Lizards in the Street! Introducing Cybersecurity Awareness in a Digital Literacy Context

Mark Frydenberg
mfrydenberg@bentley.edu
Computer Information Systems Department
Bentley University
Waltham, Massachusetts

Birgy Lorenz
birgy.lorenz@ttu.ee
School of Information Technologies
Tallinn University of Technology
Tallinn, Estonia

Abstract

Learning cybersecurity awareness builds on basic information technology concepts and digital literacy skills. In an effort to raise cybersecurity awareness among information technology students, this paper describes a series of three different interactive sessions offered to students of all levels at a business university. The sessions introduced cybersecurity awareness through identifying actual breaches and incidents, using open source intelligence tools, and participating in a capture the flag style competition. Student comments in blog posts and interviews after these sessions show the relevance of cybersecurity awareness in their daily lives and a general sense of surprise, amazement and concern at how much personal information is readily available online.

Keywords: cybersecurity awareness, digital literacy, open source intelligence tools, hacking competition

1. INTRODUCTION

Skills and competencies related to cybersecurity awareness are often included as part of courses in digital, computer, or information literacy, or as elements of life-long learning. (Ala-Mutka, Punie, & Redecker, 2008; *AP Computer Science Principles*, 2017; Chinien & Boutin, 2011) These "21st Century Skills"(van Laar, van Deursen, van Dijk, & de Haan, 2017) are vital at home, at the workplace and to function in society. Despite the perception that today's digital natives (Prensky, 2012) are tech savvy and have been born with a security mindset, having a baseline set of knowledge, skills, and abilities can go a long way toward developing core cybersecurity competencies common to many work roles (Dawson & Thomson, 2018).

Universities have introduced technical degree programs in cybersecurity to meet industry demand for graduates with specialized skills. Some courses include in-class exercises using online tools to provide hands-on experience of technical concepts such as virtualization and infrastructure automation (Marquardson, 2018), and performance testing in an isolated environment (Marquardson & Gomillion, 2018).

Cybersecurity awareness related skills often are much more applied, focusing on competencies such as good password management (using different secure passwords, storing passwords safely using a password manager, two-factor authentication), recognizing phishing attempts, detecting malicious emails, and using open source intelligence (OSINT) tools. Combining intuition, curiosity and the ability to search and analyze data gathered from the Internet and other open sources is a powerful skill to detect fake news, scams, and social manipulation in the world. (Bada, Sasse, & Nurse, 2019; Wells, Conflict, & Gibson, 2017)

Digcomp, a digital competence framework for European citizens, (Carretero-Gomez, Vuorikari, & Punie, 2017) presents competencies to protect devices and personal data from risks and threats in digital environments, and applies cybersecurity skills to realistic employment scenarios, such as the use of social media in a corporate environment. While the United States National Cyber Strategy ("National-Cyber-Strategy.pdf," 2018) points out the need to protect networks, services and information, and secure critical infrastructure, Despite all of the technology precautions in place in the workplace, organizations are realizing that humans are still the weakest link in cybersecurity (Boulton, 2017; Postimees, 2019; Zimmermann & Renaud, 2019). As an example, one recent study found that most novice users do not know how to encrypt their email messages.(Ruoti et al., 2016)

"Some say that the average computer user simply lacks knowledge and awareness of cybersecurity issues and of the secure behaviors they ought to be carrying out… [and] other researchers argue that users do not care about possible consequences, [and] are unmotivated to take responsibility." (Zimmermann & Renaud, 2019, p. 4)

2. CYBERSECURITY AWARENESS AND DIGITAL LITERACY

Cybersecurity awareness relies on individuals knowing basic ways that they can protect themselves, their data and their devices. The foundation of that awareness may be found in developing basic technology and digital literacy skills.

Digital Literacy Skills

Digital literacy skills have evolved from gaining proficiency with productivity tools, email, the World Wide Web, social media, collaboration tools, mobile devices and the cloud (Dijk & Deursen, 2014; Frydenberg & Press, 2010) to creating, organizing, sharing, and reusing online content, accessing information across devices and platforms, and maintaining privacy and identity online. (Wheeler, 2010)

When learning about cybersecurity, introductory IT courses often cover the importance of communicating safely online, demonstrating the use of computers safely and responsibly, making judgment about digital content when evaluating and repurposing it for a given audience, demonstrating responsible use of online services; selecting, combining, and using Internet services; understanding the potential of information technology for collaboration when computers are networked; using online services securely; recognizing that persistence of data on the Internet requires careful protection of online identity; understanding ethical issues surrounding the application of information technology. (*AP Computer Science Principles*, 2017; Harris & Patten, 2015) These digital literacy skills are crucial for mastering cybersecurity awareness.

Cybersecurity Skills

Stenmap (Mäses, Randmann, Maennel, & Lorenz, 2018) is a model to classify cybersecurity-related skills. Competencies range from non-cybersecurity specific to cybersecurity-specific skills along the horizontal axis, and non-technical to technical skills along the vertical axis.

