

# Student Perceptions of Ethics in Cybersecurity Education

Timo Hynninen<sup>1</sup>

<sup>1</sup>*Laurea University of Applied Sciences, Vanha Maantie 9, Espoo, 02650, Finland*

## Abstract

Ethical considerations are of growing interest in the computing education field. In particular, cybersecurity is a field where a strong moral compass is required. Cybersecurity education is often recommended to use an offensive approach as this has been demonstrated to lead to better learning results. At the same time, we must consider how students perceive the skills and knowledge gained from the offensive approach. This paper presents a case study of organizing a cybersecurity basics course for computing students using mainly an offensive approach. At the end of the course, we asked the students to reflect on their learning and what they gained from the course. As such, a thematic analysis of the 110 student reflections was conducted to find out how ethical issues are perceived by the students. We found that most students describe their learning as raised awareness of cybersecurity threats, and knowing defenses for them. While some students wrote to have learned practical hacking skills and tricks, the majority described the lessons learned in an ethically sound way. It was also noted that adding reflection questions to the learning tasks throughout the course may have increased the number of ethical considerations in the student reflections of learning.

## Keywords

cybersecurity education, hacking, ethics

## 1. Introduction

The author of this paper has taught cybersecurity in higher education for almost a decade. The teaching method has combined offensive skills (i.e. hacking) with defensive tactics to illustrate how cyberattacks work. In my experience, this has been an effective and motivating approach for students. The objectives of the cybersecurity courses have focused on how to defend against attacks but nevertheless, some of these skills and knowledge picked up along the way *could also be* used for illicit purposes. Some researchers have argued that the ethical considerations of hacking and security education must be carefully considered (e.g. [1, 2]). As the personal experiences of the author (and similar practices of many colleagues in the computing education community) are somewhat tangential to the research on the ethical stance on teaching hacking skills, perhaps there is a need for a deeper investigation of how these skills and knowledge are perceived by students.

Including offensive activities to gain hands-on cybersecurity skills and knowledge is common in computing education [3]. In general, hacking skills are considered an essential component


---

*Conference on Technology Ethics - Tethics, October 18–19, 2023, Turku, Finland*

✉ [timo.hynninen@laurea.fi](mailto:timo.hynninen@laurea.fi) (T. Hynninen)

🆔 0000-0002-1354-001X (T. Hynninen)

© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

📄  CEUR Workshop Proceedings (CEUR-WS.org)

of computing education [1] as they help students gain a better understanding of computer and information security [4]. The argument for teaching hacking skills and knowledge in technology education is straightforward: For example, Radziwill et al. [1] state, that "regardless of whether or not students are taught hacking skills, hackers will still exist," therefore having the knowledge is paramount for defending oneself in the digital age.

At the same time, many researchers and educators argue for a better alignment of ethics in the teaching of such 'unethical' skills. Some claim that teaching hacking techniques could cause institutions to be faced with ethical and legal dilemmas (for example, see Hartley et al. [5, 6] and Curbelo & Cruz [7]). Additionally, some argue that teaching students how to hack could have negative consequences such as causing them to become cybercriminals (e.g. Smith et al. [2]). However, these claims seem to be mostly anecdotal, and not much evidence supporting them exists in the computing education literature (to our knowledge). In addition, cybersecurity (and other) education usually covers also legal and ethical implications of hacking [8].

Cybersecurity educators often employ hacking and offensive skills because an offensive approach to the topic leads to better learning results [9]. This prompts the question: Is the offensive approach sufficient enough in terms of the ethical (and legal) repercussions? Are there potential problems regarding ethics with this approach?

The current paper presents an empirical case study investigating how students perceive ethical considerations of hacking or offensive technology skills in a cybersecurity course. To achieve this goal, 110 student reflections from four consecutive years of teaching the course were analyzed using the thematic analysis method. The objective is to gain a perspective into *how ethical considerations manifest in the students' descriptions of what they learned*. Thus the following research questions were formulated:

- To what extent do written student reflections depict ethical considerations?
- What ethics-related issues emerge from the reflections?
- How to mitigate these issues?

This paper is organized as follows. Section 2 presents extant literature on the ethical considerations of hacking and cybersecurity education. Section 3 presents the research methods and context of the study. Section 4 presents the findings which are then discussed in Section 5. Finally, Section 6 concludes the paper.

## 2. Related work

The extant work in cybersecurity education is well-established in the literature. The body of knowledge is detailed in several literature reviews, for example: [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 9, 21, 22, 23, 24, 25, 26, 27, 28]. In general, hacking skills and offensive approaches to teaching security are commonplace.

