Cyber Threats to Education Technological Services: a Case Study

João Moreira, Hugo Barbosa

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. Schools face Cyber Threats, so it's crucial to explore the impact that the lack of knowledge about some of the basic concepts of Cyber Security can pose to Educational Technology Systems. The main thing is knowing what we're fighting, so it's key to identify what danger the threats pose to schools' sensitive data, and provide an overview of Cyber Security essentials, aiming to prevent attacks or mitigate the damage that Cyber Threats can cause. Throughout the last few years, awareness has been raised to the importance of Cyber Security, especially during the Pandemic. 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.

Index Terms— 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 Cyber Space, studying how hackers can perform their attacks, detect design flaws and exploit weaknesses. Differ-ent 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 infec-tion 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 2 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 Cyber Space 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 Cyber Space 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 ma-nipulate 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 En-gineering exploits people through deception, making it an easy way to acquire infor-mation through the most vulnerable factor in the system, the people who use it [9].

The pandemic that struck the world in early 2020 is still a major talking point and the reality as of 2022. Due to the pandemic, everyone but essential workers were sent home, including students and teachers alike. Following government rules, schools had to hold their classes online, using online platforms and video conferencing tools. Thanks to this increased time at home and the need to work from home, an increase in Cyber Attacks and incidents was noticed, with the Education Sector facing these prob-lems like the other sectors.

With the pandemic, there was a significant increase in the regular Cyber Threats, but also a rise in new and unexpected threats, that came as a consequence of people being more online, especially for work purposes. Schools not being an exception to the norm, classes were taken online and threats such as Class and Meeting Invasions took place as a new threat, accompanied by Data Breaches and Ransomware.

This paper aims to give an overview of the risks and threats to schools and their information systems, as well as paint a landscape of Cyber Security in Education in re-cent years, offering a more detailed view of the years of 2019 and 2020. Schools are equipped with the tools to fend off attacks, however, good network design that is pre-pared to handle external threats is critical. It is crucial to educate the common users about basic

Cyber Security concepts and practices.
Section 2, 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 following section expands the first by analyzing how the pandemic changed Cyber Security, comparing the results from studies in 2019 mentioned in the first sec-tion to studies related to Cyber Security in the pandemic, exposing the new threats and explore what can be learned from the events of 2020 and how Cyber Security in Education was handled and how it should be handled going forward.
The last section presents the analysis of a survey performed in 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 disad-vantages. It allowed professors and students to work more effectively, but with pro-gress 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 Ccybercrime [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 imple-ment Cyber Security measures, which leads to a problematic situation where the ro-bustness 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 subsections represent the types of threats that impact the Education sector [14,15].

2.1.1 Data Breaches

In the context of Education, the Privacy Technical Assistance Center describes Data Breaches as "any circumstance where a school's student data system is improp-erly 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].

Data from the 2021 End of Year Report from the Identity Theft Resource Center identified more than 1800 compromises [18], a number that represents more than 700 more compromises than in 2020, with almost 300 million victims, setting it apart from the past 6 years that, even though all possess a higher number of total victims, none have reached this number of compromises. Besides these numbers, it's important to highlight the fact that due to system and human error, there were 179 data breaches, that tallied up more than 100 million victims.

Similarly, the Education Sector also was hit harder, compared to 2020, with 125 compromises reported, compared to just 42 in 2020 and 71 and 2019, with the most popular data attributes that were breached being the name, social security numbers, date of birth, home addresses and medical records of the victims [18].

There are different vectors that all play into a Data Breach, with some examples being Cyber Attacks, human and system errors, and physical attacks. Thanks to this wide array of possibilities, one of the main things that can happen is that a student loses their credentials, either physically or digitally, and with these new access creden-tials, an attacker can definitely access the school's IT systems. This is one of the human error threats, as it's up to the holder of the credentials to not lose them, which can be done through an array of other threats.

Inside of each vector, there are multiple ways that each can achieve the attack-er's goals. From the Cyber Attack vector point, there are Phishing, Ransomware and other types of Malware, Credential Stuffing and Exploit of Unpatched Software Flaws. As for human and system errors, there is lost devices or documents, emails, and mis-configured firewalls. And at last, physical attacks encompass document and device theft or improper disposal [18]. All these different ways to achieve a data breach is the reason why they occur so often and why they can be so hard to combat.

