Cyber Threats to Education Technological Services: a Case Study

João Moreira[1] and Hugo Barbosa[2] [0000-0003-1205-8990]

[1] Lusofona University, Porto - Portugal, joaobaldomero@gmail.com
[2] Lusofona University, Porto - Portugal | SIIS - Social innovation and Interactive Systems, School of Engineering of the Polytechnic of Porto, Porto, Portugal
hugo.barbosa@ulp.pt

Abstract. Information Technology systems in education have been part of the day-to-day of many schools and academic communities for many years. Thanks to the Internet and these systems, all operations in schools have become more efficient, making this sector more dependent on them. But with the transition of these systems to the education sector, the threats posed to other institutions and businesses, have propagated to the learning institutions. This paper covers some of the cyber threats that schools handle and explores the impact that the lack of knowledge about some of the basic concepts of Cyber Security can pose to educational technology systems. The threats are shortly presented and analyzed as to how they pose a threat to schools' sensitive data, providing an overview at some of the Cyber Security essentials that aim to prevent attacks or mitigate the damage that some of these threats can cause. Throughout the last few years, awareness has been raised to the importance of Cyber Security and therefore this paper seeks to find how much the academic communities in Portugal know about the Cyber Security vital concepts, resorting to a survey conducted in schools throughout the country, with the intent to investigate the knowledge that common users have seized throughout the years.

Keywords: Education; Information Technology Systems; Cyber Security; Cyber Threats; Survey Analysis; Case Study.

1 Introduction

Over the last few years, more and more organizations have become dependent on information technology systems, with the education sector not being an exception. Academia has also become dependent on the Internet, therefore cyber security has become a major concern to schools. [1]

Cyber Security experts research the threats to the cyberspace, studying how hackers can perform their attacks, detect design flaws and exploit weaknesses. Different types of threats have appeared throughout the years, but research highlights malware as a key weapon on the attackers' arsenal. [2] Malware stands for "malicious software" and it envelops a vast array of threats, all with the same objective: the infection of the target system(s); although the approach to achieve infection will vary. Common tactics include, for example, the infection of a single machine and then propagation to other

machines or deceiving a user to click on a pop-up, hyperlink or file, which proceeds to execute a drive-by download that downloads viruses or tainted files. [3] Malware can present itself in a multitude of ways, the most commonly seen being viruses, trojans, ransomware, adware, worms and spyware. [4] It can infect systems easily, but it can also easily spread, through a multitude of ways, such as an infected flash drive, through a phishing email or website or bundled with legitimate software, making it hard to contain, since it can affect systems at any point of their life cycle. Malware possesses many options of infection, spreading capabilities and an extensive span of possible victims, which include users, network devices and servers, making it one of the fastest growing and evolving threats that the cyberspace faces. [3]

Malware has the spotlight when cyber security is discussed and despite the fact that it's dangerous, it's not the only threat the cyberspace needs to face. Other threats like social engineering have come into the limelight recently and they pose just as big a threat as malware. [5]

Social Engineering is a broad term that encases a wide range of techniques that have the intent to deceive and exploit, applying different approaches in order to manipulate the common user into giving away any kind of private information. [6] These attacks attempt to bypass the cyber security systems that may be in place and exploit the human factor and, ultimately, deceiving the user. [1,7]

One of the most popular social engineering approaches is phishing. It involves a fraudulent process, masked to appear as a legitimate source while procuring to extract information from the user, usually camouflaged as a website or email. [5,8] Social Engineering exploits people through deception, making it an easy way to acquire information through the most vulnerable factor in the system, the people who use it. [9]

This paper aims to give an overview of the risks and threats to schools and their information systems. Schools are equipped with the tools to fend off attacks, however, good network design that is prepared to handle external threats is critical. It is crucial to educate the common users about basic cyber security concepts and practices.

The first section, divided into 3 parts, will analyze threats to the education technological services, exposing the major threats and risks that schools may be exposed to.

The second section presents the analysis of a survey performed in a few Portuguese schools, the results of which are the outcome of the data gathering of various members of the academic community surrounding the schools, addressing users about their basic knowledge about Cyber Security and day-to-day habits.