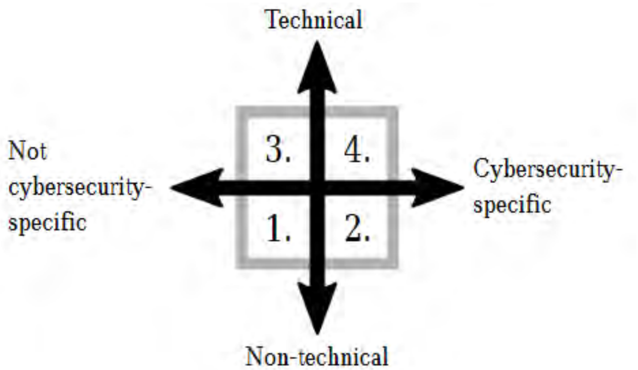
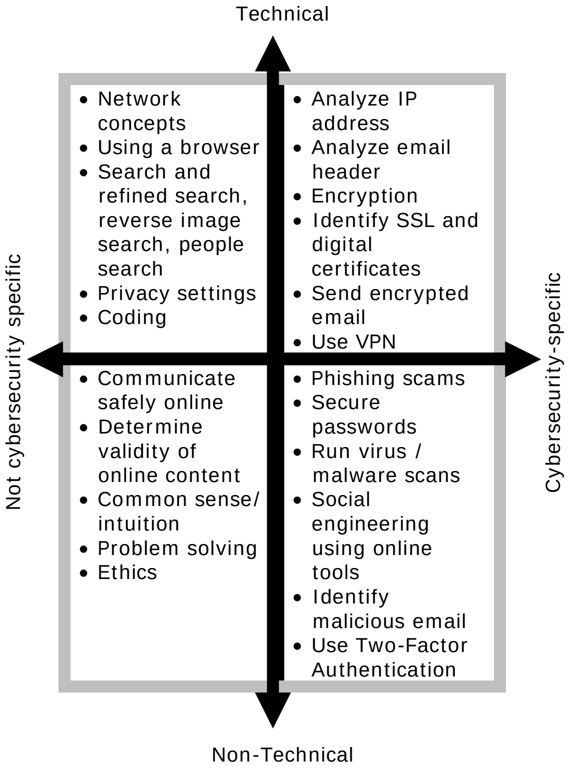


Figure 1. Classifying Cybersecurity Skills

Quadrant 1 includes skills that are non-technical and not cybersecurity-specific, such as leadership and communication skills. Team and group exercises require these highly valued skills. Quadrant 2 includes skills that are cybersecurity-specific, but non-technical, such as identifying phishing emails or the importance of secure passwords. Quadrant 3 includes technical skills that may not be cybersecurity related, such as coding and basic understanding of browsers or the Internet. Quadrant 4 requires skills that are both technical and cybersecurity-specific, such as implementing encryption or an SQL injection attack.

Mäses notes that "it is not always easy to position a skill in this Cybersec-Tech window. For example, skills related to reporting could be general nontechnical or very specific and technical. Nevertheless, this Cybersec-Tech window can help to facilitate a discussion about which skills a cybersecurity exercise should target."(Mäses et al., 2018, p. 9)

Figure 2 adapts Figure 1, listing specific digital literacy skills and where they fall within the Stenmap model:



- Network concepts
- Using a browser
- Search and refined search, reverse image search, people search
- Privacy settings
- Coding

- Analyze IP address
- Analyze email header
- Encryption
- Identify SSL and digital certificates
- Send encrypted email
- Use VPN

- Communicate safely online
- Determine validity of online content
- Common sense/ intuition
- Problem solving
- Ethics

- Phishing scams
- Secure passwords
- Run virus / malware scans
- Social engineering using online tools
- Identify malicious email
- Use Two-Factor Authentication

Figure 2. Applying Digital Literacy Competencies to Cybersecurity Skill Classifications

The AP College Board, in its computer science principles course, posits that "cybersecurity is an important concern for the Internet and the systems built on it."(*AP Computer Science Principles*, 2017, p. 34) Students should be able to identify existing cybersecurity concerns and potential options to address them. Issues of awareness mentioned include impact of DDoS attacks, hardware, software, and human components of cybersecurity; phishing, viruses, and other attacks; foundations and applications of cryptography; digital certificates. In the AP College Board Computer Science principles course, the focus on cybersecurity awareness is from an Internet-based perspective.

Open Source Intelligence Tools

Open source intelligence (OSINT) tools have emerged as an important components for locating, organizing, and differentiating recognizing new types of relevant information online. (Glassman & Kang, 2012) OSINT information and data include social media sites and online social networks, public records databases, photos, maps, and images, online surveillance cameras, code repositories, media websites. OSINT tools include special purpose search engines and other applications that can quickly gather and analyze data from hundreds of websites, perform fact-checking, scan files for viruses and malware, and determine the technology platforms used on a website. (Kissiah & eInvestigator.com, 2019)

Knowing the appropriate tools makes it possible to perform tasks such as determining which social networks have a given username registered, searching for photos and images to determine their authenticity, evaluating a user's Twitter habits; identifying common patterns in user passwords, encoding messages and files, obtaining information from an IP address search, and analyzing email headers. Knowing about several of these tools is one way to demonstrate cybersecurity awareness and digital literacy skills.