Offensive skills as part of ethical hacking are taught in cybersecurity programs to help students protect themselves from the dangers of cybercrime. The practical skills associated with hacking or cybersecurity are not easily learned by students on their own, so it is important for schools to include ethical hacking in their curricula [1, 29, 30, 8].

In terms of the negative stance on teaching hacking in schools, Radziwill et al. argue that providing young people with the tools and knowledge of accessing secure networks while not necessarily having developed skills in ethical reasoning is dangerous [1]. This concern can also be seen in faculty attitudes and opinions on teaching offensive approaches to security [7]. Pike [30] states point-blank that hacking draws students toward criminal acts. Sometimes hacking curriculums are even described as undocumented sets of tips and tricks [31].

Similarly, teaching offensive skills or hacking skills can at times be perceived by non-professionals as ethically unsound, or even banned by university administration [5]. Cybersecurity professionals also share this concern to a degree; For example, the study of Smith et al. on teaching ethical hacking to students calls for "instructors to instill correct knowledge of laws concerning hacking and their repercussions" to students [2]. In a similar vein, the study of Logan and Clarkson concludes that 'instructors should carefully consider the design of all "red team" (offensive) exercises' [3]. However, the most vocal studies on the dangers of teaching hacking are based on the opinions of security professionals (i.e. Pike [30]) or faculty (i.e. Curbelo & Cruz). Thus, the voices in extant literature have been mostly anecdotal, and do not portray how students would use these skills and knowledge.

The offensive approach is generally considered more effective in students achieving learning outcomes [5, 6, 32]. Many educators believe that institutions should teach ethical hacking to undergraduate students [3, 32, 7, 33]. For example, Wilson [33] argues that security awareness and defense can and should be taught through offensive tactics. Likewise, Trabelsi & McCoe state that offensive methods are becoming a must for security curricula [34]. In a similar vein, Patrignani & Kavathatzopoulos argue that teaching of technology is also teaching of ethics [35].

Hacking and an offensive approach can be used to motivate students, even in non-cybersecurity topics [36, 3]. Conti et al. suggest that hacking competitions are an untapped resource in security education [37]. Dimkov et al. even challenged their students to break into offices and steal faculty laptops from the campus and found that their hands-on assignment increased the students' awareness of security mechanisms [36]. Students did not perceive the exercises described in Dimkov et al. as harmful, although they were not seen as particularly useful either [36]. This suggests that the best assignment for students is not only hands-on but also incurring knowledge that is applicable in everyday life.

Some research articles have explicitly discussed the ethical considerations in cybersecurity education. Logan & Clarkson [3] explore the potential ethical problems of introducing "red teaming" and attack-based exercises into information security courses. However, most students are unaware of the university's acceptable use policies, and thus, students should only train offensive activities under supervision [3]. Pashel [8] discusses the ethical nature of teaching computer students how to hack in an attempt to strengthen their skills in the field of information systems security. Hartley [5] argues that an ethical hacking pedagogy may be effective in preparation to combat unethical hacker intrusions associated with the Internet and computer networks.

Overall, extant research suggests that teaching hacking skills raises ethical concerns but arguably the benefits outweigh the drawbacks, as these skills are necessary to better prepare future information security professionals. However, it is unclear how the knowledge gained from offensive activities translates to learning results and students' ethical perspectives. Additionally, few studies investigating students' responsible use of hacking skills exist [30]. Therefore, the

current paper takes steps to investigate this research gap.

### 3. Research method and context

#### 3.1. Cybersecurity course outline and content

The current study collected data from a *cybersecurity fundamentals* course arranged at a polytechnic higher education institute. The data was collected during the past four years of running the course for Information Technology (IT) and Software Engineering (SE) students, one course implementation per year. Although the course is aimed at computing students, it is arranged early in the studies with little or no prior computer science experience expected from the participants. The high-level learning goals for the course were planned as follows. The students know how to think of actions in terms of security, assess security risks, talk about security using professional vocabulary, define a security policy, and protect personal communications. After the course, the students know what cybersecurity is in computer systems, what kind of threats are there in a digitalized world, and what are the current security needs and security technologies.

