Towards Improving Online Security Awareness Skills with Phishing and Spoofing Labs

Alexander Kerr[1] and Timo Hynninen[1,2]
[1]South-Eastern Finland University of Applied Sciences, Mikkeli, Finland
[2]Laurea University of Applied Sciences, Espoo, Finland
alexander.kerr@xamk.fi; timo.hynninen@laurea.fi

***Abstract*—It can be especially hard for novices to examine their online browsing habits, or to be aware of the dangers related to online security. In this paper, we describe laboratory exercises designed to improve awareness of online security, in addition to teaching cybersecurity knowledge and skills. The lab exercises were used as a part of an information security fundamentals course for IT students with none or only novice experience in the field. These lessons are suitable for both delivery in the classroom and online in a virtual laboratory environment. The lab exercises were developed using the design science research methodology (DSR). Following DSR principles, the evaluation of the developed material was done by extracting observations from student reports. The thematic analysis method was used to process the data. The evaluation of the student learning reports revealed that the labs and the course were successful in the following ways: Improving security knowledge, improving critical thinking skills, and improving security awareness. Students also gained hands-on cyber awareness skills by analysing metadata in messages. Additionally, the material was perceived as useful for future working life.**

Keywords—cybersecurity;education;curriculum design

I. Introduction

Information and cybersecurity are recommended to be tightly integrated into computing education [1], [2]. This is because the need for cybersecurity knowledge and awareness is on the rise; Not only is the cybersecurity field in dire need of qualified professionals [3], [4] but security awareness is also paramount in other computing and IT-related jobs.

Cybersecurity is a multifaceted topic [5]. All computing students need to understand security to some degree, and they generally learn the necessary domain skills in their respective areas; For example, web application security can be covered in web development courses and infrastructure security in computer networking classes. However, all students should have the basic security thinking and awareness skills early on, as security cannot be an afterthought [6]. One important topic in security thinking and awareness is online phishing and spoofing scams.

Phishing attacks are common [7]. For example, the Anti-Phishing Working Group (APWG) reported having observed between 68 000 and 94 000 phishing attacks per month in 2022 [8]. According to APWG, the most targeted industries for phishing attacks are financial institutions, SaaS and Webmail systems, and social media providers [8]. Clearly, phishing attacks are common against services that everyone uses daily.

The current paper describes a case study in which laboratory exercises ('labs') are designed to illustrate phishing and online spoofing scams. These lab exercises include the investigation of online scams, the design and implementation of phishing and spoofing, and remedies to said dangers. The objective of the study is to improve awareness and security knowledge related to online browsing safety.

The rest of the paper is organized as follows. Section II presents related work on information and cybersecurity education. Section III describes the research methodology used in the study, particularly the thematic analysis method that was used to codify the data. Next, Section IV presents the design of the lab exercises and results from the data analysis. Finally, Section V concludes the paper by discussing the findings, and limitations of the work.

II. Related work

Cybersecurity is an interdisciplinary field that requires a strong foundation in computing technologies but also an understanding of the human and social aspects of computing [5].

The extant work in cybersecurity education is well established in the literature. The body of knowledge is detailed in several tertiary studies, e.g. [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28]. These studies can be found using the Google Scholar search engine with the keywords *("cybersecurity" OR "cyber security")+("teaching" OR "education")+("literature review" OR "mapping study" OR "meta analysis").*

According to the systematic review by Sağlam et al. [16] there are three main themes in the cybersecurity education literature: what to teach, how to teach, and who should teach. Cybersecurity courses should combine practical and theoretical education, with hands-on approaches being both popular and effective [17], [16], [29]. Roepke and Schroeder [15] point out that new cybersecurity tools and challenges arise constantly, and teaching should aim to foster the transfer of knowledge to solve new problems in a sustainable way. Usually students are able to gain an understanding of abstract security concepts early on [30].

With regards to best practices, technical cybersecurity should be taught using virtual laboratory environments

using an offensive approach [20]. According to the study by Wilson [31], teaching students to attack rather than to defend will increase learning results and student motivation. Virtual laboratory environments can also have the technical limitations which prevent them from portraying real-world situations true in every respect, however modern virtualization technologies can usually overcome these obstacles [25].