2.1.2 Malware-related Threats

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 at-tacks can be in other forms like Trojans, Spyware, Worms, and Viruses. These Mal-ware-related threats have unique ways of operating and infecting devices, with the aim of gathering information, deleting, or altering data [12].
Ransomware is a very popular type of Malware, and it works by hindering the us-er's access to their files, systems or networks, normally tending towards the disruption of operation and inflict the loss of critical data. Users can accidently download Ran-somware onto a device, through emails or clicking on ads. After downloading this Ransomware code, it'll lock access to the device, encrypt the computer's storage and demand for a ransom for the encrypted data, often showing proof that they can de-crypt the data by presenting a way to unlock a certain file [19].

Trojans are a type of Malware that, like the name suggests, presents itself as a program that'll perform an action, but in reality, it's performing other malicious ac-tions. The more prominent fronts for this threat to use are free software and legiti-mate-looking ads [20].

Spyware is a more passive kind of malware, as it aims to hide itself and work, as the name implies, like a spy. It is programmed to track the user's activities, including what is typed on the keyboard, what websites are accessed, what files are download, among other possibilities. On extreme cases, some Spyware can even enable cameras and microphones without detection. What makes this threat so dangerous is the way it's meant to exist, silent and invisible, for as long as possible. Although known as a Cyber Threat, it is also used for legal purposes, like companies that want to monitor productivity of their workers and parental controls often possess Spyware, as to block access, for example, to adult content [21].

Worms and Viruses, while sometimes grouped together as similar, these are two different threats. The first big difference comes from the fact a computer virus fully depends on a host, that can be a program or an operating system. Worms, on the other hand are malware that is programmed to replicate through networks without any other help needed.

Another distinction comes from the way these infect the system or network. Vi-ruses normally come in the form of an executable file, as Worms normally come from a downloaded file or a network connection [22].

2.1.3 Social Engineering Attacks

Social Engineering Attacks involve different types of attacks, but the most com-mon form is Phishing. Social Engineering is a method in which an attacker gathers in-formation about a target through the exploitation of human weaknesses, using decep-tion or manipulation to access sensitive information [23]. 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, along to sending these emails to as many emails as possible [5].

Along with Phishing, there's also Spear fishing, Smishing and Vishing. Spear fish-ing, unlike Phishing's approach is way more targeted. Attackers that choose this ap-proach are likely to find a target or a small group of targets and try to gather infor-mation about them, as to use that information in the form of photographs, birth dates, addresses and any other type of valuable and believable information to give the scam as much credibility and chances of success as possible.

Smishing, on the other hand, works through text messages. These come in various formats, but the one common thing is that victims receive a text message from the at-tacker posing as, for example, the postal service or a company of some sort, notifying the user that they've won something like a special limited offer or a contest they didn't apply for. Along with this explanation comes a link, sometimes spoofed, as to look as believable and closest to the source as possible, in the hopes to either collect the user's login credentials or get them to pay a non-existent shipping fee for a non-existent prize [24].

Finally, there's Vishing that executes scams through the phone, concretely through verbal deception, making use of phone calls primarily to convince that what the user is being recommended to pay for is in their best interests, this way employing the first stage of the con. Next, the scammer will attempt to persuade the user into paying, providing them with the request for the necessary card information and promptly leaving, without further contact once the payment goes through. At this point, the user has become a victim of Vishing and the scam is complete. Whatever so-lution was promised doesn't actually work and the victim will not be able to reach the scammer anymore, losing their money.

This type of Social Engineering normally works by providing a solution to a non-existent problem that is created by the scammers. Normally, there's some embed-ded malware in a link or file that'll trigger some kind of reacting and inform the user that this can be solved only if they call the scammer. The unbeknownst user calls this scammer that knows the problem and offers to solve it when they get paid, finishing the con [25].

2.1.4 Denial of Service

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 ser-vice performance or even stopping the service altogether, which tends to cost an or-ganization both their time and money. 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 [26].

Normally, these attacks will target, but aren't limited to, email services, websites, online and physical banking systems, or any other kind of service that relies on a network to function. One important thing to note is that, even though a certain network may not be the target, it may be affected by it, which is the case for regular users when their Internet Service Provider (ISP) gets targeted by this type of attacks.