Guiding Questions

Given the importance of raising cybersecurity awareness among students from both technology and general backgrounds, the following guiding questions for this study emerge:

- What concepts, skills, and applications must students know to demonstrate cybersecurity awareness?
- What OSINT tools can students use to prepare for the cybersecurity challenges that they will face?
- How can these be presented in ways that introduce or reinforce digital literacy concepts and skills that students learn in an introductory IT course?

3. METHODOLOGY

To provide outside of class, informal opportunities for students to learn about cybersecurity, the presenter offered three 80-minute interactive sessions on cybersecurity topics, biweekly between February 5 and March 5, 2019. Sessions were open to all students at XXXXXXX University, a business university in XXXXXXXXXXXXX. The topics of these sessions are shown in Table 1:

Table 1. Cybersecurity Awareness Session Topics

Session 1	Cybersecurity Stories
Session 2	Open Source Intelligence Tools and How to Hack through Search
Session 3	Capture the Flag (CTF) Style Hacking Competition

While the three cybersecurity awareness events were not tied to a single course, instructors of introductory IT, web design, database, cybersecurity, and other undergraduate CIS courses encouraged their students to attend. In addition, two IT instructors and two technology administrators on campus attended two of the sessions.

Participants self-selected to attend these events, and used their own devices (laptops, tablets or mobile devices). Some instructors offered extra credit to students in their classes who wrote a short report after attending. An average of 20 participants attended each session, with 24 participants attending the final CTF session. Session 2 on OSINT Tools was recorded, and the video posted online for the benefit of students who were unable to attend, or who wanted to review prior to the competition in Session 3. The study used an action research method (Johnson, 2012) where the presenter was actively participating in the lectures as a facilitator and as the source of cybersecurity facts.

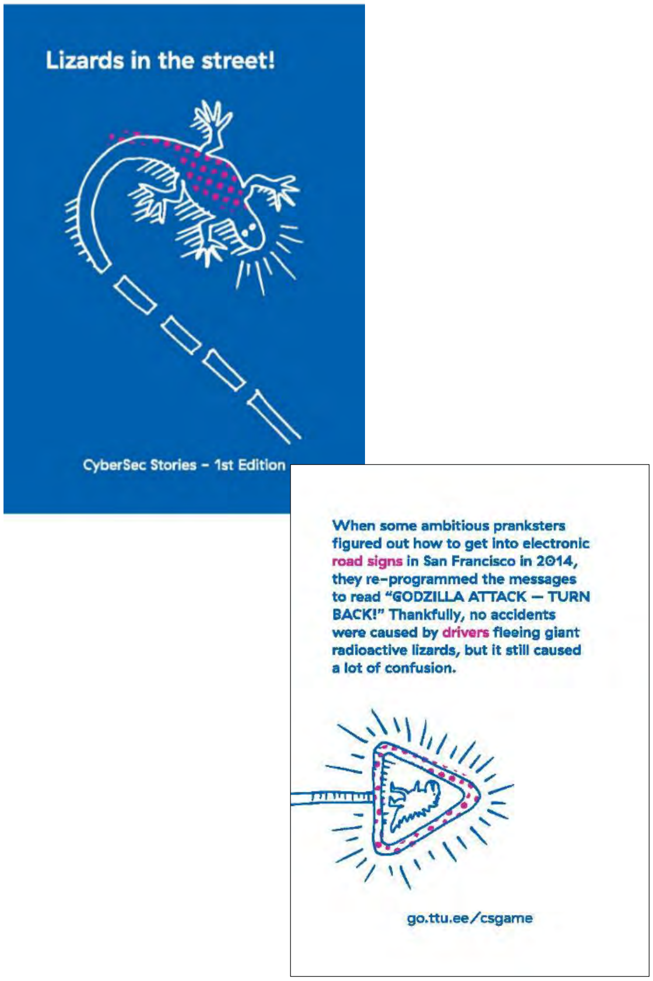
Each session took place in a technology lab where students sat at tables to facilitate group work; the room had two projection screens for participants to see the presenter's slides easily. The first two sessions were methodologically lecture with hands-on practice exercises and the final CTF session was structured as a team competition.

Session 1: Cybersecurity Stories

The first presentation provided a general overview of cybersecurity concepts and cases that happen in Internet realms. The content of the sessions were text, pictures, videos, a game called CyberSec Stories 1 (Lorenz, 2018) and open discussion. CyberSec Stories is a card game focusing on various security cases in the digital world. The game was developed by persons that are involved with Tallinn University of Technology Centre for Digital Forensics and Cyber Security scientists, lecturers, students, and partners. The game consists of 54 cases that help to raise overall awareness of cybersecurity. Players take turns reading a short headline on the card (such as, "Lizards in the street!") and then try to guess what happened. The reverse side of each card contains a short summary of the case for members to read to give clues to their teammates, or the team can search online to find out more information.