In addition, serious games can be an effective method to provide training [21]. Cybersecurity games have been shown to have a a positive effect on learning outcomes [28]. Games are especially useful for teaching security awareness and teaching students how to defend from cyberattacks [21].

Albeit the topic of cybersecurity education is abundant in literature, there is room for development. For example, the literature review by Chowdhury & Gkioulos [17] concludes that there is no existing consensus on the delivery methods and design of cybersecurity lab exercises. This suggests that evaluation of the cybersecurity lab exercises and their learning outcomes is a fruitful research avenue, and this paper attempts to fill the research gap.

III. Research method

The Design Science Research (DSR) method [32], [33], [34], [35] is suitable for various engineering work. DSR is an outcomes-based method that provides scaffolding for the creation and evaluation of useful artefacts [33], [34]. The artefacts can range from theories to designs and tangible products [36]. The novelty, quality, and applicability of the artefacts are evaluated based on their usefulness and capability to solve real problems [37], [33]. In this study, the Design Science Research approach will act as the guiding framework in the design and evaluation of the cybersecurity laboratory exercises.

Following the DSR method's requirement to evaluate designs in real-world context, the courseware will be analyzed using student reflections of their learning during the course. Therefore, the primary data source in this study is student submitted reports to a learning task at the end of the course. Turning in this reflection task was voluntary as such but it would accumulate points toward the course total, or students could opt to complete the reflection task instead of another laboratory assignment.

In this learning task, students were asked to name three things they learned during the course, and to explain their choices. Specifically, we asked the students to reflect on the following:

- name/choose three topics or things they learned during the course
- give a short explanation to justify the selection
- explain the importance of the chosen topics
- explain how the knowledge can be useful

The answers were open-ended. The *thematic analysis* research method was chosen to code the open-ended data. The thematic analysis method is a "qualitative research method for identifying, analyzing and reporting patterns (themes) within the data" [38]. In the data collection, processing, and analysis the ethical principles of research with human participants by the Finnish national board on research integrity were adhered to.

IV. Implementation and Results

A. Course design

In the autumn semester of 2022 we organized an introductory course in information and cybersecurity. The course focused on the following topics:

- cybersecurity concepts
- threats, attacks, and attackers
- security needs and security technologies
- computer security and access control
- network security, network defenses
- encryption, secured web communications, and certificates
- security processes and users in the process

The course's lectures followed the outline of the topics presented above. Weekly hands-on laboratory exercises were designed to implement the concepts in practice. While the course objectives were not designed to be particularly biased toward offensive or defensive approaches the labs turned out to follow a more offensive style. These lab exercises could be completed either in the virtual laboratory environment (the Virtual ICT Lab [39]), or in the classroom by installing the virtual machine images locally.

It was assumed that the majority of the students participating would have little to no knowledge of 1). Basic cybersecurity principles. and 2). The Linux operating environment. For this reason, detailed instructions were given for each lab. One week focused solely on getting familiar with the nested virtual environment, and Linux in general.

B. Virtual laboratory environment

The labs were implemented in a sandbox environment using virtual machines running in the Virtual ICT Lab. Figure 1 presents the topology of virtual machines (VMs) which were created for the students. The main platform for this was a Linux Ubuntu desktop 20.04, which was run as the main desktop that students used. Additionally, a standard Windows 10 desktop was available. The primary Linux VM was installed with all the required elements that students were expected to use over the semester. Several lab scenarios were available for the different weekly lab topics. The configuration included a Linux server running nginx (web server) and an IMAP (email) server (but students did not need to interact with the server directly).

The main VM was configured to use a lighter Xubuntu desktop manager and dynamic 25GB of storage. This made the VM capable of running on 1 virtual CPU, and it ran moderately well with 1GB of RAM. The initial installation would take up 9.25GB of storage.