To protect against these attacks, tools to analyze the network flow are key, as they'll filter the abnormal DoS traffic and let through the normal traffic, as well as creating disaster recovery plans, as to make sure that, in case that preventative measures aren't enough, that mitigation and recovery measures will allow for the most positive outcome possible [27].

2.2 The value and importance of schools' data

The education sector is a key target for attackers. According to the K-12 Security Information Exchange, 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 par-ents).

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 vul-nerabilities 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 [28].

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 identifica-tion 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 [29]. 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 [30].

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 infor-mation and to prevent attacks directed to their resources and IT systems.

2.3 Techniques and Best Practices for 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 [31].

2.3.1 Techniques for Attack Prevention and Mitigation

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. The following subsections depict some of the most frequently used techniques by organizations to protect the Cyber Space from the various Cyber Security Threats [32].

2.3.1.1 Implementation of Intrusion Detection Systems

Intrusion Detection Systems (IDS) are applications that provide constant moni-toring of computer systems, alerting to when suspicious activity might be occurring. One key detail of this type of tool is that while it can't prevent intrusions, it'll alert the people responsible of the possibility of an occurring malicious activity.

These tools constantly monitor systems and when it suspects an intrusion might be taking place, it'll evaluate it and emit an alert. Because this detection device isn't able to prevent any attack, it is equally not a replacement for further protection tools, such as firewalls and antivirus software. It should be thought of as a reinforcement to an already well-working system and not a substitute for other measures [33,34].

There are different types of intrusion detection systems as well as different detec-tion methodologies, and each warrant different requirements, which creates con-straints, depending on what specifications the system where this tool will be imple-mented has.

Each methodology has pros and cons, with these being the different basis of how the system will detect intrusions. There are 3 different methodologies: signature-based, anomaly-based and stateful protocol analysis. As for the different detection approaches, there are 5: statistics-based, pattern-based, rule-based, state-based and heuris-tics-based [35].

2.3.1.2 Implementation of Anti-Phishing Techniques

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 [36].

Some of these techniques may seem obvious, but they go a long way in keeping users safe from these Cyber Threats. Simply keeping up to date with Phishing tech-niques is important because it's better to find out about them earlier, as the risk of get-ting scammed by it increases over time.

Verifying if a given website is secure is another thing any user can do. All secure websites have their URL starting with "https", with the "s" indicating a secure certifi-cate, while websites without it do not possess a trusted certificate. Another thing on websites involves clicking the lock. It should be closed, and the certificate should be present. Browsers will also help with this, as many sites are insecure, and the browser will not allow the user to enter immediately. It will, however, display a warning on screen.

A habit that most users don't follow up on is checking their accounts or changing their passwords often. This habit is crucial, as accounts that aren't visited for a while could mean attackers have gotten hold of it, and changing passwords regularly is also a very important habit, as it'll keep all the accounts safe, granted that the passwords are strong.

Pop-ups are potentially very dangerous and tend to appear as though they're part of the website that they've popped up from. Most of the time they're either phishing attempts or contain malware. A good solution is visiting the web browser's settings and blocking pop-ups. A good rule of thumb, if one manages to squeeze through the blockade, is to never click buttons that seem like they're the ones to click, even if they say "Cancel" or "Quit" or some other variation. These tend to

lead the user down a rabbit-hole of scams. It's always best to close the window directly or, if on smartphones, using the normally very small "X" that'll appear at one of the top corners is best [37].

Finally, never giving out personal information is key. Even it's a trustworthy looking source, website or email, a user should never share personal information over the Internet. When in doubt, it's best to not follow through, try to get a hold of the company's customer support number or email and contact them. Many Phishing scams will have a very similar-looking user interface but will ask for financial infor-mation or login credentials, for example. Always check the URL and, when in doubt, compare it to the main company's link, as there might be something off [38].

2.3.1.3 Implementation of Firewalls

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 and external networks [39].

There are different types of firewalls, each with its own set of advantages and disadvantages. The first and most common type of firewall is a packet filter. When this firewall receives network packets, it'll cross reference it with a set of predefined rules or access control lists and, according to the rules set, these packets will either be for-warded or dropped.