A sample game card is shown in Figure 3. "Lizards in the street!" refers to an electronic road sign in San Francisco that was hacked to read "Godzilla Attack! Turn back!" (Rosenblum, 2014) All of the game cards for CyberSec Stories 1st Edition are available at https://sites.google.com/view/tty-csgame/.

Topics include how big is the Internet today and how the hacker mindset works. Cases discussed included how to crash a car with piece of paper; who one becomes professional with just typing spaces; why a digital company might need to force everyone to use paper systems for 6 months; why companies in Ukraine infected their own systems with virus; trusting people because of face value or because they wear a uniform; how to deal with ransomware and what can happen when you answer spam email.



When some ambitious pranksters figured out how to get into electronic road signs in San Francisco in 2014, they re-programmed the messages to read "GODZILLA ATTACK — TURN BACK!" Thankfully, no accidents were caused by drivers fleeing giant radioactive lizards, but it still caused a lot of confusion.

Figure 3. Front and back of a CyberSec Stories game card.

The presentation concluded with a discussion of minimal cybersecurity skills that students need to function in the world today, and students shared their own cybersecurity stories and experiences.

Session 2: Open Source Intelligence Tools

The second session featured a presentation on Open Source Intelligence (OSINT) tools to find and determine the validity of online information. The presentation included slides, videos, small group exercises, and open discussion. Topics included three different hats of a hacker (white, gray, and black); the term *OSINT*; and several OSINT tools to locate analyze online data.

Appendix I Table 1 contains several OSINT tools, many of which were demonstrated during this session.

Students tried some of the OSINT tools working in small group exercises. Exercises had them create a fake online persona using websites to generate fictitious names, locations, occupations, and profile photos; they completed a phishing quiz; analyzed information available from their IP address, and determined if their personal account information has been compromised in a recent data breach.

Session 3: Capture the Flag Competition

The series concluded with a Capture the Flag (CTF) style competition where participants worked in self-selected teams to solve cybersecurity-related challenges or evaluate truthful information online. The puzzles were of varying difficulty and required participants to exercise different skill sets to solve. Many of the solutions involved using OSINT tools presented in the previous session.

"In the cybersecurity world, 'capture the flag' competitions are the simulated crucible in which the curriculum lessons are tested and validated by the students. Instead of a playing field with physical flags to capture, … teams defend and attack computer networks and the flags are data and services that are either preserved or disabled."(Serapiglia, 2016, p. 28) Some CTF competitions may last for a few hours, a day or more; participants may be students, enthusiasts, or professionals. Players can attempt the various challenges individually, or they can work with team members to attempt to score the highest number of points. Once an individual challenge is solved, a flag, or code value, is given to the player and they submit this flag to the CTF server to earn points.

Exercises included: looking at secret data contained in a file (GPS address, additional text inside the picture); detecting problems such as missing hardware components in a computer; analyzing pictures to find a password; decrypting code or solving puzzles using mobile phone, base64 encoder, and a book; analyzing email headers; and finding an alternative way to access websites that have been geoblocked. (Geoblocking is a means of refusing incoming requests for web content that originate in specific countries.)

Many of the solutions relied on students grasp of digital literacy skills and technology concepts: understanding parts of a URL, recognizing an IP address, using a search engine effectively, evaluating social media posts; using productivity software, and other topics. Students were given hints as needed once the competition was underway.

Sample CTF exercises and puzzles are shown in Appendix 2. Please contact the authors for more information.

4. RESULTS AND DISCUSSION

The authors gathered immediate feedback after each session and feedback within two weeks after the final session by asking students enrolled in an introductory technology concepts course to write a short blog post describing their impressions and lessons learned and what they think college students should know about cybersecurity. The authors also discussed with faculty teaching the Introductory Computing Concepts course about possibilities and challenges to integrate some of these cybersecurity awareness exercises and concepts in the current course.

Sessions 1 and 2 Debrief

Session 1 discussions analysis show the topics raised from the first session: the idea was to talk about actors on the internet, connect history into modern world and inventions and discuss what competencies one should have when finishing their college experience. Usually, in awareness sessions, people tend to talk about social media and passwords, here the talk went to a deeper level - related more on technology and its possibilities. Session 2 topics analysis focused more on OSINT possibilities, also how hackers think, how phishing is done (different techniques to detect hacking, malicious content), developing a fake online persona, using fake pictures and videos, social engineering and ethics.

Exercises chosen for Session 2 were based on applying common digital literacy skills to demonstrate cybersecurity competencies. OSINT exercises were related to finding information from the Internet, such as identifying photos of real and fake Picasso works of art.

Steganography, the practice of concealing information within a message, image, or video file, was used to demonstrate how one might hide information inside a file, analogous to how hackers might hide malicious code in email attachments. Forensics exercises let participants detect phishing and viruses from the email header or hash analyze changes in the server or website; GPS exercises let participants discover how to find out where a picture was taken. Hardware exercises taught about how the computer is made, how the network is built. Cryptography exercises helped participants understand secret codes and language ciphers.

Most worrisome and interesting to participants were discussions about hackers, viruses and how to analyze malicious emails, OSINT and its techniques and social engineering.