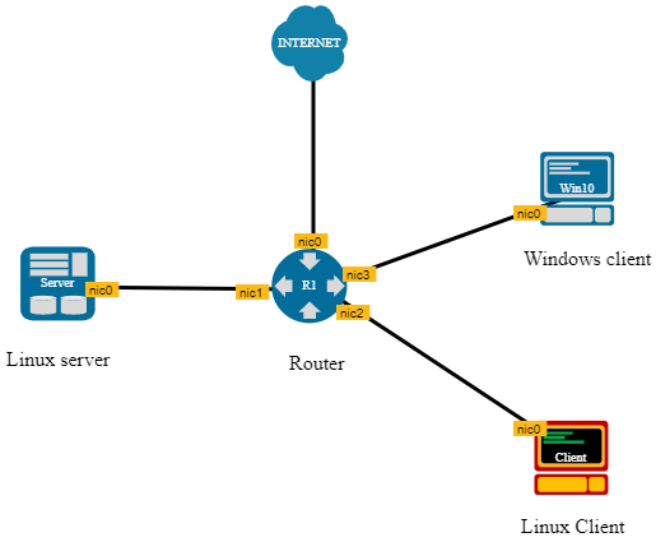

Fig. 1. Topology of virtual machines in the virtual laboratory environment

C. Lab exercise design

The Xubuntu VM was available as part of a virtual scenario where the students completed various cybersecurity hands-on labs. Table I presents the web security focused lab exercises.

The first lab demonstrated the ease of creating scam and phishing websites. First, the students were asked to design a scam and a phony website to accompany it. Then, the students were given some basic instructions on how they could create a targeted phishing site on the web.

The second lab exercise focused on manipulating e-mail headers. The students were tasked with sending emails from fabricated addresses using command-line tools. The objective was to demonstrate that on its own email is not inherently secure, and how easy phishing mail is to construct. In addition, the goal was to increase the awareness of other attack methods, giving the students a deeper understanding of how systems could quickly be compromised.

The third lab was designed to highlight awareness of phishing, spoofing, and password vulnerability. This was realized as the design and implementation of a credential harvesting portal. Students would copy a legitimate webpage for credential harvesting, and then point the victim's computer to the phony site by altering the Linux hosts file. This lab was also used to demonstrate browser features that can aid students in deciding if a website is legitimate or not.

D. Observations

In order to elicit information on how successful the phishing and spoofing laboratory exercises were, the responses to the reflection task were inspected by the two instructors (authors of this paper) of the course. Overall there were 39 students who submitted reports for the course. Out of these we selected 22 for closer inspection using the thematic analysis approach. This selection was based on whether student submitted reflection was related to the spoofing and phishing labs. The rest of the submissions described learning outcomes related to other course material, for example, unrelated labs or lecture material.

For the 22 selected reports an initial open coding process was done by both authors individually. This process involved reading the student reflection, and recording observations on *how the text described the spoofing and phishing labs*. Next, an axial coding process was conducted, both authors codified the observations into categories and concepts together. The resulting text categories are presented in Table II.

Most of the reflections (N=16) described how the tasks had increased the student's general awareness of phishing, spoofing, or online scams. Another common response was that the students found out how easy spoofing can be on the web (N=13). Many students also described gaining either generic or specific technical knowledge (N=12).

Next, a group of less common but equally important recurring themes were found. Some students reflected on the usefulness of the knowledge and skills in later working life (N=5). Other students reported on how they had gained new hands-on skills in analyzing email messages and their metadata (N=4). A few students described how the knowledge is useful given how common scams are on the web (N=3). Finally, the last students mentioned how the labs helped in developing critical thinking skills (N=2).

V. Discussion and Conclusions

This paper outlined our experiences in running hands-on laboratory exercises related to phishing and spoofing on an early information and cybersecurity course. The

TABLE I
ONLINE SECURITY AWARENESS RELATED LAB EXERCISES DURING COURSE

Name	Description
Desining convincing internet scams	Students used Google Sites (or other CMS editor) to design websites for malicious purposes. Students were instructed to design a convincing fraud or scam that could fool a user who lands on the website.
Email spoofing	Students used Linux command line tools to send email messages to an insecurely configured IMAP server. The message headers were altered to spoof the senders' email address.
Creating a phishing site	Students familiarized themselves with credentials harvesting. They studied the HTML and CSS code of a legitimate website and produced a convincing copy. Then the students would act as a malicious intruder and modify the Linux hosts file in an attempt to fool users to land on a credential harvesting site.