Another type of firewalls comes in the form of Application-Gateway firewalls, which will handle the connections made by evaluating whether a connection has been made and how it was made. This way, each connection coming from inside or outside the firewall will be stopped, which is, by definition, a proxy connection. It functions by either establishing itself as the host of the incoming connection if that connection has been allowed or drops it [40].

Circuit-Gateways Firewalls provide a high level of protection and hide the infor-mation effectively inside private networks. It scans network extensions and allows on-ly genuine connections, commonly used in pair with VPNs, offering security and pro-tection in private networks. The connection acts as a virtual circuit, as the proxy cre-ates an end-to-end connection between the client trying to establish said connection and the application that they're trying to access. Its biggest disadvantage is the lack of single packet filtering [41].

Next, there's Web Application Firewalls that are designed for, like the name im-plies, web applications. These firewalls help us protect this type of application by ap-plying filtering and monitoring of the HTTP traffic, which is essential, as it's the pro-tocol that the Internet runs on, acting as its foundation. It helps in the fight for a lot of web-based attacks, such as Cross-Site Scripting (XSS) and SQL Injections, but it is not a solution for all attacks, it should be integrated as a part of the defense solution, not as the solution [42].

Ultimately, there's hybrid firewalls. These Firewalls are, as the name suggests, hy-brid versions of the three previous types discussed above, with a lot of Firewalls being used today having packet-filtering functionalities paired with support for proxies [40].

2.3.1.4 Analysis of Anomalies in the Network Traffic

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 [43].

Anomalies in traffic means atypical traffic in the network. And by analyzing the traffic, we can detect these anomalies, normally caused by atypical network users or by known or unknown attacks. To find anomalies, there's 2 groups of methods that can be used: statistics and density based, although, these aren't the only approaches, as some approaches make use of machine learning techniques, such as Support Vector Machines [44,45].

Analyzing the network traffic demands specific software or devices that can do this. There are many companies that offer different types of products to achieve this goal. One of the solutions stems from Security and Information Event Management (SIEM) tools, that helps keeping logs of all activity to protect against Cyber Attacks and Attackers.

In many cases, Intrusion Detection and Prevention Systems, paired with Firewalls cannot solely protect a network against many of the targeted advanced malware, that is specifically designed for these devices; therefore, we can't just stop the threats at the border, we need to look within, into the inside of the network and be able to detect anomalies in it.

With these tools, we can promote the protection of the IT infrastructure, through many of the essentials that SIEM provides, such as the analysis of data across the net-work and real-time threat analysis and incident response. Like other examples in this list, the presence of this tool in our array of security techniques, doesn't discard the need for other tools, but it does play an important role in the understanding of what happens across the network and making a correct diagnosis of the possible threats to the IT infrastructure [46].

2.3.1.5 Implementation of Anti-Malware Software

Anti-Malware software is often associated with the term anti-virus. Although both have similar objectives, succinctly, anti-viruses 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 [47].

There are multiple anti-malware techniques and the oldest one is the file signature analysis. With this technique, the companies that produce antiviruses possess a database that is complete with signatures of all the Malware previously detected, blocking any file that doesn't match the stored signatures. There's a more advanced version of this type of analysis and it uses heuristics to determine if a program is malicious or not.

Along with these techniques, there's also cloud-based malware detection that takes client-server approach, due to the cloud-based architecture, which will block any invalid soft-

ware from a blacklist and validate authentic software from a whitelist [50].

Another approach comes in the form of Endpoint Detection and Response (EDR) agents. EDR is an endpoint security solution, which works by securing entry points of the end-user devices, such as laptops and phones, preventing them from being ex-ploited. This solution continuously monitors these devices, trying to detect Cyber Threats like the ones mentioned in this paper, for example, Ransomware.

The EDR itself works by recording the behavior of end-user devices and through various techniques, differing from company to company, detect suspicious behavior and proceed to block said activity that it believes to be malicious. The EDR provides many advantages, such as endpoint visibility, behavioral protection, fast response and, in many cases, a cloud-based solution [51].

2.3.1.6 Implementation of Virtual Private Networks

Virtual Private Networks (VPNs) are encrypted tunnels that operate over the Internet or un-trusted networks in general, acting to provide confidentiality to transmissions and en-sure their integrity. These are generally used to safely communicate in private, while resorting to public networks. In general, this is achieved through end-to-end encryp-tion and strong authentication.