2 Cyber Threats to Education: An Overview

Cyber Threats are malicious acts that seek to gain unauthorized access to systems, aiming to damage the integrity of the data, sensitive or otherwise, present within the system by stealing or damaging it or just to disrupt a system or network, interrupting the system's normal life cycle. Cyber Threats are what Cyber Security aims to prevent and protect against.

2.1 Cyber Threats to the Education Technology Services

The expansion of technology services to schools provided advantages and disadvantages. It allowed professors and students to work more effectively, but with progress came some downsides; these being the threats that can potentially damage the school and its intellectual property. [10] Despite the raise in awareness over the years and investments made in Cyber Security, schools have become victims of cybercrime. [11] School systems are notoriously prone to attacks since they present themselves as an exploitation possibility with multiple avenues, as many schools possess a very lackluster Cyber Security infrastructure that, often, isn't capable of handling many of the prevalent threats. [12] Since schools are institutions that have had a significant growth in the amount of digital information acquired, it becomes difficult to implement Cyber Security measures, which leads to a problematic situation where the robustness of the Cyber Security infrastructure may have to be sacrificed, in favor of its simplicity, so the users can utilize the systems. [13]

In this regard, it's important to identify what the threats that impact schools are and that pose a risk to its technology services. The following list represents the types of threats that impact the Education sector: [14,15]

- Data Breaches,
- Malware-related Threats,
- Social Engineering Attacks,
- Denial of Service.

In the context of Education, the Privacy Technical Assistance Center describes data breaches as "any circumstance where a school's student data system is improperly accessed, compromised, or disclosed to a third party". [16] This threat can result in a wide array of complications, including identity theft, privacy violations and fraud. What makes data breaches hard to control and prevent is the many ways in which the data can be breached and leaked, which encompass theft through digital or physical means, human error, and hacking. [17]

Malware-related threats involve all sorts of malware. The most prevalent form of it is Ransomware, representing the second biggest threat type to education. These attacks can be in other forms like trojans, spyware, worms, and viruses. These malware-related threats have unique ways of operating and infecting devices, with the aim of gathering information, deleting, or altering data. [12]

Social Engineering Attacks involve different types of attacks, but the most common form is Phishing. Social Engineering is a method in which an attacker gathers information about a target through the exploitation of human weaknesses, using deception or manipulation to access sensitive information. [18] Phishing is a form of Social Engineering attack in which the attackers set out to obtain sensitive information through methods like malicious emails or websites that are designed to be as close to an admissible source as possible. [5]

Denial of Service (DoS) attacks are a major cyber threat, but it isn't as popular on the education sector, as only a slim percentage of attacks reported are DoS attacks. DoS attacks aim to exhaust the target's resources, attempting to minimize the target's service

performance or even stopping the service altogether. These attacks come in two major categories: Network Based Attacks, relying on the misuse of network protocols to flood the targets with requests, which will damage the victim's ability to provide service, and Host Based Attacks that exploit the victim's vulnerabilities found by attackers in systems or applications. [19]

2.2 The value and importance of schools' data

The education sector is a key target for attackers. According to the K-12 Cybersecurity Resource Center, in 2019, there were "348 publicly-disclosed school incidents" relating to cyber-attacks in various forms, representing a 200% increase in the number of incidents reported in 2018, displaying a worrying increase in the incident count. [14] Schools are reliant on their technology to manage and store the extensive amount of sensitive data gathered from the entire academic community (staff, students and parents).

Given these findings, it's important to analyze exactly what data most schools store and why it reaches the crosshair of hackers. Schools tend to deal with attacks by managing risks, which involves removing the source of the threat, addressing the vulnerabilities and lessening the impact by mitigating damage and restoring the regular functioning. The problem stems from the fact that these tasks are time and labor intensive, often only occurring after an attack as occurred. [20]

Schools are in possession of such a big array of data, storing an extensive amount of personal data, which comprises a big list of items, ranging from: student identification numbers, social security numbers, names, genders, race, addresses, dates of birth, city and country of residence, telephone numbers, email addresses, test scores and grades, information from members outside the student, faculty and staff group, like family members and alumni. [1]

Be it the sensitive information of students, faculty and staff or outside members, this amount of data turns schools into a bank of ample and valuable data, which puts a giant target on schools' backs [21]. Pairing the vast variety of valuable data with the fact that schools do not expend as many resources on Cyber Security as other sectors that are equally dependent on technology, we can identify a laid-back and complacent stance on a sensitive topic that can have brutal consequences. [22]

Considering the points above, it's important for schools to analyze threats and to implement techniques and best practices that allow them to better protect their information and to prevent attacks directed to their resources and IT systems.