Overall the course was arranged four times during the past four academic years, from 2019-2020 to 2022-2023, with the course outline remaining the same with only minor changes. The lecture content, exercises, and laboratory assignments remained identical, although deliverables for students varied: In the first two years students turned in all exercises as small, weekly assignment reports. Later the same weekly tasks remained but only four of them were submitted for grading, and the reports were more comprehensive. The last assignment of the course was a reflection of the course as-a-whole, and these reflections were used as the data source.

Table 1 presents the course outline from the last implementation. The course was arranged over 15 teaching weeks of which 13 lectures were covered. In 2019-2020 the lectures were held live. In 2020-2021 the lectures were held online, and in 2022 the lecture videos were delivered on YouTube giving students the freedom to watch them any time and any place.

Weekly exercises and laboratory assignments (labs) were arranged to connect theory and practice. The exercises contained various different activities relating to the course content. Most of the exercises used an offensive approach. The learning activities turned more technical as the course progressed. In the beginning, students researched ways to forge physical documents and types of online scams. Then, a virtual machine running a pre-configured Linux operating system was introduced to complete more technical tasks, such as file encryption, message authentication codes, and digital signatures in practice. Additionally, the students learned how to (mis-)use an email system to forge email headers, retrieve password hashes and crack them using Linux and Windows, and create a phishing site to harvest credentials using the Nginx [41] web server. Finally, the learning tasks concluded with using reverse shells to gain remote access to computer systems, performing SQL injections on a web service, and investigating other web security methods such as clipboard poisoning and ransomware.

During the last course implementation (2022-2023) a pedagogic intervention was designed to help investigate the ethical perceptions of the students while studying the course: Several small reflection questions about both the legal and illicit ways to use the tools presented were added to the exercise and assignment instructions. The objective of this intervention was to see

**Table 1**

Latest version of the cybersecurity fundamentals course outline

Week	Lecture	Exercises	Lab assignment
Week 1	Security principles and security in practice	Forging signatures on physical documents	
Week 2	Cyberattacks	Physical penetration testing with <i>Malduino</i> [38]	
Week 3	Attackers	Creating a website for an online scam	
Week 4	Security needs	Using the Linux virtual machine	
Week 5	Encryption	Steganography and file encryption on Linux	
Week 6	Stream ciphers	<i>No exercises</i>	Crafting phishing messages and email spoofing
Week 7	Block ciphers	Using hashes, message authentication codes, and digital signatures in practice	
Week 8	Integrity, message authentication codes, and hashes	<i>No exercises</i>	Linux password cracking with John the ripper
Week 9	Security technologies	Windows password cracking with <i>Ophcrack</i> [39]	
Week 10	Computer security	<i>No exercises</i>	Retrieving Windows password hashes with <i>mimikatz</i> [40] and cracking them
Week 11	Certificates and credentials	Creating a phishing site for credentials harvesting, and modifying the Linux hosts file	
Week 12	Security tricks and human factors	<i>No exercises</i>	Using a reverse shell to gain remote access to a computer
Week 13	Web security	SQL injections	
Week 14	<i>No lectures</i>	<i>No exercises</i>	Final reflection
Week 15	<i>Exam week, no lectures</i>	Clipboard poisoning and trust on the web. Creating ransomware	

if explicit questions about the ethics of hacking prompt students to reflect on the ethical uses of the skills learned at the end of the course. Thus, the tasks in the learning activities remained the same but minor pedagogic scaffolding was added to better support the ethical deliberation along the way.

### 3.2. Reflections and the thematic analysis process

To assess how the course, its content, and teaching methods helped students achieve learning goals, a summative final assignment was used throughout the course's four-year life cycle. This last learning task followed the form of a student reflection. In the assignment, we asked the students to *describe three examples of things they have learned on the security fundamentals course* in the following way:

- What (specific) thing did you learn?
- Why is this thing important?
- Why did you choose this thing or topic (to write about)?
- How will/can you make use of this knowledge now and in the future?

Submitting the reflection task was voluntary but students were allowed to count this assignment toward the course total (i.e. students were able to turn in this task instead of some other laboratory assignment). The assignment was not graded in terms of content or correctness. Students received a passing mark if the above criteria were fulfilled regardless of what they wrote about (for example, a student could have said that they gained interpersonal and teamwork skills, even though these are not cybersecurity-related topics).

We used the *thematic analysis* research method to analyze the student reflections. The thematic analysis method is a "qualitative research method for identifying, analyzing and reporting patterns (themes) within the data" [42]. The thematic analysis was deemed appropriate as the data is open-ended. The thematic analysis had two objectives: First, the students' chosen topics (of learning) were collected and categorized. Second, we analyzed the essay texts to look for explicit or implicit mentions of ethical considerations.

