutch students only.
- Year was coded year as 0 for the early years (2012, 2013, 2014), and 1 for later years (2014, 2015, 2016).

Quality of the results:

- Method was coded as 0 for a survey and 1 when students performed an experiment to test an intervention.
- Randomisation was coded as 0 when the student researchers assigned subjects to the control group, 1 when they had not controlled the subject assignment, and 2, in the case of surveys, i.e. not applicable.
- Statistical significance tests was coded as 0 when significant results were reported, 1 when the student researchers either argued, typically due to a limited data set, that no significant results would be possible or when they did the analysis and found no significant results, or 2 when no statistical analysis had been performed.

The fourth dependent variable describing the topics of the papers was coded as follows:

- 0 for projects on illegal activity reduction. This required the subjects in the project to engage in (simulated) illegal activity, such as illegal downloading, littering, illegal parking, or using fake IDs.
- 1 for studies on password usability improvement. This required subjects to select, enter, remember, or recover passwords.
- 2 for research on raising awareness of phishing risks.
- 3 for studies on raising awareness of privacy risks. Studies on raising awareness required subjects to interact via communication means (i.e. email, Facebook, face-to-face, brain computer interfaces, web cams, Geo-tagged photos, or QR codes) by means of hardware or software provided by the student researchers.
- 4 for research on raising awareness of security risks. This required subjects to interact with deliberately poorly managed hardware or software, such as wireless access points, drive by downloads websites, fake login screens, face adverts, phone charging stations, unattended laptops, out-of-date software, or lost USB sticks.
- 5 for threat assessments. To demonstrate to what extent it is possible to use the information for illegal purposes, subjects were ask to surrender information via a variety of methods. Examples include Tor exit nodes to de-anonymise traffic, Wi-Fi access points to access them illegally, Wi-Fi enabled devices to break into homes, online social sports sites to break into homes, online sources to confront subjects with the info, or online sources to create fake ids.
- 6 for victimization studies. In these projects the subjects are targets of a form of cybercrime, such as harassment, or ransom ware.

Student surveys

At the end of the course, students were asked to complete a course evaluation questionnaire. We took inspiration from the Intrinsic Motivation Inventory scale (IMI)[6] for the wording of the survey questions. We did not use the IMI scale itself, as we did not want to overload our students with questions and we reworded the questions to fit our study better. As with the IMI scale, the subjects were asked to indicate on a 5-point scale (from 5=strongly disagree to 1=strongly agree) their level of agreement on a set of propositions:

- I had sleepless nights for fear of our experiment going wrong. (11)
- I had to work harder than average on the course. (3)
- The course has increased my interest in social science research. (8)

- I am confident that, during my career, I will be using what I have learned during the course. (14)
- I will never forget the course. (4)
- I had a lot of fun doing the experiment. (7)
- I am less likely to fall for a social engineering attack. (not related to the IMI scale because this is not a motivation)

The numbers in parentheses refer to the corresponding IMI items[6]. The independent variables were code as described in Section "student papers" above.

Student interviews

We invited all 30 students who attended the last edition of the course for a one hour structured face-to-face interview. The main purpose of the interviews was to investigate the effect of diversity on student performance, we wanted to give the interviewees some guidance. For this, we used the six constructs of the Intercultural Effectiveness Scale (IES)[12]. These constructs are: adaption to new situations (e.g. feeling comfortable/ uncomfortable while interacting with people from other cultures), foreign language skills (e.g. proper use of English language); distance (e.g. difficulty or easiness to interact with people from other cultures); expression (e.g. difficulty or easiness to follow conversations in a foreign language); respect (e.g. paying attention to cultural differences while interacting with people from other cultures); being relaxed (e.g. feeling relaxed while interacting with people from other cultures). We printed the given description of each construct on a card and placed the six cards before the interviewee.

We asked the interviewees eight open questions focussing on decision making within their student teams. We asked why these decisions were made and whether the six IES constructs had played a role in the decision-making process. The questions that we asked the students were:

- Which nationalities were represented in your team (including your own)?
- Which topic did your team choose?
- Did your team decide to conduct a survey or an experiment?
- Did your team decide to analyse the statistical significance of the data?
- Did your teamwork influence your interest in social science research?
- Did working in the team influence your study progress?
- How did your teamwork influence your ability to withstand social engineering attacks?
- Is there anything else that you would like to mention about your experience in the team?

The interviews were recorded and each interviewee received 10 Euros for his/her time.