2.3 Techniques and Best Practices Attack Prevention and Mitigation

Knowing the threats posed to Education, the value of the data and why it might be a target to intruders and attackers, it's important to know what measures to apply and how to mitigate the impact of a possible attack, taking on a proactive stance towards the Cyber Threats. In Cyber Security, it's important to take on a stance that aims to prevent and protect information and equipment, following the best practices and learning from worst-case scenarios to avoid being an easy target. [23]

The knowledge of the threats allowed us to develop techniques over the years, trying to evolve to protect against the constant surge of emerging threats. Below is a list with some of the mitigation techniques that can and should be applied, including a description of what each is and does. These are some of the most frequently used by organizations to protect the Cyber Space from the various Cyber Security Threats: [24]

- Implementation of Intrusion Detection Systems (IDS),
- Implementation of Anti-phishing Techniques,
- Implementation of Firewalls,
- Analysis of Anomalies in the Network Traffic,
- Implementation of Anti-malware software.

Intrusion Detection Systems are applications that provide constant monitoring of computer systems, alerting to when suspicious activity might be occurring. [25]

Anti-phishing techniques involve all sorts of techniques that we can implement to reduce the possibilities of a successful phishing attack. These techniques involve the use of email filters and content analysis, which is used to intercept spamming and phishing emails, the creation of Blacklists that contain a range of URLs that are known to be malicious and general best practices like only opening email attachments from trusted parties, never sending financial or personal information through email, using the latest versions of browsers, firewalls and IDS, and installing security patches when available. [26]

Firewalls are some of the most frequently implement mitigation techniques. "A firewall is a security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules". These devices can be hardware or software based or both. They are the first line of defense in network security, establishing a barrier between the internal network and the external networks. [27

Analysis of Anomalies in the Network Traffic encompasses the analysis of all the traffic that flows through the network, making use of patterns collected from normal traffic and comparing them to the current traffic, aiming to find anomalies, enabling the possibility of enhancing and refining the network security. [28]

Anti-malware software is often associated with the term antivirus. Although both have similar objectives, succinctly, Antiviruses primarily aim to defend systems from viruses and other similar threats, Anti-malware software is way broader. It works in a spectrum that involves viruses, but bundles ransomware, trojans, worms and other threats. [29]

Along with techniques, we should consider the implementation of measures that can be encapsulated in the broader spectrum of Cyber Security. The measures below aren't designed to just protect school's information, it allows us to protect employees and all other users of the overarching school infrastructure and community, allowing us to implement prevention mechanisms where possible: [1,30,31, 38]

- Develop an Information Security Policy,
- Conduct Training and Awareness Raising Practices,
- Define roles and responsibilities,
- Device Management,

- Strong Authentication,
- Stay up-to-date and install security patches when available,
- Logout of websites and shut down the devices when done working.

Developing an Information Security Policy is a key step in Cyber Security. As such, one should be developed and revised as needed. It should involve what the school's objectives are and it should be presented to all parties, while advocating for compliance. A Security Policy will be helpful to lay down the guidelines that every interested party should follow, and in the process, also identifying who and what we're trying to protect, against whom or what and listing all the resources necessary to achieve said protection. [38]

Another major factor that plays into Cyber Security is the human factor. There should always be training and awareness raising practices implemented, because it doesn't matter how much security is implemented, physically or digitally. If users aren't aware of risks and good practices, they become a weak link in the defense and are open to exploitation, mainly through Social Engineering techniques. [1,5]

One integral step of writing a Security Policy is to attribute different levels of classification to information. The same way that we label information, we should attribute roles and responsibilities to the users. Every user should be conscious of their functions and roles towards information security, so that every party can be held accountable for their behavior and responsibility towards the school's security. [1]