VPNs allow for us to make it harder for a third party to track the network traffic, activities or even steal data, given that the encryption of all communication is done in real time. Thanks to this, if any attacker tried to access this data and successfully got their hands on it, it would be virtually impossible to decode it. Plus, a VPN provides a cloak to the IP address, by using the network redirect the address through a server, normally remote when it comes to widely available commercial offers, that is ran by a VPN host [52].

2.3.1.7 Strong Authentication

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 se-curity token is used, normally sent to the user's email address or phone number. Cur-rently, 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 [63].

A study from 2021 directed by the U.S. National Institute of Standards and Tech-nology taxonomized authentication [64]. From this study, there are two identified classes: confirmation and attestation. The type of authentication that is relevant for this paper falls into one of three domains of the confirmation class: Human-Human, Human-Machine and Machine-Machine.

Confirmation is classified as a mechanism that confirms that a device, piece of hardware, or software is valid and can access the intended application or resource. The domain is Human-Machine, which is identified by the human being in control of the hardware or software that represents themselves as an entity. Inside this domain are 4 different families that represent the factors presented above. These being: Memorized Secret, Apparatus and Biometrics and a last family denominated as Multi-Modal, which is the widely known two factor authentication (2FA).

The memorized secret, as the name implies, is the "Something you know". It rep-resents the login credentials, such as PIN numbers and passwords. It is the most popu-lar form of authentication, even if not as secure as it once was.

The apparatus is the "Something you have", being in the form of digital certifi-cates, smartcards, or RFID devices. The vulnerability normally found in this type of authentication factor is that these can be easily lost, posing a very big weakness to the system that it's implemented on. The most common form of this type of authentication uses it as a secondary authentication mechanism, often seen as an email or text message, in the form of a one-time password (OTP).

Next there's biometrics, referring to the "Something you are". Some examples of biometric authentication use fingerprints, facial identification, and voice recognition. The main problem with this type of authentication is that it tends to be very expensive and complex to implement, which reduces its value, therefore, most organizations tend to default towards the final type of authentication.

The final authentication mechanism is designated as Multi-Modal. It consists of the combination of two or more human-machine authentication mechanisms. By com-bining different methods, we can achieve a more robust authentication process and, therefore, a more secure system. The most implemented type of multi-factor authenti-cation requires the user's login credentials, which represent something they know and, the use of text or email messaging, representing something they have, to send a token that will be needed to complete the authentication process [64].

2.3.2 Best Practices for Attack Prevention and Mitigation

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 [1,49-53].

2.3.2.1 Develop an Information Security Policy

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 in-terested 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 [53].

An Information Security Policy is a set of rules and guide-

lines that all interested parties must abide by. It dictates how the resources of Information Technology should be used, managed and protected, as this are high value and importance assets for any company. There are many elements of an Information Security Policy, but the most important ones sit on the definition of roles and responsibilities for all users, the security controls and what are the consequences if this policy is broken [54].

There are three stages associated with Information Security Policies: its develop-ment, the implementation and maintenance and, ultimately, evaluation. The develop-ment stage involves the identification of key stakeholders and the definition of roles and responsibilities, followed by the identification of the security needs of the institu-tion and the actual drafting and review of the first final version of document.

After developing the policy, it's important to make sure that it's implemented and maintained correctly. The responsible parties should distribute the policy and com-municate it to all stakeholders, through any communication means, such as meetings or seminars and, ultimately, make sure that it's enforced.

The last stage is the evaluation of the policy, through periodic reviews, where feedback from stakeholders should be collected and any incident reports should be an-alyzed, resulting in a possible new risk assessment phase [55].

2.3.2.2 Conduct Training and Awareness Raising Practices

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].

Both are extremely important and although these are often paired together, they are not the same. Awareness raising allows us to put a focus on Cyber Security and recognize that there are threats we can be exposed to. Training allows users to be pre-pared and know how to deal with the threats, especially when considering threats such as Social Engineering, so that users are able to recognize these threats and effectively evade their attempts.

Doing this comes with its challenges, as keeping ahead can prove to be a chal-lenge, because there's a series of factors to consider, such as social factors, the business environment, organizational and economic factors. All of these stem from the constant evolution of Social Engineering and other Cyber Threats' techniques [56].