Results

We describe the results of the data collection and analysis of the three data sets for each of the four quality influencing factors.

Learning by doing course

Analysis of the student papers shows that over the past six years, 196 students (158 male, 38 female; 124 Dutch, 72 international) wrote 72 papers (44 experiments, 28 surveys) in teams of usually three but sometimes two students, and in one case four students. In each academic year students produced between 8 to 19 papers, 29 in the first three years, and 43 in the last three years. One study was based on only N=4 subjects, and the maximum number of subjects was N=762. From the 72 teams, 28 teams contained at least one female, and 38 teams contained at least one international student. Phishing was the topic chosen most often

(27.8%), followed by security awareness (25%), and the usability of passwords (13.9%). Reduction of illegal behaviour and privacy awareness were both chosen by 11.1% of the teams. Threat assessments (8.3%) and victimization studies (2.8%) were chosen the least. All papers were coded by one of the authors and a random selection of seven papers (10%) was coded by one of the other authors. Out of the 49 items (i.e. 7 papers x 7 variables), the two coders had different opinions on 4 items (8%). After discussion, the two coders agreed that the differences were all due to coding errors and not due to different understanding about these items.

Analysis of the student surveys shows that over the past six years, 124 students (100 male, 24 female) out of the total population of 196 students (response rate 63.2%) completed our survey. The majority were Dutch (65.9%). The international students originate from 34 different countries across the world. The respondents of the surveys did not agree nor strongly agree with the first two propositions: 64.5% of the students did not have sleepless nights, and 54.8% did not work harder than in other courses. The students agreed or strongly agreed on the remaining propositions. For 52.4% of the students, the course raised interest in social science research, 56.5% felt that they would be using what they had learned in their future career, 60.5% would not easily forget the course, 62.9% had fun, and 47.6% are now better prepared to face social engineering threats. Cronbach's alpha for the 7-item scale from the survey was 0.7, showing that our combined measure is reliable.

Analysis of the student interviews shows that out of the 10 teams taking part in the last edition of the course, representatives of four teams accepted to be interviewed (40%). Two interviewees represented all-male, all-Dutch teams and two interviewees represented teams with at least one international student. One of the interviewees was female.

Improvements to the course contents over the years

Analysis of the student papers shows that during the last three years students investigated statistical significance more often than in the first three years (Table 1). This was a significant result. Students did also randomise the control group more often in later years but this was not statistically significant.

Table 1 Results of student studies were statistically significant by course iteration.

Statistically significant results have been found.	*First three years*	*Last three years*
Yes	23.3%	44.8%
No	25.6%	41.4%
Not investigated	51.2%	13.8%
N	43	29

Chi-Square=10.6, df=2, p=.005

Analysis of the student surveys shows that the opinion of the students on the course did not differ significantly year-by-year with one exception. Table 2 shows that during later years students thought they would be more likely to fall for social engineering attacks than during early years.

Table 2 Susceptibility to social engineering attack by course iteration.

I am less likely to fall for a social engineering attack.	*First three years*	*Last three years*
Strongly agree or agree	52.8%	34.4%
Neutral	16.9%	34.4%
Strongly disagree or disagree	30.3%	31.4%
N	89	35

Chi-Square=5.3, df=2, p=.070

The student interviews did not provide new insights into the improvements of the course over the years.

Choice of research method and choice of topic

Analysis of the student papers shows that there was a significant relationship between the chosen topic and the research method used (Table 3). Some topics were studied more often using experiments (e.g. phishing) and some more often through surveys (e.g. threat assessments).

Table 3 Choice of topic by research method.

Choice of topic.	*Survey*	*Experiment*
Reduce tendency to illegal activity	3.7%	15.6%
Study or improve the usability of passwords	18.5%	11.1%
Increase awareness of phishing risks	14.8%	35.6%
Increase awareness of privacy risks	11.1%	11.1%
Increase awareness of security risks	25.9%	24.4%
Threat assessments	18.5%	2.2%
Victimisation studies	7.4%	0.0%
N	27	45

Chi-Square=14.1, df=6, p=.028

Table 4 shows that in later years the number of experiments increased and the number of surveys decreased. This was a significant finding.

Table 4 Surveys vs. experiments by course iteration.

Applied research method.	*First three years*	*Last three years*
Survey	46.5%	27.6%
Experiment	53.5%	72.4%
N	43	29

Chi-Square=2.6, df=1, p=.011

The student surveys and interviews did not provide new insights into the choice of research method and the choice of topic.