Every device should be managed. That is to say that updates should be installed when available, devices should be password protected, install antivirus and anti-malware software. These are all good practices, but there's a different avenue to address proper device management. Personal devices like laptops and smartphones are less secure than the organization's devices; therefore, no sensitive information should ever be present in these devices. As such, this topic should also be addressed in the implemented Security Policy. [30]

Strong Authentication involves the use of more than just a Password, it applies the use of an additional identification factor. The three factors for authentication are Something you know ("SYK"), Something You Have ("SYH") or Something You Are ("SYA"). Nowadays, some systems apply the use of 2-factor authentication, which combines 2 of these factors, normally SYK and SYH. The most common combination being SYK and SYH. The Credentials are something the user knows. As for SYH, a security token is used, normally sent to the user's email address or phone number. Currently, the use of strong authentication is almost mandatory. The use of passwords is not enough anymore, so schools should implement strong authentication methods to access their resources or IT systems. [32]

Staying updated involves software and the users themselves. It's important to maintain software running its latest version. Often, security patches are launched to keep Operating Systems secure against threats and the same applies to antivirus and anti-malware software. Simultaneously, it's important for users to be informed about emerging threats and risks, particularly new phishing scams. [31]

This last practice is something that users don't realize is a dangerous behavior and this can be due to the world being progressively more connected to the internet,

especially with the Internet of Things. Users should always logout of the websites or applications that they were using when they're done using them. Along with logging out of websites, they should shut down their computers or end the session, so that access is locked behind authentication. [31]

3 Analysis of the Case Study

Regarding the theme of this paper, a case study was conducted, in the form a survey with the aim to examine the knowledge in basic concepts of Cyber Security from various members of different schools' academic communities, sent to different regions of the country, attempting to get as big a sample as possible, so as to produce discernible results that grant us the ability to analyze the knowledge of members from within said communities.

Google Forms was used as the platform upon which we built the survey itself and distributed it. This platform was chosen as a result of some factors that were taken into consideration: the ability to guarantee every participant's anonymity and the integrated tools that allow for data analysis. The survey consisted of 14 questions about the participants and their knowledge in basic concepts of Cyber Security.

The survey obtained a total of 153 submissions, of which we can display some demographic details. The following table presents the results of the population analysis.

Table 1. Demographic Information of the Participants

Age	Gender
Up to 15 years old 30,7%	Male 45,1%
16-18 years old – 30,1%	Female – 53,6%
19-25 years old – 7,8%	Prefer to not disclose – 1,3%
26-50 years old – 24.2%	
50+ years old – 7,2%	
Occupation	**Academic Studies Completed**
Elementary–Senior Year Student 62,7%	Elementary School – 6,5%
College Student – 6,5%	Freshman Year – 50,3%
Elementary–Senior Year Teacher – 22,2%	Senior Year – 14,4%
College Teacher – 2%	Bachelor's Degree – 17%
Non-Teaching Staff – 6,5%	Master's Degree – 9,8%
	Doctorate – 2%

This section presents an analysis of the questions regarding the participant's knowledge of basic practices in Cyber Security that they should know and implement in their day-to-day lives. Below, there're two tables that reflect two different types of questions. The first table presents the data from five questions with yes or no answers relating to the participants' normal behavior and the second table presents the data from table two's questions 2-5 and the academic studies completed by the participants.

Table 2. Questions with yes or no answers

Question No.	Question	Answer (%)	
1	Do you possess any knowledge in Cyber Security?	Yes (85,6%)	No (14,4%)
2	Do your passwords include numbers and special characters? (e.g., +*!-<>)?	Yes (76,5%)	No (23,5%)
3	Do you use the same password for different services (e.g., email, social networks, etc.)?	Yes (38,6%)	No (61,4%)
4	Do you access your personal accounts on your institution's devices?	Yes (43,1%)	No (56,9%)
5	Do you access the Internet through public wireless networks (e.g., cafés, shops, etc.)?	Yes (60,8%)	No (39,2%)

Table 3. Correlation between the academic studies completed and the replies to the questions in table 2