The coding process was conducted by the author alone. Single-coder approaches to thematic analysis are sufficient if the coding is binary or checklist-based [43]. For this reason, a data collection instrument was constructed prior to the coding phase. Therefore, the purpose of the data collection instrument was to provide a semi-structured coding process to better avoid researcher bias. Table 2 presents the data collection instrument.

Overall the thematic analysis process consisted of five phases, presented as follows.

1. *Familiarization with the data.* An overview of the data was formed with an informal inspection of all submissions. The students' chosen topics were collected during this initial review.
2. *Generating initial codes.* After the initial inspection, each essay was read, and codified using the data collection instrument. Once an observation was noted backtracking was employed to go through submissions that were already codified, in case something was missed relating to the new observation.

**Table 2**

Data collection instrument

<b>Code</b>	<b>Detailed description</b>
Offensive approach	Describes an offensive skill or knowledge of offensive skills
Defensive approach	Describes a defensive skill or knowledge of defensive skills
Unclear application	The student described that they do not know how to use the gained knowledge or skills in the future
Practical skill	Descriptions of practical skills, related to both offensive and defensive tools used on the course
Knowledge gain	Descriptions of gaining knowledge and awareness about cybersecurity attacks
Happens to self (Good ethical)	Descriptions of the knowledge being useful in case oneself is the target of a cyberattack
Learn to defend (Good ethical)	Describes the ability to work in defensive cybersecurity
Awareness raised (Neutral ethical)	Gained awareness about different cyberattacks
Learned skills (Unclear ethical)	Describes how the student learned a to use a tool in practice
Explicit ethical stance	Reflection contained an explicit ethical consideration, for example, "I will use the skills in testing my own security"
Implicit ethical stance	An implicit but clear statement about the ethical use of the tools and knowledge, for example, "I now have more awareness about cyberattacks" or "I am now more knowledgeable and thus can employ better security practices"

3. *Searching for themes.* The resulting codes were inspected once the essays were codified. The prevalence of each code was calculated, and similar codes were merged when possible.
4. *Reviewing themes.* After themes were established explanations and features explaining the codification were drafted.
5. *Defining and naming themes.* Evaluating and refining the themes, giving them succinct names, and generating clear definitions.

In the process of analyzing the data, we followed the ethical principles of research with human participants by The Finnish National Board on Research Integrity TENK. The ethical guidelines also affected the choice of research method; The work was (in part) limited to analysis of the reports as surveys could not be used post-hoc.

## 4. Results

Next, the results of the data collection based on the thematic analysis process are presented. Overall, the data consists of observations from 110 student reflections. The codified topics (i.e. "what did you learn") are presented in Table 3. When reading the reflections, we listed all the topics ("things") the students reported to have learned from the course. The students chose

multiple different course topics in their learning reflections. In some cases, students would choose more than three topics to describe and therefore, a total of 375 achieved learning goals were codified from the submissions.

The most prevalent topics were: Cryptography (theoretical knowledge of how cryptography is used), (theoretical knowledge of understanding attacks), cyberattacks (theoretical knowledge of understanding attacks), encryption (practical skill involving encrypting and decrypting files), and email spoofing (practical skill of how to spoof email headers). Among the most popular choices were also the CIA (confidentiality, integrity, and availability) security model, risk management approaches, certificates and credentials, and computer security.

It is notable that within the student choices, hands-on hacking skills, for example, *Email spoofing* (N=28), *Password cracking techniques* (N=15), *Linux password cracking* (N=13), or *Windows password cracking* (N=12), were no more popular than the security awareness and defensive skills topics. In fact, most students would pick some generic umbrella topic within security (for example, *Cryptography* or *Cyberattacks*) over practical hacking skills.

The coding process continued with identifying statements related to the ethics of hacking. We looked for paragraphs of text, where some explicit or implicit statement was made. For example, an explicit statement could be "I would never use hacking skills without permission." In contrast, anything that points towards ethical hacking or security awareness was considered an implicit statement, for example, "these skills are useful for a possible career in cybersecurity."