Group diversity

The analysis of the student papers also indicated that there were no significant differences by gender or nationality. The only point worth noting is that all-male, all-Dutch groups carried out all six threat-assessments.

Analysis of the surveys indicated that gender or nationality differences did not significantly influence student opinion scales with one exception: international students reported that their interest in social science research had increased, but Dutch students did not (Table 5).

Table 5 Increased interest in social science research by nationality.

The course has increased my interest in social science research.	*International students*	*Dutch students*
Agree	77.5%	40.2%

Neither agree nor disagree	17.5%	34.1%
Disagree	5.0%	25.6%
N	40	82

Chi-Square=15.8, df=2, p<.005

Analysis of the interviews shed light on group diversity issues. The interviewees agreed that the six IES constructs had more influence on the interaction between the team and their subjects than on the team itself. In particular all interviewed teams had given considerable attention to formulating their questionnaires, briefings, and informed consent forms, in plain English and sometimes also in plain Dutch. The IES constructs did not influence the decision making of the teams, with one exception: the only native English speaker in the class used a more elaborate form of English than his teammates could handle. During the interviews students stated that cultural factors did not affect them or the way their group had functioned.

Discussion

We will now discuss the four factors that influence the quality of the student works in detail.

Learning by doing course

Three of the student papers contained sufficient original ideas to be published after a thorough revision. We briefly summarise these papers.

- The first paper[14], by two Dutch students, investigated show easy it is to discover the home address of subjects from their web presence. Thinking like a thief, the students hypothesized that people are more likely to “leave their tracks” on a social sports site if they feel proud of an achievement. The students collected the Runkeeper (see https://runkeeper.com) profile of 304 subjects, and calculated the home address from the set of tracks of each runner. Since most people start running from home, and stop running to cool down close to home, the address could be determined accurately in most cases. The students then tried to obtain the home address also from other sources, such as the Facebook profile of the runners. Discovering the home-address from Runkeeper profiles was twice as successful as from Facebook. This work has been revised by one of the supervisors and was published in a scientific journal.
- The second paper[4], by one international and two Dutch students, researched the effect of anti-phishing training on 159 school children, aged between 9 and 12. There was a statistically significant difference between the experimental group, which received training and the control group, which did not receive training. This work has been revised by one of our PhD students and has won the distinguished paper award at the 2017 ACM SOUPS conference.
- The third paper[10], by three Dutch students, presents an experiment where passers-by on one of the main squares in a small city were approached to participate in survey. Subjects were randomly assigned to the control group (25 subjects) or the experimental group (22 subjects). The survey for the experimental group included some questions designed to raise awareness about phishing. Subjects in the experimental group did significantly better than the control group. A student not involved in the original work collected a new data set, analysed the results and rewrote the paper. The paper was published in a scientific journal with an ISI impact factor of 3.435.

These three publications indicate that mastery of social science research skills applied to crime prevention is within reach of students. The three published papers were innovative, and one was even worthy of an award at the top conference in the field. The three publications also indicate that it is not only feasible to allow students to perform experiments in the real world, but that this may lead to high quality results as well. With proper guidance and sufficient revision, computer science master students are indeed able to conduct research during a 5 EC course that is worthy of publication. We believe that the learning experience with such a result is tremendous.

Improvements to the course contents over the years

During the last three years student researchers performed more experiments and analysed the statistical significance more often than in the first three years. These differences are significant; hence we may conclude that the delivery of social science research methods has been improved over the years.

What has deteriorated is the self-reported ability of the students to resist social engineering. This difference is also significant. We think that the two changes are related. Shifting the attention from crime science to social science research methodology also diverts the attention from the main tool employed by offenders: social engineering. The challenge therefore is to maintain a good balance between content and form. We are trying to achieve this by explicitly commenting on methodological issues when we present papers from the literature in our lectures.

Choice of research method and choice of topic

Consistent with the course aims, the number of experiments (44) exceeded the number of surveys (28). This is a significant finding; hence it indicates that within the constraints of a one semester 5 EC course, it is possible to perform a (cyber) crime prevention experiment from start to finish.

Some topics were studied more often in experiments (phishing) and some more often in surveys (threat assessments); this was a significant finding. While, in principle, all topics are amenable to experimentation, doing so within the time constraints of a 1-semester course remains a challenge.