As this proves to be an effective way to educate the general public, it should be noted that there are a multitude of ways to achieve awareness and to train users, but one of the counteracting strategies that proves fruitful, in terms of achieving aware-ness, is game-based Education. There are a few notable serious games, but the follow-ing are very good examples: Kahoot, Jigsaw Phishing Quiz and Riskio [57-59].

These games aren't created with entertainment as the key focus, but rather edu-cational purposes. There are different ways to approach this type of game-based edu-cation, such as quizzes or tabletop games, but the takeaway is that there are benefits that can be gained by adopting this approach [60].

Kahoot, while not a platform directed at Cyber Security, possesses many differ-ent subjects for various quizzes, as well as allow for the creation of custom games, so if the available quizzes aren't well-suited to what is needed, a new one can be created.

The premise is simple, the game host (teacher) will share a pin that the partici-pants (students) will use to access the game. After everyone is connected on their de-vices, the host needs a big screen so that they can share the questions and the answers. Each device possesses the possible answers, and the participants will vote on the op-tion they think is correct. To add more of an incentive, the faster a participant answers correctly, the more points they gain and whoever has more points at the end is deemed the winner [57].

The Jigsaw Phishing Quiz doesn't possess the ability to be played multiple times, but the one that can and should be played is chock-full of information and real-world scenarios. This quiz is only 8 questions long, but it challenges the participant to identi-fy what a Phishing attempt is and what a legitimate email is. Regardless of answering correctly or not, the user is told why it is or isn't a Phishing scam, pointing out the most important aspects that can help identify a possible Phishing attempt [58].

At last, there's Riskio, a tabletop game that allows for a maximum of 5 players and a Game Master. In this game, the 5 players are the students, and the Game Master is a Cyber Security expert. The main objective of the game is rooted in learning about secu-rity vulnerabilities and how to act in order to appropriately defend oneself against them.

The game can be played by players of any background, being a good tool for both IT-related fields or participants with no technical background. The game proposes scenarios where the players will take the roles of both defenders and attackers, while at the same time learning how to protect themselves against these threats [59,61].

2.3.2.3 Define Roles and Responsibilities

One integral step of writing a Security Policy is to attribute different levels of clas-sification 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].

After identifying the key stakeholders in the development stage, it's important to define the roles and the responsibilities of these interested parties. It's important to in-volve all different stakeholders in the development phase and make sure that their re-sponsibilities are properly be stated and documented, so that the identification of the security requirements can be specifically detailed to the institution's needs [55].

2.3.2.4 Device Management

Every device should be managed. That is to say that updates should be installed when available, devices should be password protected, install antivirus and an-ti-malware software. These are all good practices, but there's a different avenue to

ad-dress 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 im-plemented Security Policy [49].

With these devices becoming more and more vital to the efficient day-to-day of organizations, it's important to analyze what access is made to critical information, to be sure of what threats are present in the cases of hacking, theft or loss of the device. This way, device management tools should be implemented so that the IT or Security departments of schools can manage those devices, which ties into the roles and responsibilities defined previously in the Information Security Policy, because those per-sonal devices should possess role-based access to the institution's information and, preferably provide a VPN to avoid connecting to unprotected wireless networks [62]

2.3.2.5 Staying Up-To-Date and Install Security Patches When Available

Staying updated involves software and the users themselves. It's important to maintain software running its latest version. Software is easy to keep updated, with a lot of applications and programs having the ability to update themselves without the user noticing. Simultaneously, it's important for users to be informed about emerging threats and risks, particularly new Phishing scams.

Along with the software, the user should always attempt to stay in the loop when it comes to Cyber Security. New threats are discovered every day and new Phishing attempts and techniques are developed by malicious actors, therefore, it's crucial for a user to not only be able to identify Social Engineering attempts, but also stay in the loop for new ones, as there are some very good and legitimate-looking scams on the Internet.

Often, security patches are launched to keep Operating Systems secure against threats and the same applies to antivirus and Anti-Malware software. Browsers and smartphone applications follow in the same path, but it's important to know that not all possess this amount of support from its developers, hence the need for a user to in-stall these patches when available, but always try to keep in the loop for newly discovered vulnerabilities, Data Breaches or threats of applications they use [50].