Table 4 describes the observations made from the student essays. First, we categorized the essays based on if they described offensive skills and knowledge (N=54), or defensive skills and knowledge (N=82). We also recorded whether the essay described gaining practical skills (N=46) or gaining security awareness and knowledge (N=90). Then, based on the given discussion prompt "how will/can you make use of this knowledge" we evaluated we recorded instances of how the students described the usefulness of the learning. Particularly, we noted instances of:

- if there was an unclear or unknown future use of the knowledge ("unclear application") (N=12)
- if the text described usefulness in protecting the student themselves ("happens to self"). This was considered a positive ethical stance (N=27)
- if the student describes learning defensive skills ("learn to defend"). Likewise, this was considered a positive ethical stance (N=64)
- if the student described increased awareness ("awareness raised"). This was considered a neutral ethical stance (N=59)
- if the student described learning a practical hacking skill. This was considered an unclear ethical stance (N=4)

It should be noted that the categorization of all the above criteria was done for all essays. Similarly, one student essay could be placed in multiple categories, for example, if the essay described both defensive and offensive skills or if it described both awareness and defensive skills.

Next, we focused on how the student essays described the ethics involved in hacking and cybersecurity. The essays were categorized based on whether they contained an explicit statement about ethical considerations, an implicit but clear statement, or no statement at all.



**Table 3**

Student choices

<b>Student choice</b>	<b>Detailed explanation</b>	<b>N</b>
Cryptography	How encryption algorithms work, how hashing and MACs work	46
Attacks	How cyberattacks work (denial-of-service, brute-force etc). Also to some degree mitigations of attacks	34
Encryption	How to encrypt and decrypt files or data communications (skill)	30
Email spoofing	How to send email with fabricated headers	28
CIA Model	Meaning of confidentiality, integrity, and availability	24
Risk management	Risk management, human elements, cybercrime	19
Importance of security	Importance of security as a topic. OR: Basics of cybersecurity	18
Certificates and credentials	How cryptography is used to secure online communications in web servers	17
Computer security	Generic computer security topics, such as using firewalls, anti-virus, and up-to-date software	17
Password cracking	Password cracking in general as a skill	15
Linux password cracking	Specifically dictionary attack	13
Windows password cracking	Specifically rainbow tables	12
Digital signatures	How to sign documents	11
Linux skills	Being proficient at using Linux	11
Social engineering techniques	Topics such as phishing, spear-phishing, and whaling.	11
Clipboard hijacking	Copying text directly from a website can be harmful (hidden text)	9
Steganography	Hiding data inside innocent looking files	9
Detecting vulnerabilities on Linux	Vulnerability detection and compliance audit on Linux using the Lynis software	7
Malduino	Scripting and deploying bad USB attacks using Malduino devices	7
Password security	General observations about password strength, reasons to use two-factor authentication etc.	7
SQL Injections and web security	Knowledge of how SQL injections work and how to test a vulnerable web application	7
Reverse shell	Scripting and deploying a reverse shell connection using netcat (nc)	5
Sandboxing	Use virtual machine as an isolated environment for safety purposes	5
Network defences	Network defences or network security concepts (for example, firewall intrusion detection, dmz, honeypots)	4
Malware	Understanding what malware is and how malware programs work in general	2
Protocols	How communications protocols are used to create interconnected systems, and how to secure those communications	2
Creating a fake website	Creating a website for phishing or online scams	2
Principle of least privilege	How compartmentalising and computer management is used to improve security	1
Critical thinking	Critical thinking skills, such as not falling for online scams	1
Forging documents	How to make copies of digital or physical documents	1
Total		375

**Table 4**

Descriptive statistics of the student reflections

	2019-2020	2020-2021	2021-2022	2022-2023(*)	Total
Number of students (N)	34	24	28	24	110
Offensive approaches	17	6	9	22	54
Defensive approaches	30	20	23	9	82
Unclear application	7	3	2	0	12
Practical skill	11	3	14	18	46
Knowledge gain	30	20	20	20	90
Happens to self (Good ethical)	11	9	3	4	27
Learn to defend (Good ethical)	20	12	16	16	64
Awareness raised (Neutral ethical)	17	11	11	20	59
Learned skills (Unclear ethical)	1	1	0	2	4

\* Year 2022-2023 contained reflection questions throughout the course

**Table 5**

Number of ethics related statements from the student reflections.

	Students	Explicit	%	Implicit	%	Impl. + Expl. combined	%
All years	110	32	29 %	44	40 %	76	69 %
19-20	34	5	15 %	14	42 %	19	56 %
20-21	24	7	29 %	10	42 %	17	71 %
21-22	28	11	39 %	8	29 %	19	68 %
22-23(*)	24	9	38 %	12	50 %	21	88 %

\* Year 2022-2023 contained reflection questions throughout the course

Table 5 presents the number and percentage of these statements. If both explicit and implicit statements are counted, the proportion of essays where the ethical nature of the skills and knowledge gained on the course was discussed is 69% over the years. The number of ethics-related statements varies by year but the most ethics-related statements were observed from the year 2022-2023 (the year that included the intervention).