The students who were interviewed wanted to develop an intervention and conduct a proper experiment to measure objectively whether the intervention worked. They did not consider a survey as rewarding. One of the interviewees stated that:

> *Surveys are boring. It's difficult to get the sample. Field experiments help you to find out what the problem is in the real world.*

One interviewee explained that the choice of topic requires considerable time and dedication. He stated, that his teammates had opposing views on a specific technology (two-factor authentication, 2FA). Some team members used 2FA all the time, and some never. The team decided to study whether the population at large held also opposing views. We believe that it is important to allow the students sufficient time to choose a topic that they are all genuinely interested in.

Group diversity

There were no significant differences by gender or nationality on team performance. Also, in the interviews, students were of the opinion that cultural factors neither affect them, nor the way their group functioned. Instead students indicated that different skill levels were relevant. One of the interviewees stated that:

> *The different skill sets in the team were a factor. One person did not have any data analysis skills. The cultural differences did not have an influence.*

International students reported that their interest in social science research had increased, but Dutch students did not; this difference is statistically significant. The course did not include any training to withstand social engineering, so an improved resilience to social engineering cannot be due to the course material. The interviewees said that they learned a lot about social engineering from the work of their peers. One of the interviewees commented that:

The experience made me realise that a lot of people around me do not understand that social engineering is a valid attack vector. That was a very good education experience.

We believe that our International students are well adapted to the way of working in the Netherlands because most of them have been in the country for at least half a year and some considerably longer.

Limitations

The subjects of this study are 196 students from four Dutch universities. The majority is Dutch but the International students from 34 different countries represent a large minority. Ours is therefore a study of moderate size. Our results may not be representative for all countries and for all higher education organizations due to the international nature of the university where the study was carried out.

We have used a small subset of the items of the IMI scale, which does not necessarily preserve the validity of the scale.

One of the limitations of teaching related research is that the students are also subjects of this study and the lectures are also researchers of this study. To reduce the risk of politically correct answers, the surveys and interviews have all been taken after the students received their marks.

Conclusions

The main lessons learnt were:

- It is possible within a 5 EC one-semester course for computer science students to conduct social science research that lays the foundation for high quality publications. Three out of the 72 student papers were eventually published after heavy revision.
- Giving students the freedom to choose the topic they wish to research creates a stimulating learning experience.
- There is no significant effect of gender or nationality difference on student performance.
- Teaching engineers about social science research methods broadens the students' view, as it forces them to consider the point of view of others rather than just their own view or that of their immediate peers.
- During the entire course, students are peer-reviewing each other's work. The final mark is determined by peer-review (moderated by the lecturers). We believe that this helps students to learn more from each other than from a traditional lecturer-student interaction.

We offer the following recommendations for teachers of similar courses:

- Include social science research methods in a cyber security curriculum, as cyber security professionals do have to deal with the human factor. Ideally this should be a separate course, but a combination with a course like ours that focuses on cyber crime is an alternative.
- Because students have complete freedom to choose their own research topic, projects can vary a lot. Accordingly, personal attention is important. Therefore we suggest providing regular feedback to the students on their progress, for example by hiring teaching assistants with a social science background who regularly meet with each student team separately. We believe this is important to make a success of each study.
- A social science research methods course should include an experiment where the students themselves are the subjects. This will help them understand the fine points of

research ethics.

- Discuss the student proposals with a representative of the IRB before the students submit their proposals to avoid unnecessary delays.
- Provide the students with checklists to make sure that they do remember to provide the IRB with every relevant detail.
- Smoothen the path through the IRB by preparing a small set of standard applications, such as an online survey, an awareness campaign, and a usability study. Most students will then be able to follow a standard approach and avoid common mistakes.
- Work with the IRB to implement a fast-track procedure for approval of standard experiments to maximize available time and reduce burden on institutional ethical bodies.
- Create an inventory of logistical mishaps from previous experiments to increase the probability of success for new experiments.

After six iterations, we are still keen to improve our course. We are currently considering the following questions:

- Students generally prefer to select their own teammates. This tends to create homogenous groups, which, according to the literature can be less creative than non-homogeneous groups. We are looking for ways promote group diversity without annoying the students.
- We would like to integrate the cyber crime teaching better with the social science research methods. For example we are explicitly commenting on the research method when we discuss cyber crime studies from the literature.
- Some studies are harder to do with informed consent than without, because signing the informed consent may bias the subject. We are looking for ways to reduce the risk of bias.

We hope that this article will help others with similar aims, and that we may hear from other teachers who have solved similar problems.