Question No.	4th Grade	9th Grade	12th Grade	Bachelor's	Master's	Doctorate
2	Yes (5%) No (1%)	Yes (39%) No (1%)	Yes (10%) No (4%)	Yes (12%) No (5%)	Yes (8%) No (1%)	Yes (2%) No (0%)
3	Yes (1%) No (5%)	Yes (18%) No (32%)	Yes (8%) No (6%)	Yes (7%) No (10%)	Yes (3%) No (7%)	Yes (1%) No (1%)
4	Yes (3%) No (3%)	Yes (25%) No (25%)	Yes (7%) No (8%)	Yes (6%) No (11%)	Yes (2%) No (8%)	Yes (1%) No (1%)
5	Yes (3%) No (4%)	Yes (32%) No (18%)	Yes (10%) No (4%)	Yes (12%) No (5%)	Yes (3%) No (7%)	Yes (1%) No (1%)

Starting with the first table, question 1 aimed to analyze if users felt confident about their knowledge in Cyber Security, trying to establish a comparison between an initial portion of participants that felt like they possessed knowledge and the portion that did. The question itself doesn't allow us to assume anything from what the participants know, but it allows us to establish an initial number that can be useful to keep in mind for the questions that followed. An encouraging 85,6% (131) of participants reported that they felt like they had some knowledge in the topic. Even though this number is very positive, the following questions (2-5) that targeted the participants' day-to-day habits that pertain to their online security habits, showed that a generous amount of the participants doesn't know a lot of the important basics.

Starting with questions 2 and 3, as they are connected, 76,5% (117) of participants reported that they include special characters in their passwords and 61,4% (98) report that they don't reuse the same password. Regarding the use of special characters in passwords, this is a simple but easy thing to do to increase the security of passwords as they become harder to guess or to be found through brute force methods. [33] As for the reuse of passwords, it is a dangerous behavior because, assuming a hacker gets hold of a user's password, they'll have access to an array of accounts, not just the one,

possibly compromising an entire network. [34] Of the 153 participants, 55 reported to reusing passwords and 15 of them reuse passwords and don't including special characters, which is a big vulnerability.

For questions 4 and 5, the participants were asked about accessing their personal accounts in their institution's devices and if they connected to wireless public networks. In question 4, 43,1% (66) of participants reported to accessing personal accounts on their institution's devices. This shows the lack of proper device management, since these are not institutional accounts, these are personal ones that can become a vulnerability for both the users and the network, as the user may leave the account connected and not end their session and through that account, infect the network as computers in schools tend to be directly connected to the internal network, not a peripheral one. [35] Both questions pose underlying issues, but especially question 5 relates to a bigger issue, the connecting to free wireless public networks, ones present in cafés and malls. This type of behavior is dangerous for the users, especially since they may be dealing with sensitive information, and hackers may gain access to their private information stored in their mobile devices. [36]

Table 3 establishes a connection between the answers to questions 2-5 from table 2 and relates them to the different levels of studies completed. This table was created with the intention to examine how different levels of education influenced the results. With this connection established, it's worthy to note the following: 28 out of 77 participants with 9th grade completed reported that they actively reuse the same password for different services, 38 of those participants also report to accessing personal accounts on their institution's devices, 49 access public wireless networks. This denotes the need for better awareness raising between 5th and 9th grade, and possibly up to 12th grade, as a significant portion of participants that completed 12th grade show that they possess those same habits.

This covers the first two tables and the first part of the survey. The second part focuses on technical terms, and it has 2 questions. The first question is regarding phishing and the second one, ransomware. The first question possessed 3 possible answers, only one of them correct. The second question was a multiple-choice question having a definition of the term ransomware and the choices were 4, only one being Ransomware.

Table 4: Results of the questions related to technical terms

Question No.	Question	Correct	Wrong
6	Phishing is…	80,4% (123)	19,6% (30)
7	Malware is…	41,8% (64)	58,2% (89)

These two questions worked towards the same goal, but the first one being phishing had the purpose of it being a topic that has been brought to light by media outlets as of recently, also being that this type of attack sky-rocketed in recent years. [37] The overwhelming majority of participants, 80,4% (123) answered correctly to the question, but it's important to examine the fact that 19,6% (30) of participants, still don't know this term. As for the question about ransomware, this one was a bit more complicated for the participants, as only 41,8% (64) of participants answered correctly. Seeing that

ransomware is such a destructive and powerful tool in attackers' arsenals, this is an alarming response, as not even half of the participants could answer correctly.