Students' and teachers' feedback centered around how to detect problems, gather evidence and get to know all these cases on a deeper level. Discussions around competencies listed the need to have overall awareness and understanding how the Internet works.

Discussions also showed that there has not been a conversation about what kind of security skills should one have when finishing university. Teachers identified links between cybersecurity awareness and critical thinking; students were much more practical in wanting to learn tangible skills such as understanding passwords habits and how to deal with constant flow of emails (spam and phishing attacks), or even whom to turn when something happens. without being ashamed. When completing the hands-on activities, participants wanted to know which OSINT tools and websites to use to solve the exercises.

The sessions also brought up ethical discussions of issues such as: Who is to blame when code is insecure? Who is responsible for the security of personal data stored online?

Session 3: CTF Debrief

In Session 3, the CTF competition, of the 80 minutes available, 10-15 minutes were used to give an introduction and organize groups; 50 minutes were available to complete the activity, and 15-20 minutes at the end were available to debrief. The presenters learned that the time available for the exercise (approximately 50 minutes) was insufficient to complete most of the 25 exercises provided. Students solved most of the easier level OSINT exercises as they were most used to using Google or another search engine to gather answers for homework or personal life needs. For example, exercises had students find the default password for a Wi-Fi router or detect a missing word from a news headline. Students were also successful in completing the visual exercises (such as to find a password from a photo taken in a professor's office). Hardest exercises (most of which were not solved) were related to cryptography, analyzing code form the website or computer screen from server logs. It was interesting that even though the best teams accomplished approximately one-third of the exercises and need to strategize on how to do them, they were so happy that they had used the computer and developed critical thinking skills by solving puzzles, detecting problems and proposing solutions.

Feedback showed that most of the groups (8 groups, 3 people in each) found different exercises that were interesting to them and from what they were empowered the most. A similar theme was that when they worked in a team to help each other rather than working individually, they accomplished more; also solving the hardest exercises on which they spent most of their time were those that impressed them the most. They pointed out various tools and websites they learned about during the session.

Student Comments

After attending at least one of the three sessions, several participants wrote blog posts on "What should the college students know and learn about cybersecurity?" Feedback from student blogs (which were completed within two weeks of the final session) showcased the relevance of cybersecurity awareness in their own lives. The biggest impact topics were how to use search tools, logical filtering and social engineering skills to acquire information about people, places, companies and how to analyze it as a hacker would; and how to analyze data (website, email, personal) legitimacy for updating the defense of being phished.

One student said: "I feel as though many students are unaware of many issues that come along with cybersecurity or lack thereof in this case. Throughout this year, I and many other students, have received countless phishing emails that cause devices to obtain viruses if you click a certain link. Towards the beginning of this year, it was obvious when an email was a scam, however, more recently it seems like they have been disguised a lot better. For example, I received emails that were from my close friends about topics that we both had sent or received emails about. This made me realize that because a friend of mine was hacked, hackers had some of my information as well. An email about a cheer event was sent to me from my teammate's email account and was very believable until I realized the suspicious layout of the email. Overall, I believe it'd be useful to include one class during the IT101 course that is devoted to identifying when an email is unsafe and how to prevent viruses from computers."

Students pointed out a better understanding of how to use safety precautions (need for more complex passwords, contained online presence, evaluated use of media tools) and minimize risks as in the process of exercises they could experience being also in the attacker side. At the end of the sessions, they did an audit of their own devices and environments, and passwords to improve their online safety and experience.

Privacy was a concern for students from the point of view of a consumer and a marketer. One future marketing major suggested:

- ○ Discuss clearing cookies how does this have an impact on marketers? Why or why not should cookies be cleared?
- ○ Discuss privacy in terms of social media advertisements. What do timely, relevant ads mean for the consumer?
- ○ Discuss the legality and ethics behind big data and privacy. Why should there be a federal definition of what big data is?
- ○ Discuss privacy - example how can we tell when a job offer is a scam? Is the offer from social media or sent by email legit?
- ○ Should information like our social security number, financial information of other information be submitted on an application?

Students commented on what they thought they knew about cybersecurity before the session, and the lessons they learned: "Before this class I feel like I had the general knowledge of cybersecurity that comes with growing up in my generation. Certainly, always err on the side of caution and assume non trusted sites and emails are not safe. I did know that you were supposed to change your password frequently and that passwords should be a complex variation of numbers, letters, and symbols. I did not know there were sites that you could run emails and other media through to scan for viruses. I also learned a lot about the variations of different viruses and malware. Aside from viruses and malware this is also a whole section of cybersecurity which directly involves protection from hackers and people. People who use the internet to attack others can do so in a variety of ways. Even social hacking can be implemented to steal information about someone from a third party which you assume would be secure."

Students were taken by the amount of information available through social media posts. Said one student: "It can be surprising how much information that someone can find about you just by looking at old tweets or Instagram posts. College students are already aware of employers looking through social media accounts, but they need to be more aware about what they post because cyberhackers can find anything. I believe that this big lesson in here is, do not post things that you do not want strangers to find out about you."