TABLE II
AXIAL CODES GENERATED DURING THE THEMATIC ANALYSIS PROCESS

#	Axial code	Number of observations	Detailed decription
1	Awareness	16	Descriptions of increased awareness of online security.
2	Critical thinking	2	Descriptions of increased critical thinking about messages on the web.
3	Gained knowledge	12	Free-form descriptions of different knowledge related to the phishing and spoofing exercises.
4	Useful in working life	5	Descriptions mentioning the awareness of phishing and spoofing when working in an organization.
5	Inevitability	3	Descriptions of spoofing being commonplace, and how everyone should be aware of the topic.
6	Analysing message metadata	4	Descriptions of gaining hands-on skills for analysing message metadata to verify the authenticity of the sender.
7	Spoofing ease	13	Descriptions of how easy it is or how little skill it takes to create spoofed messages.

labs should be suitable for a wide range of students - even though they were designed for IT students there was no prerequisite knowledge needed to take the course.

A. Findings

At the end of the course, we evaluated student reflections on what they perceived as the most important topics. It was found that the students described their experiences in seven different categories: Gaining awareness of online security; gaining critical thinking skills; gaining new knowledge; the course topics are useful for the future working life; scams are so ubiquitous that one must be wary of online dangers; gained hands-on computing skills to check email metadata; and learning that it takes little skill to concoct attacks online.

As a result, the data suggest, that the labs (and the course as a whole) helped students pick up both practical skills and knowledge about online security. Specifically, students reported now exercising more caution in online messaging / emails and they know some remedies for phishing attacks. Students generally have more awareness of phishing and spoofing online, and they are thus better prepared for professional working life. Additionally, students gained professional computing and IT knowledge about email systems and their operation.

B. Limitations and future work

The scope and limitations of the current study warrant some discussion. First, our sample of 22 student reflections is relatively low. However, the results are in line with previous findings (e.g. [20]). Additionally, the sample was taken from a larger pool of answers.

The research method employed a thematic analysis method. As thematic analysis uses an open coding approach it is possible that researcher bias affects the findings. For this reason both authors conducted the coding first individually, and then agreed on the resulted axial codes.

In future work we continue to evaluate our labs and improve the designs. We aim to answer the call given by Chowdhury & Gkioulos [17] to document and publish best practices in the cybersecurity education and course content.

REFERENCES

[1] S. Peltsverger and O. Karam, "Is teaching with security in mind working?" in *2010 Information Security Curriculum Development Conference*. ACM, 2010, pp. 15–20.

[2] The Joint Task Force on Computing Curricula, "Curriculum guidelines for undergraduate degree programs in software engineering," New York, NY, USA, Tech. Rep., 2015.

[3] (2017) This is what the future of cybersecurity will look like. [Online]. Available: https://www.weforum.org/agenda/2017/08/the-us-is-upping-its-game-against-cyber-attacks-but-the-security-industry-faces-a-huge-challenge

[4] F. Goupil, P. Laskov, I. Pekaric, M. Felderer, A. Dürr, and F. Thiesse, "Towards understanding the skill gap in cybersecurity," in *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1*, ser. ITiCSE '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 477–483. [Online]. Available: https://doi.org/10.1145/3502718.3524807

[5] H. Suryotrisongko and Y. Musashi, "Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective," in *2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA)*. IEEE, 2019, pp. 162–167.

[6] J. McManus, "Security by design: teaching secure software design and development techniques," *Journal of Computing Sciences in Colleges*, vol. 33, no. 3, pp. 75–82, 2018.

[7] S. Bell and P. Komisarczuk, "An analysis of phishing blacklists: Google safe browsing, openphish, and phishtank," in *Proceedings of the Australasian Computer Science Week Multiconference*, 2020, pp. 1–11.

[8] The Anti-Phishing Working Group. (2022) The APWG phishing activity trends report. [Online]. Available: https://apwg.org/trendsreports/

[9] L. Zhang-Kennedy and S. Chiasson, "A systematic review of multimedia tools for cybersecurity awareness and education," *ACM Computing Surveys (CSUR)*, vol. 54, no. 1, pp. 1–39, 2021, publisher: ACM New York, NY, USA.