With these results in mind, a few observations can be made. A lot of participants are aware of some of the basics and while some of the questions display a positive response, others arise a more alarming response. There can be improvement, especially in the range of 4th grade up to 12th grade, as it's in this range that most participants displayed a general lack of knowledge in Cyber Security.

4 Conclusions

There's a lot of threats that are thrown in schools' way, but with a comprehensive understanding of Cyber Security basics, everyone can benefit, and a more secure cyber space can be in sight, for all members of the academic communities. Investing in a proactive stance towards attacks and threats is the first step in protecting schools and their many members.

Overall, schools should invest in teaching Cyber Security to children and teens. As the current and future generations will continue growing up with technology, strides need to be made so the people are aware of the dangers and how to protect themselves. Keeping up with every advancement is hard, so schools should look to make strides in teaching, as to establish the principals of the subject earlier, which could go a long way in the formation and safety of children, teens, and young adults.

In this sense, schools should strive to achieve this as there is a variety of possibilities in which this objective can be reached, like lectures with experts, updating the curriculum to include a more focused emphasis on Cyber Security and demonstrations of threats and attacks in a safe environment to expose the risks and damage these threats can cause, especially to the younger and more impressionable populous.

References

1. Richardson, Michael D.: Lemoine, Pamela A.; Stephens, Walter E.; Waller, Robert E. Planning for Cyber Security in Schools: The Human Factor. Educational Planning 2020(27), 23-39 (2020).
2. Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime. https://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=coms%2Fcybercrime%2Freport.htm., last accessed on 2021/10/13.
3. Jang-Jaccard, J., Nepal, S.: A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences. 80, 973–993 (2014).
4. A Roadmap for Cyber Security Research, https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap_0.pdf, last accessed 2021/10/13.
5. Breda, Filipe & Barbosa, Hugo & Morais, Telmo. SOCIAL ENGINEERING AND CYBER SECURITY. 4204-4211. 10.21125/inted.2017.1008 (2017).
6. "Hacking the human operating system: The role of social engineering within cybersecurity", Technical report, Intel Security (2015).
7. Prashant Kumar Dey, "Prashant's algorithm for password management system", International Journal of Engineering Science, pp.2424 (2016).

8. Nalin Asanka Gamagedara Arachchilage, Steve Love, Konstantin Beznosov, "Phishing threat avoidance behaviour: An empirical investigation", Computers in Human Behavior, Vol.60, pp.185-197 (2016).
9. Mitnick, K. D., Simon, & L., W. The art of deception: controlling the human element of security. Indiana: John Wiley & Sons (2011).
10. Schuesster, J. H. Contemporary threats and countermeasures. Journal of Information Privacy & Security, 9(2), 3-20 (2013).
11. Alavi, R., Islam, S., & Mouratidis, H. An information security risk-driven investment model for analysing human factors. Information and Computer Security, 24(2), 205–227 (2016).
12. Katzan, Jr., H. Contemporary issues in cybersecurity. Journal of Cybersecurity Research, 1(1), 1-6 (2016).
13. Lestch, C. Cybersecurity in K-12 education: Schools face increased risk of cyber-attacks (2015).
14. K-12 Cybersecurity 2019 Year in Review. Part III: Cybersecurity Incidents: 2019, https://k12cybersecure.com/year-in-review/2019-incidents/, last accessed 2021/11/02.
15. Rock, A. Report: K-12 schools experienced 122 cyber-attacks in 2018. Campus Safety, (2019, February 10).
16. A parent's guide for understanding K-12 school data breaches, https://studentprivacy.ed.gov/resources/parent%E2%80%99s-guide-understanding-k-12-school-data-breaches, last accessed 2021/11/30.
17. College and University Data Breaches: Regulating Higher Education Cybersecurity Under State and Federal Law, http://docplayer.net/2539829-College-and-university-data-breaches-regulating-higher-education-cybersecurity-under-state-and-federal-law.html, last accessed 2021/11/30.
18. Nabie Y Conteh, Paul J Schmick, "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks", International Journal of Advanced Computer Research, Vol.6 pp.23-31 (2016).
19. Gu, Qijun, and Peng Liu. "Denial of service attacks." Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications 3: 454-468 (2007).
20. Sen, R., & Borle, S. Estimating the contextual risk of a data breach: An empirical approach. Journal of Management Information Systems, 32, 314-341(2015).
21. Davis, D. Best practices for balancing technology use and safety in a modern school. In Society for Information Technology & Teacher Education International Conference (pp. 1026-1030). Washington, DC: Association for the Advancement of Computing in Education (AACE) (2018).
22. Goldsborough, R. Protecting yourself from ransomware. Teacher Librarian, 43(4), 70-71 (2016).
23. Kleinberg, H., Reinicke, B., & Cummings, J. Cyber security best practices: What to do? Journal of Information Systems Applied Research, 8(2), 52 (2015).
24. Mamoona Humayun, Mahmood Niazi, NZ Jhanjhi, Mohammed Alshayeb, Sajjad MahMood. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study (2020).
25. Jorge Gonçalves, Hugo Barbosa. A Survey of Cyber Security Systems: Approaches for Attack Detection, Prediction and Prevention (2020).
26. Jyoti Chhikara, Ritu Dahiya, Neha Garg, Monika Rani. Phishing & Anti-Phishing Techniques: Case Study (2013).
27. Cisco. What is a Firewall? https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html, last accessed 2021/11/22.