Said another student: "At the cybersecurity workshop, I learned lots of different methods to approach our computers and personal information. The most important one for me is the email with links. Once people click into the links, their personal information would be taken by hackers. We were taught how to distinguish real or fake emails. Basically, we look at the senders and other information in the email to make sure its authority. And if we click into links or accidentally go into random websites, we do not give out any personal information including bank information. I think that is important because it is close to our life. Other things that people should know is how to protect their all kinds of accounts. Such as how to make sure no one logs in their accounts."

Some also got inspired by the exercises to develop decoding experiences for others, others had more inspired by learning more about ethical hacking overall or history of cybersecurity. A few people also asked about career possibilities in the field. Students also wanted to know how hacking works (from the actions of the hacker, providing demonstrations) and how to recover after being hacked, clicking a bad link, or sharing information that should have remained private.

Students' concerns with cybersecurity also had to do with keeping their phones safe, protecting their social media data, not being taken by phishing scams, and determining the validity of online information.

5. CONCLUSIONS AND FUTURE WORK

Developing cybersecurity awareness skills is crucial for preparing students to take their place as information technology workers in their future careers. The ability to detect spam, phishing, malware, and other attacks, as well as the ability to maintain privacy of one's information online and determine the validity of information online are valuable skills whose foundations require basic digital and technology literacy skills.

This paper presented a model for classifying cybersecurity skills within the context of digital literacy and described three different sessions for raising cybersecurity awareness at a university through an interactive game, open source intelligence tools, and a capture the flag style competition Any of the three sessions can be incorporated into a technology concepts course or shared as an extracurricular activity to raise cybersecurity awareness. Student results suggest that these sessions were informative and increased interest in keeping students' data and devices safe.

In future iterations of this project, the authors will update and present current OSINT tools, describing use-cases that demonstrate their application. Another goal is to modify the CTF competition exercises to be more attainable given the time allotted and will examine them to ensure a balance between categories in Mäses model for describing cybersecurity skills.

The rise of cybercrimes, the ongoing security breaches, the continuing threats of malware and ransomware, the growth of phishing and other online scams, and the ease in which misinformation can spread online all necessitate making students aware of cybersecurity issues, and teaching them to use OSINT tools to protect themselves and the organizations that will employ them, from cybersecurity attacks.

Teaching cybersecurity awareness in the university and training employees in the workplace can be a challenge due to the lack of experts in this field. Developing solutions, tools to automate the process, and activities that will spark students' interest will benefit students, teachers, and society at large. Ethics issues will emerge as users will need to trust systems using current technologies such as artificial intelligence, Internet of Things, or blockchain, that they may not fully understand. Universities also should look beyond their current cybersecurity needs to predict future developments and how to incorporate the impact of these and other current technologies in the cybersecurity awareness curriculum for information technology students.

6. REFERENCES

Ala-Mutka, K., Punie, Y., & Redecker, C. (2008). *Digital Competence for Lifelong Learning. Policy Brief*.

AP Computer Science Principles. (2017). Retrieved from https://apcentral.collegeboard.org/pdf/ap-computer-science-principles-course-and-exam-description.pdf

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* 11.

Boulton, C. (2017, April 19). Humans are (still) the weakest cybersecurity link. Retrieved July 7, 2019, from CIO website: https://www.cio.com/article/3191088/humans-are-still-the-weakest-cybersecurity-link.html

Carretero-Gomez, S., Vuorikari, R., & Punie, Y. (2017, April 28). DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use [Text]. Retrieved July 3, 2019, from EU Science Hub - European Commission website: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-21-digital-competence-framework-citizens-eight-proficiency-levels-and-examples-use

Chinien, C., & Boutin, F. (2011). *Defining Essential Digital Skills in the Canadian Workplace: Final Report*. 87.

Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology*, *9*. https://doi.org/10.3389/fpsyg.2018.00744

Dijk, J. van, & Deursen, A. van. (2014). *Digital skills: Unlocking the information society* (First edition). New York, NY: Palgrave Macmillan.

Frydenberg, M., & Press, L. (2010). From Computer Literacy to Web 2.0 Literacy: Teaching and Learning Information Technology Concepts Using Web 2.0 Tools. *Information Systems Education Journal*, *8*(10). Retrieved from https://eric.ed.gov/?id=EJ1146965

Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, *28*(2), 673–682. https://doi.org/10.1016/j.chb.2011.11.014

Harris, M. A., & Patten, K. P. (2015). Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum</title>. *Journal of Information Systems Education*, *26*(3), 219.

Johnson, A. P. (2012). *A short guide to action research* (4th ed). Upper Saddle River, N.J: Pearson.

Kissiah, M., & eInvestigator.com. (2019, February 4). Open Source Intelligence Tools and Techniques for Investigations. Retrieved July 7, 2019, from Private Investigator and Investigation Resources website: https://www.einvestigator.com/open-source-intelligence-tools/

Lorenz, B. (2018). CyberSec Stories 1st Edition. Retrieved July 2, 2019, from https://sites.google.com/view/tty-csgame/

Marquardson, J. (2018). Infrastructure Tools for Efficient Cybersecurity Exercises. *Information Systems Education Journal*, *16*(6), 23.