## 5. Discussion

Next, the results are discussed in the context of the original research questions. *To what extent do written student reflections depict ethical considerations?* We found that, overall, most students had included some ethical aspects of using hacking skills and knowledge in their essays. Sometimes this was an explicit statement of the ethical nature of the work (e.g. "I will only try these methods to audit my own systems"). Most often ethical considerations were expressed implicitly (e.g. "Now I have more awareness about cyberattacks, to defend from them better"). Implicit and explicit mentions of the ethics of hacking were present in a total of 69% of the reflections. When the course material was modified slightly to include more reflections throughout the course, the number of ethical statements rose to 88%. Both these numbers can be considered good, as the final essay did not specifically instruct students to write about the ethics of hacking.

*What ethics-related issues emerge from the reflections and how to mitigate them?* 11% of the essays were unsure about the practical applicability of the skills and knowledge gained from the course. This could be mitigated with purposeful pedagogic design; For example, by investigating real-world case studies which is often suggested in the cybersecurity education literature (see for example [44]). Proven successful course designs also include situated learning [45, 46, 47], use of real-world case examples (for example, news stories) [44, 48], or a special focus on industrial environments [49].

To answer the main research question *how ethical considerations manifest in the students' descriptions of what they learned*: The most common themes from the student reflections were related to security awareness and security technologies. Surprisingly, when asked about the things learned in the course the students often chose topics related to security awareness, security technologies, and defensive approaches more often than offensive hacking skills. While a portion of the students mentioned picking up offensive skills, the overwhelming majority of them (106 out of 110) described the learned skills in an ethically sound way. Conversely, only a small minority of students (4) described just learning to use hacking tools. Therefore, the horror scenarios about the dangers of teaching hacking depicted by some earlier research are, for the most part for our students, a non-issue.

Finally, the last offering of the course included additional reflection questions in the weekly exercises and labs. This may have helped with students' ability to reflect on the ethical considerations of the skills and knowledge from the course, as the number of observed ethics-related statements grew to be the highest of all teaching years. However, without further validation, this is only a cautious indication of the intervention's results, and currently, the results may not be statistically significant. Overall, this suggests that while we were able to prompt some students to think more about the ethics of hacking using minor pedagogic scaffolding, the hacking content (offensive skills) itself was not a significant factor in the course content.

## 6. Conclusion

Extant literature maintains that ethical considerations must be addressed in computing and cybersecurity education. However, the current study suggests that, even for novices in the field, there are seldom ethical issues regarding how to use hacking knowledge. It seems that in the cybersecurity course, most students implicitly understand the context and the 'right' way to use the knowledge and skills in an ethically sound manner.

Future work and limitations remain in the field. This paper presented only descriptive data but no statistical analysis. As the data source was observations from the thematic analysis process, a statistical analysis would have been difficult due to the many underlying confounding factors and, probably spurious correlations. Additionally, the data analysis was completed by the author alone. To mitigate researcher bias, a data collection instrument was designed before data analysis was conducted.

As the observations were recorded from data over several years, the analysis had to be conducted post-hoc. Given that the data comes from formal student reports, students might be simply writing what they think their teachers want to hear. However, the learning task (reflection) did not specifically ask students to take an ethical stance. Finally, even if students

are trying to please the teachers by moderating how they write about the course, this on its own suggests that students make conscious choices and ethical considerations while writing the reflection.

The increase in ethical considerations within the student reflections during the last implementation of the course was an encouraging indicator. In future, the effect of the intervention should be further explored by using a validated instrument and appropriate statistical analysis method.