28. Félix Iglesias, Tanja Zseby. Analysis of Network Traffic for Anomaly Detection (2019).
29. Mohammed Talal, A.A. Zaidan, O.S. Albahri, Bilal Bahaa. Compreensive review and analysis of anti-malware apps for smartphones.
30. Arlitsch, K., Edelman, A.: Staying safe: Cyber security for people and organizations. Journal of Library Administration. 54, 46–56 (2014).
31. Coventry, L., Briggs, P., Bythe, J.: Using behavioural insights to improve the public' s use of cyber security best practices. Government Office for Science. (2015).
32. Do van Thanh, Jorstad, I., Jonvik, T., Do van Thuan: Strong authentication with mobile phone as security token. 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems. (2009).
33. Das, A., Bonneau, J., Caesar, M., Borisov, N., Wang, X.F.: The tangled web of password reuse. Proceedings 2014 Network and Distributed System Security Symposium. (2014).
34. Spafford, E.H.: Preventing weak password choices. Computers & Security. 11, 273–278 (1992).
35. Rhee, K., Jeon, W., Won, D.: Security Requirements of a Mobile Device Management System. International Journal of Security and Its Applications. 6, (2012).
36. Ayaburi, E.W., Wairimu, J., Andoh-Baidoo, F.K.: Antecedents and outcome of deficient self-regulation in unknown wireless networks use context: An exploratory study. Information Systems Frontiers. 21, 1213–1229 (2019).
37. Portugal is the 2nd country in the world most affected by spam and phishing, https://www.safecommunitiesportugal.com/cybercrimealerts/portugal-is-the-2nd-country-in-the-world-most-affected-by-spam-and-phishing/, last accessed 2021/12/2.
38. Bulgurcu, Cavusoglu, Benbasat: Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly. 34, 523 548 (2010).
39. Gyunka, B. A., & Christiana, A. O. Analysis of human factors in cyber security: A case study of anonymous attack on Hbgary (2017).
40. Aziz, A. The evolution of cyber attacks and next generation threat protection. RSA Conference (2013).
41. Blythe, J. Cyber security in the workplace: Understanding and promoting behaviour change. Proceedings of CHItaly 2013 Doctoral Consortium 1065, (pp. 92- 101) (2013).
42. Atkinson, S., Furnell, S., Phippen, A.: Securing the next generation: Enhancing E-safety awareness among young people. Computer Fraud & Security. 2009, 13–19 (2009).
43. Javidi, G., & Sheybani, E. K-12 cybersecurity education, research, and outreach. In 2018 IEEE Frontiers in Education Conference (FIE) (pp. 1-5), Cincinnati, OH. IEEE (2018, October).