Marquardson, J., & Gomillion, D. (2018). Cyber Security Curriculum Development: Protecting Students and Institutions While Providing Hands-On Experience. *Information Systems Education Journal*, *16*(5), 12.

Mäses, S., Randmann, L., Maennel, O., & Lorenz, B. (2018). Stenmap: Framework for Evaluating Cybersecurity-Related Skills Based on Computer Simulations. In P. Zaphiris & A. Ioannou (Eds.), *Learning and Collaboration Technologies. Learning and Teaching* (Vol. 10925, pp. 492–504). https://doi.org/10.1007/978-3-319-91152-6_38

National-Cyber-Strategy.pdf. (2018, September). Retrieved July 4, 2019, from National Cyber Strategy website: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Postimees. (2019, April 1). Editorial: The weakest link in cyber security is human. Retrieved from https://arvamus.postimees.ee/6559321/juhtkiri-kuberturvalisuse-norgim-luli-on-inimene

Prensky, M. R. (2012). *From Digital Natives to Digital Wisdom: Hopeful Essays for 21st Century Learning*. Corwin Press.

Rosenblum, G. (2014, May 15). SF Traffic Sign Hacked To Warn Drivers Of "Godzilla Attack." Retrieved July 2, 2019, from https://sanfrancisco.cbslocal.com/2014/05/15/prank-san-francisco-street-hack-godzilla-warning-sf-traffic-sign-hacked-to-read-godzilla-attack/

Ruoti, S., Andersen, J., Heidbrink, S., O'Neill, M., Vaziripour, E., Wu, J., … Seamons, K. (2016). "We'Re on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 4298–4308. https://doi.org/10.1145/2858036.2858400

Serapiglia, A. (2016). The Case for Inclusion of Competitive Teams in Security Education. *Information Systems Education Journal*, *14*(5), 25.

van Laar, E., van Deursen, A. J. A. M., van Dijk, J. A. G. M., & de Haan, J. (2017). The relation between 21st-century skills and digital skills: A systematic literature review. *Computers in Human Behavior*, *72*, 577–588. https://doi.org/10.1016/j.chb.2017.03.010

Wells, D., Conflict, M., & Gibson, H. (2017). *OSINT FROM A UK PERSPECTIVE: CONSIDERATIONS FROM THE LAW ENFORCEMENT AND MILITARY DOMAINS*. 32.

Wheeler, S. (2010, November 2). Digital literacy 1: What digital literacies? Retrieved July 7, 2019, from Learning with 'e's website: http://www.steve-wheeler.co.uk/2010/11/what-digital-literacies.html

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*. https://doi.org/10.1016/j.ijhcs.2019.05.005

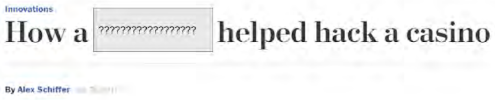
Appendix 1. OSINT Tools

Table 1. Open Source Intelligence Tools for Cybersecurity Awareness

Try this tool:	To accomplish this task:	At this web address:
Base64	Encode or decode data to / from base 64	https://www.base64encode.org/
BuiltWith	Determine a website's Content Management System and other technologies	https://builtwith.com
Check Usernames	Check availability of usernames on social networks	https://checkusernames.com/
Decode Ciphers	Encrypt / Decrypt SMS messages with T9 mode	https://www.dcode.fr/t9-cipher
Gaijin	Analyze Email Header to determine sender and recipient	https://www.gaijin.at/en/tools/e-mail-header-analyzer
Google Image Search Tin Eye	Reverse image search	https://images.google.com/ https://tineye.com
Have I Been Pwned?	Determine if your personal data has been compromised	https://haveibeenpwned.com/
IPLocation	Analyze IP address and details	https://www.iplocation.net/find-ip-address
Panopticlick	Determine if you are trackable in your browser	https://panopticlick.eff.org/
Phishing Quizzes	Learn about Phishing	https://phishingquiz.withgoogle.com/ https://www.sonicwall.com/en-us/phishing-iq-test-landing https://www.opendns.com/phishing-quiz/ https://accellis.com/phishing-quiz/
PhoneSpell	Encode a phone number to words	https://www.phonespell.org/
RandomUser UI Faces Fake Name Generator Fake Person Generator	Develop a fake identity online	https://randomuser.me/photos https://uifaces.co/ https://www.fakenamegenerator.com https://www.fakepersongenerator.com
Scam Advisor	Determine if a website is safe (http vs https)	https://www.scamadviser.com/
SleepingTime	Determine sleep patterns based on Twitter usage	http://sleepingtime.org/
Social Catfish	Find a person by a photo or social media information	https://socialcatfish.com/
VirusTotal	Analyze a suspicious file or web address to detect malware	https://www.virustotal.com
Web Mii Pipl	Find information about a person	http://webmii.com/ https://pipl.com/

Appendix 2. Sample CTF Exercises and Puzzles.

What word is missing?