## References

- [1] N. Radziwill, J. Romano, D. Shorter, M. Benton, The ethics of hacking: Should it be taught?, arXiv preprint arXiv:1512.02707 (2015).
- [2] L. Smith, M. M. Chowdhury, S. Latif, Ethical Hacking: Skills to Fight Cybersecurity Threats, EPiC Series in Computing 82 (2022) 102–111. Publisher: EasyChair.
- [3] P. Y. Logan, A. Clarkson, Teaching students to hack: curriculum issues in information security, in: Proceedings of the 36th SIGCSE technical symposium on Computer science education, 2005, pp. 157–161.
- [4] E. Alashwali, Incorporating hacking projects in computer and information security education: an empirical study, International Journal of Electronic Security and Digital Forensics 6 (2014) 185–203.
- [5] R. D. Hartley, Ethical hacking pedagogy: An analysis and overview of teaching students to hack, Journal of International Technology and Information Management 24 (2015) 6.
- [6] R. Hartley, D. Medlin, Z. Houlik, Ethical hacking: Educating future cybersecurity professionals, in: Proceedings of the EDSIG Conference ISSN, volume 2473, 2017, p. 3857.
- [7] A. M. Curbelo, A. Cruz, Faculty attitudes toward teaching ethical hacking to computer and information systems undergraduates students, in: Proceedings of the Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology, 2013.
- [8] B. A. Pashel, Teaching students to hack: Ethical implications in teaching students to hack at the university level, in: Proceedings of the 3rd annual conference on Information security curriculum development, 2006, pp. 197–200.
- [9] L. Riihelä, Teaching information security: A systematic mapping study, Master's thesis, LUT University, Finland, 2019.
- [10] L. Zhang-Kennedy, S. Chiasson, A systematic review of multimedia tools for cybersecurity awareness and education, ACM Computing Surveys (CSUR) 54 (2021) 1–39. Publisher: ACM New York, NY, USA.
- [11] V. Švábenský, J. Vykopal, P. Čeleda, What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences, in: Proceedings of the 51st ACM technical symposium on computer science education, 2020, pp. 2–8.
- [12] S. Laato, A. Farooq, H. Tenhunen, T. Pitkamaki, A. Hakkala, A. Airola, Ai in cybersecurity education-a systematic literature review of studies on cybersecurity moocs, in: 2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT), IEEE, 2020, pp. 6–10.
- [13] X. Mountroudou, D. Vosen, C. Kari, M. Q. Azhar, S. Bhatia, G. Gagne, J. Maguire, L. Tu-

- dor, T. T. Yuen, Securing the human: a review of literature on broadening diversity in cybersecurity education, *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education* (2019) 157–176.
- [14] N. A. A. Rahman, I. Sairi, N. A. M. Zizi, F. Khalid, The importance of cybersecurity education in school, *International Journal of Information and Education Technology* 10 (2020) 378–382.
- [15] H. Aldawood, G. Skinner, Educating and raising awareness on cyber security social engineering: A literature review, in: 2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE), IEEE, 2018, pp. 62–68.
- [16] R. Roepke, U. Schroeder, The Problem with Teaching Defence against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education., in: *Proceedings of the 11th International Conference on Computer Supported Education (CSEDU 2019)*, 2019, pp. 58–66.
- [17] R. B. Sağlam, V. Miller, V. N. Franqueira, A Systematic Literature Review on Cyber Security Education for Children, *IEEE Transactions on Education* (2023). Publisher: IEEE.
- [18] N. Chowdhury, V. Gkioulos, Cyber security training for critical infrastructure protection: A literature review, *Computer Science Review* 40 (2021) 100361. Publisher: Elsevier.
- [19] W. Chen, Y. He, X. Tian, W. He, Exploring Cybersecurity Education at the K-12 Level, in: *SITE Interactive Conference, Association for the Advancement of Computing in Education (AACE)*, 2021, pp. 108–114.
- [20] M. Coenraad, A. Pellicone, D. J. Ketelhut, M. Cukier, J. Plane, D. Weintrop, Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games, *Simulation & Gaming* 51 (2020) 586–611. Publisher: SAGE Publications Sage CA: Los Angeles, CA.
- [21] F. Alotaibi, S. Furnell, I. Stengel, M. Papadaki, A review of using gaming technology for cyber-security awareness, *Int. J. Inf. Secur. Res.(IJISR)* 6 (2016) 660–666.
- [22] J. Jeong, J. Mihelcic, G. Oliver, C. Rudolph, Towards an improved understanding of human factors in cybersecurity, in: 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), IEEE, 2019, pp. 338–345.
- [23] R. Ramirez, N. Choucri, Improving interdisciplinary communication with standardized cyber security terminology: A literature review, *IEEE Access* 4 (2016) 2216–2243. Publisher: IEEE.
- [24] S. Das, SoK: a proposal for incorporating accessible gamified cybersecurity awareness training informed by a systematic literature review, in: *Proceedings of the workshop on usable security and privacy (USEC)*, 2022.
- [25] J. Pittman, Understanding system utilization as a limitation associated with cybersecurity laboratories—A literature analysis, *Journal of Information Technology Education. Research* 12 (2013) 363. Publisher: Informing Science Institute.
- [26] M. Lamond, K. Renaud, L. Wood, S. Prior, SOK: young children’s cybersecurity knowledge, skills & practice: a systematic literature review, in: *Proceedings of the 2022 European Symposium on Usable Security*, 2022, pp. 14–27.
- [27] J. Hautamäki, M. Karjalainen, T. Hämäläinen, P. Häkkinen, Cyber security exercise: Literature review to pedagogical methodology, in: *INTED Proceedings, IATED Academy*, 2019. Issue: 2019.