2.3.2.6 Logout of Websites and Shut Down the Devices When Done Working

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, espe-cially with the Internet of Things. It is part of Device Management, but it is a simple practice that is definitely worthy of being talked about separately, as it doesn't cross users' minds of the possible dangers of not doing it. 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 ses-sion, so that access is locked behind authentication.

A lot of users aren't aware of their surroundings when using their devices, which can result on "shoulder surfing", which means that other people are actively trying to get a look into the user's personal information, while they're in a public or a workplace setting. If a user isn't aware of their physical surroundings, they may be inputting their login credentials or banking information and a user may be collecting this data to later use it for malicious acts like taking advantage of this newly acquired personal infor-mation for personal gain or selling it [50].

3 Cyber Threats to Education during the Covid-19 Pandemic

In the early months of 2020, one topic swept the world off its collective feet. With the Covid-19 pandemic hitting most of the world, governments all around implemented lockdown measures, which shaped the coming months of countless people. With peo-ple at home for extended periods of time and the inability to work on-site, companies resorted to information technology to be able to keep working, even if at a seemingly reduced pace.

All sectors got hit hard and Education is one of those sectors. As teaching was impossible in person for the foreseeable future, schools also resorted to information technology to not impede the progress of students more than what the pandemic was doing. In this sense, schools found themselves using a wide array of tools to be able to continue education in the most regular way possible. Platforms for online learning and video conferencing were widely used to hold classes and meetings for students and staff alike. But with these platforms and tools catching the spotlight from people with legitimate interests, so did it catch the always opportunistic eyes of attackers, that took advantage of the shift in attention from security that came as a consequence of trying to adapt to the new reality that people had to now face [65].

This shift in focus came accompanied of technical issues that the video confer-encing platforms encountered, as well as the overload of service providers that had an overnight increase of network traffic, leading to downtime in some cases. Although this caused trouble for many users, these were arguably the best consequences when we consider that alongside these problems came a rise in Ransomware attacks, Phish-ing attacks, Data Breaches and Denial of Service attacks. [66]

With people more online than ever, this proved to be an advantageous landscape for attackers to perform attacks, as more unaware users would have to be online for longer, increasing the window of opportunity for malicious acts.

This section will cover this undeniably key topic of Cyber Security during the pandemic, while at the same time, staying in the domain of education, which repre-sents the relevant component for this paper.

The subsections that follow will contain a general view of the Cyber Threats to Education during 2020, since there were some unforeseen threats emerge, accompa-nied by many other threats that can be highlighted, due to the volume of incidents amidst 2020. Included in this section is also a comparison between pre-pandemic numbers and post-pandemic numbers, with the intention of examining the impact of the pandemic on

Cyber Security and Education, as to reflect on the results of both years.

Following the topic, there's an analysis of what can be learned from the whole pandemic situation and what we can take forward, as the world continues its efforts to recover from this major worldwide occurrence.

3.1 An Overview of the Cyber Threats to Education during the Covid-19 Pandemic

The section above discussed and analyzed the different Cyber Threats to the Edu-cation sector and its information technology infrastructure, along with the different members of the academic communities that may face these threats. This section, on the other hand, will focus on cyber threats to education amidst the Covid-19 pandemic. Due to this occurrence of global scale, schools had to resort to IT solutions so that classes could proceed with an almost normal cadence.

Since classes in person were not possible, learn tions fell back on the available tools to hold classe and means of evaluation like exams and present most noteworthy examples are online learning or platforms, such as Moodle and Google Classroom conferencing platforms, which included Zoom Me Microsoft Teams [67-70].

These efforts proved to be fruitful, as classes ret students experienced learning through remote r hough this effort allowed most institutions to keep classes, this response with resort to information highlighted some significant gaps and, in some cas failures in the security ecosystem of K-12 schools [6