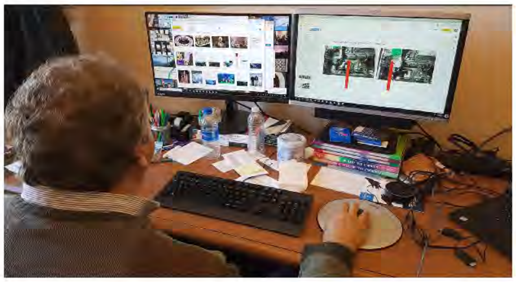


Innovations

How a ?????????????????? helped hack a casino

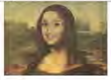
By Alex Schiffer

What's my password?

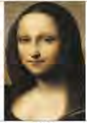


Create the sequence of numbers corresponding to photos that are not fakes.

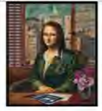
112



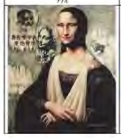
078



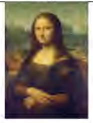
221



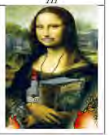
774



198



222



You have received a letter from your coach in the file list.exe

Hash is:
SHA-256:
24d004a104d4d54034dbcffc2a4b19a11f39008a575a
a614ea04703480b1022c

What does the message say?

We have intercepted a message from a well-known cybercriminal gang… try to decrypt it:

8444447777 4447777 66688777 2224426622233
933 633338 28 83366 76
7777337277733 9996668877777733555333

Crack a Wi-Fi Network

Open Wi-Fi networks can be a security risk. A service provider set up the Wi-Fi at your grandmother's house using an Asus RT-AC66U router.

The device is in the factory settings/configuration.

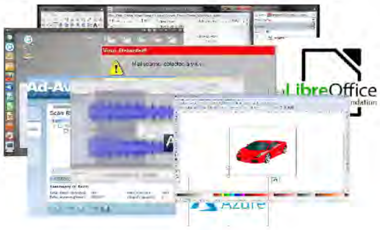
What is the default user name and password?

In a study with 10-12th graders, what is the correct descending order of situations that they have experienced?

A. Friends shared pictures of me in public that I did not agree to
B. I posted publicly information that I should not
C. Never happened anything of that kind
D. My phone is missing or stolen
E. Someone accessed my data without permission
F. Someone hacked my social media account
G. Someone hacked my email

Know your programs
Pair the program topic and the original software name. Flag is the first letters of the programs original names. Be sure to use the original name or the program!!

- Office software
- Virus
- Operating System
- Vector graphic program
- Raster graphic program
- Audio program
- Antivirus
- Removes adware and spyware
- Cloud software

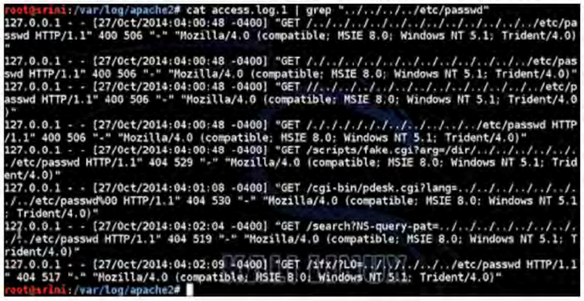


What's the address where this photo was taken?

- Analyze the domain name https://www.betterinternetforkids.eu/
- Who owns it?

- The LA Times website (www.latimes.com) is not visible for EU Citizens because of the GDPR challenges.
- List different ways how one can still see the website and find out news from example 1.09.2018 morning.

What happened?
What was accessed?
What is the name of this type of hack?



```
root@srini:/var/log/apache2# cat access.log.1 | grep "../../../../etc/passwd"
127.0.0.1 - - [27/Oct/2014:04:00:48 -0400] "GET /../../../../../../../../../../../etc/pa
sswd HTTP/1.1" 400 506 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
"
127.0.0.1 - - [27/Oct/2014:04:00:48 -0400] "GET /./../../../../../../../../../../etc/pas
swd HTTP/1.1" 400 506 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
127.0.0.1 - - [27/Oct/2014:04:00:48 -0400] "GET //../../../../../../../../../../../etc/p
asswd HTTP/1.1" 400 506 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0
)"
127.0.0.1 - - [27/Oct/2014:04:00:48 -0400] "GET /./././././././../../../../../etc/passwd HTTP
/1.1" 400 506 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
127.0.0.1 - - [27/Oct/2014:04:00:48 -0400] "GET /scripts/fake.cgi?arg=/dir/../../../../../.
./etc/passwd HTTP/1.1" 404 529 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trid
ent/4.0)"
127.0.0.1 - - [27/Oct/2014:04:01:08 -0400] "GET /cgi-bin/pdesk.cgi?lang=../../../../../../.
./../etc/passwd%00 HTTP/1.1" 404 530 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1
; Trident/4.0)"
127.0.0.1 - - [27/Oct/2014:04:02:04 -0400] "GET /search?NS-query-pat=../../../../../../../.
./../etc/passwd HTTP/1.1" 404 519 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; T
rident/4.0)"
127.0.0.1 - - [27/Oct/2014:04:02:09 -0400] "GET /ifx/?LO=../../../../../etc/passwd HTTP/1.1
" 404 517 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
root@srini:/var/log/apache2# 
```