[10] V. Švábenskỳ, J. Vykopal, and 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.

[11] S. Laato, A. Farooq, H. Tenhunen, T. Pitkamaki, A. Hakkala, and 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.

[12] X. Mountrouidou, D. Vosen, C. Kari, M. Q. Azhar, S. Bhatia, G. Gagne, J. Maguire, L. Tudor, and 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*, pp. 157–176, 2019.

[13] N. A. A. Rahman, I. Sairi, N. A. M. Zizi, and F. Khalid, "The importance of cybersecurity education in school," *International Journal of Information and Education Technology*, vol. 10, no. 5, pp. 378–382, 2020.

[14] H. Aldawood and 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.

[15] R. Roepke and 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.

[16] R. B. Sağlam, V. Miller, and V. N. Franqueira, "A Systematic Literature Review on Cyber Security Education for Children," *IEEE Transactions on Education*, 2023, publisher: IEEE.

[17] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review," *Computer Science Review*, vol. 40, p. 100361, 2021, publisher: Elsevier.

[18] W. Chen, Y. He, X. Tian, and 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.

[19] M. Coenraad, A. Pellicone, D. J. Ketelhut, M. Cukier, J. Plane, and D. Weintrop, "Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games," *Simulation & Gaming*, vol. 51, no. 5, pp. 586–611, 2020, publisher: SAGE Publications Sage CA: Los Angeles, CA.

[20] L. Riihelä, "Teaching information security: A systematic mapping study," Master's thesis, LUT University, Finland, 2019.

[21] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, "A review of using gaming technology for cyber-security awareness," *Int. J. Inf. Secur. Res.(IJISR)*, vol. 6, no. 2, pp. 660–666, 2016.

[22] J. Jeong, J. Mihelcic, G. Oliver, and 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 and N. Choucri, "Improving interdisciplinary communication with standardized cyber security terminology: A literature review," *IEEE Access*, vol. 4, pp. 2216–2243, 2016, 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*, vol. 12, p. 363, 2013, publisher: Informing Science Institute.

[26] M. Lamond, K. Renaud, L. Wood, and 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, and P. Häkkinen, "Cyber security exercise: Literature review to pedagogical methodology," in *INTED Proceedings*. IATED Academy, 2019, issue: 2019.

[28] M. Hendrix, A. Al-Sherbaz, and B. Victoria, "Game based cyber security training: are serious games suitable for cyber security training?" *International Journal of Serious Games*, vol. 3, no. 1, pp. 53–61, 2016.

[29] L. Wang, J. Yang, and P.-J. Wan, "Educational modules and research surveys on critical cybersecurity topics," *International Journal of Distributed Sensor Networks*, vol. 16, no. 9, p. 1550147720954678, 2020.

[30] 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.

[31] B. Wilson, "Teaching security defense through web-based hacking at the undergraduate level," 2017.

[32] S. Gregor and A. R. Hevner, "Positioning and presenting design science research for maximum impact." *MIS quarterly*, vol. 37, no. 2, pp. 337–355, 2013.

[33] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *MIS Q.*, vol. 28, no. 1, pp. 75–105, Mar. 2004. [Online]. Available: http://dl.acm.org/citation.cfm?id=2017212.2017217

[34] A. R. Hevner, "A three cycle view of design science research," *Scandinavian journal of information systems*, vol. 19, no. 2, p. 4, 2007.

[35] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of management information systems*, vol. 24, no. 3, pp. 45–77, 2007, publisher: Taylor & Francis.

[36] B. Kuechler and V. Vaishnavi, "On theory development in design science research: anatomy of a research project," *European Journal of Information Systems*, vol. 17, no. 5, pp. 489–504, 2008.

[37] A. Hevner and S. Chatterjee, "Design science research frameworks," *Design Research in Information Systems: Theory and Practice*, pp. 23–31, 2010.

[38] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[39] J. Kasurinen and M. Kettunen, "Learning cyber security: Teaching technically challenging topics with games and virtual laboratories," *International Journal on Information Technologies and Security*, vol. 10, no. 3, pp. 103–114, 2018.