- [28] M. Hendrix, A. Al-Sherbaz, B. Victoria, Game based cyber security training: are serious games suitable for cyber security training?, *International Journal of Serious Games* 3 (2016) 53–61.
- [29] Y. A. Younis, K. Kifayat, L. Topham, Q. Shi, B. Askwith, Teaching Ethical Hacking: Evaluating Students’ Levels of Achievements and Motivations, in: *International Conference on Technical Sciences (ICST2019)*, volume 6, 2019, p. 04.
- [30] R. E. Pike, The “ethics” of teaching ethical hacking, *Journal of International Technology and Information Management* 22 (2013) 4.
- [31] S. Bratus, A. Shubina, M. E. Locasto, Teaching the principles of the hacker curriculum to undergraduates, in: *Proceedings of the 41st ACM technical symposium on computer science education*, 2010, pp. 122–126.
- [32] Z. Trabelsi, W. Ibrahim, Teaching ethical hacking in information security curriculum: A case study, in: *2013 IEEE Global Engineering Education Conference (EDUCON)*, IEEE, 2013, pp. 130–137.
- [33] B. Wilson, Teaching security defense through web-based hacking at the undergraduate level (2017).
- [34] Z. Trabelsi, M. McCoey, Ethical hacking in information security curricula, *International Journal of Information and Communication Technology Education (IJICTE)* 12 (2016) 1–10. Publisher: IGI Global.
- [35] N. Patrignani, I. Kavathatzopoulos, Teaching of technology is teaching of ethics. but how?, in: *Technology Ethics–Tethics 2021*, University of Turku, 2021.
- [36] T. Dimkov, W. Pieters, P. Hartel, Training students to steal: a practical assignment in computer security education, in: *Proceedings of the 42nd ACM technical symposium on computer science education*, 2011, pp. 21–26.
- [37] G. Conti, T. Babbitt, J. Nelson, Hacking competitions and their untapped potential for security education, *IEEE Security & Privacy* 9 (2011) 56–59.
- [38] Malduino, 2023. URL: <https://malduino.com/>.
- [39] Ophcrack, 2023. URL: <https://ophcrack.sourceforge.io/>.
- [40] mimikatz, 2023. URL: <https://github.com/ParrotSec/mimikatz>.
- [41] Nginx: Advanced load balancer, web server, & reverse proxy, 2023. URL: <https://www.nginx.com/>.
- [42] V. Braun, V. Clarke, Using thematic analysis in psychology, *Qualitative research in psychology* 3 (2006) 77–101.
- [43] N. McDonald, S. Schoenebeck, A. Forte, Reliability and inter-rater reliability in qualitative research: Norms and guidelines for csw and hci practice, *Proceedings of the ACM on Human-Computer Interaction* 3 (2019) 1–23.
- [44] R. English, J. Maguire, Exploring student perceptions and expectations of cyber security, in: *Computing Education Practice*, 2023, pp. 25–28.
- [45] Z. A. Wen, Z. Lin, R. Chen, E. Andersen, What. hack: engaging anti-phishing training through a role-playing phishing simulation game, in: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–12.
- [46] T. Denning, A. Lerner, A. Shostack, T. Kohno, Control-alt-hack: the design and evaluation of a card game for computer security awareness and education, in: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 915–928.

- [47] M. Canepa, F. Ballini, D. Dalaklis, S. Vakili, Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain, in: INTED2021 Proceedings, IATED, 2021, pp. 3489–3499.
- [48] T. Hynninen, On the learning activities and outcomes of an information security course, in: Proceedings of the 19th Koli Calling International Conference on Computing Education Research, 2019, pp. 1–2.
- [49] T. E. Gasiba, K. Beckers, S. Suppan, F. Rezabek, On the requirements for serious games geared towards software developers in the industry, in: 2019 IEEE 27th International Requirements Engineering Conference (RE), IEEE, 2019, pp. 286–296.