References

1. G. Conti, T. Babbitt, and J. Nelson. Hacking competitions and their untapped potential for security education. IEEE Security & Privacy, 9(3):56-59, May 2011. http://dx.doi.org/10.1109/MSP.2011.51.
2. B. Endicoytt-Popuvsky. Ethics and teaching information assurance. IEEE Security & Privacy, 1(4):65-67, Jul 2003. http://dx.doi.org/10.1109/MSECP.2003.1219073.
3. M. Gondree, Z. N. J. Peterson, and T. Denning. Security through play. IEEE Security & Privacy, 11(3):64-67, May 2013. http://dx.doi.org/10.1109/MSP.2013.69.
4. E. Lastdrager, I. Carvajal Gallardo, P. H. Hartel, and M. J. Junger. How effective is Anti-Phishing training for children? In 13th Symp. on Usable Privacy and Security (SOUPS), pages 229-240. USENIX, Jul 2017. http://www.usenix.org/conference/soups2017/technical-sessions/presentation/lastdrager.
5. G. Laycock. Defining crime science. In M. J. Smith and N. Tilley, editors, Crime science: new approaches to preventing and detecting crime, pages 3-24. Willan Publishing, Uffculme, UK, 2005.
6. E. McAuley, T. Duncan, and V. V. Tammen. Psychometric properties of the intrinsic motivation inventory in a competitive sport setting: a confirmatory factor analysis. Research Quarterly for Exercise and Sport, 60(1):48-58, Mar 1989. http://dx.doi.org/10.1080/02701367.1989.10607413.
7. C. McGinley and C. Till. Design Out Crime: Using design to reduce injuries from alcohol related violence in pubs and clubs. Design Council, Mar 2010. http://www.designcouncil.org.uk/sites/default/files/asset/document/design-out-crime-alcohol.pdf.
8. L. A. Meadows and D. Sekaquaptewa. The influence of gender stereotypes on role adoption in student teams. In Engineering Education: Frankly, We Do Give a D*mn, page Paper 6744, Atlanta, Georgia, Jun 2013. American Society for Engineering Education, 2013. https://www.asee.org/public/conferences/20/papers/6744/view.
9. L. I. Millett, B. Fischhoff, and P. J. Weinberger, editors. Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions. The National Academies Press, Washington DC., 2017.https://www.nap.edu/catalog/24676/foundational-cybersecurity-research-improving-science-engineering-and-institutions.

10. M. Junger, A. L Montoya, and F.-J. Overink. Priming and warnings are not effective to prevent social engineering attacks. Computers in Human Behavior, 66:75-87, Jan 2017. https://doi.org/10.1016/j.chb.2016.09.012.
11. S. L. Pfleeger and D. D. Caputo. Leveraging behavioral science to mitigate cyber security risk. Computers & Security, 31(4):597-611, Jun 2012. http://dx.doi.org/10.1016/j.cose.2011.12.010.
12. T. Portalla and Guo-Ming Chen. The development and validation of the intercultural effectiveness scale. Intercultural Communication Studies, 19(3):21-36, 2010. http://web.uri.edu/iaics/2010-vol-19-no-3/.
13. J. B. Shaw. Fair go for all? the impact of intragroup diversity and diversity-management skills on student experiences and outcomes in team-based class projects. J. of Management Education, 28(2):139-169, Apr 2004. http://dx.doi.org/10.1177/1052562903252514.
14. B. Stottelaar, J. Senden, and A. L. Montoya Morales. Online social sports networks as crime facilitators. Crime Science, 3:Article 8, 2014. http://dx.doi.org/10.1186/s40163-014-0008-z.
15. J. Taylor, J. McAlaney, S. Hodge, H. Thackray, C. Richardson, S. James, and J. Dale. Teaching psychological principles to cybersecurity students. In Global Engineering Education Conf. (EDUCON), pages 1782-1789, Athens, Greece, Apr 2017. IEEE. http://doi.org/10.1109/EDUCON.2017.7943091.

Susanne Barth is PhD candidate at the University of Twente. Her research interests are cyber security and privacy, and usability testing. Contact her at s.barth@utwente.nl

Dr Pieter Hartel is professor of cyber security at Delft University of Technology and at University of Twente. His research interests are crime science, cyber crime, and block chain technology. Contact him at pieter.hartel@tudelft.nl

Dr Marianne Junger is professor of cyber security and business at University of Twente. Her research interests are cyber crime, crime science, and the human factor. Contact her at m.junger@utwente.nl

Dr Lorena Montoya is coordinator of the Graduate School at University of Twente. Her research interests are risk in general, and crime prevention and disaster management in particular. Contact her a.l.montoya@utwente.nl