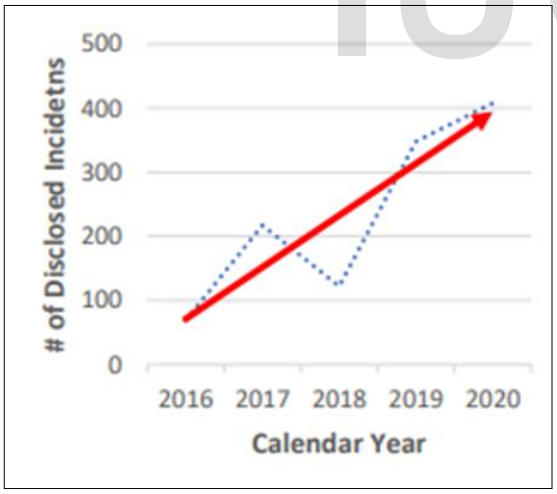


Fig. 1. The Growing Threat of School Cyber Incidents [66]

According to the K-12 Security Information Exchange, the year of 2020 saw an in-crease in the number of publicly disclosed incidents, a total of 408, compared to the 2019's 348 incidents [66]. Even though there was an increase, the most important thing about these incidents is not the volume of occurrences, but what threats caused them.

In the year of 2020, the most frequent type of threat was accredited to the combi-nation of Class and Meeting Invasions, Email Invasions and Website Defacement. These threats arose and became a big problem, especially during the second and third quarters of the year, being the most prevalent type of incident during that section of the year.

This new and prevalent type of incidents that plagued schools stemmed from the shift that schools experienced, coming from the appropriation of the video conferenc-ing tools to provide students and teachers with the ability to hold synchronous online classes and meetings, due to the cease of all in-person function.

As these threats presented are new, it's important to define them and, as such, a class invasion can be defined as any incident where an unauthorized user disrupts online classes and a meeting invasion is defined by the use of same tactic where an unauthorized individual will disrupt a meeting, but this type of meeting will be, for example, a parent-teacher meeting and orientation sessions. This type of invasion happened so often that it lead to some institutions sharing documents with best prac-tices of how to deal with these invasions, with a set of instructions for teachers and students to follow, so as to not have this happen so often [71].

These invasions proved to be an opportunity to display disturbing media files, such as images and videos and threaten participants with violence or hate speech, which constituted a dismal reality until vulnerabilities were patched later in the year, preventing these occurrences to happen as often. These Cyber Threats were responsible for 45% of all incidents happening in K-12 schools, in the United States., making it clear that this was a hindrance to teachers and students alike.

Due to the Covid-19 pandemic, this combination new threats were able to de-throne Data Breaches as the most frequently occurring cyber threat, which represented a clear number one in the past two years, although, Data Breaches still edge out any other singular type of Cyber Threat, with large numbers of data from current and past students and staff members' data being compromised, leading to consequences such as fraud and identity theft [14,72].

Along with these two prevalent threats, Ransomware still prevailed at 12%, with DoS attacks representing 5% and Phishing only 2% of all incidents. Above all, it's im-portant to denote that with a shift occurring in focus to technology coming from schools, so did it occur for attackers, that chose to take advantage of the often inade-quately prepared users that were now using whatever available tools there were without appropriate verification [66].

With classes being executed remotely, students and teachers had to use their per-sonal devices in their homes, which represent untrusted networks and, therefore, these devices should be analyzed for any threat such as Malware, like Worms or Trojans be-fore they are able to connect to the school's network. These can pose a very big threat, when considering that these devices may or may not have been updated, have an up-to-date antivirus and may lack inspection when it comes to malware, making it a possible weakness, considering how easy some Malware can spread through networks.

Comparatively, 2019 had less incidents overall and the most prevalent threats that plagued the year of 2020 were not visible, due to the normal educational circum-stances. Thus, the biggest threat, in comparison, was Data Breaches, followed by

Ran-somware attacks, DoS attacks and Social Media Defacement, and Phishing.

This shows that a change of circumstances this big, like going from in-person to remote learning, highlighted that schools have exposed themselves to more threats, as well as severely handicap themselves. At the same time, lessening their chances to mitigate these threats and prevent further incidents, due to the Covid-19 restrictions [66].

3.2 The Key Takeaways from Cyber Security in Education during the Pandemic

With the way the pandemic struck the world, impacting all sectors and businesses, it's important to not fall on the same pit again. The theme of the pandemic is still a big concern, and it highlights that almost no one was prepared to the sheer scale of events in store when the pandemic was first reported. With all sectors taking to remote working and learning, it became very apparent that Cyber Security is and should be a main concern. With more people at home, there was more uptime, and with it, came a record year for Cyber Security incidents. In this way, it's of the utmost relevance to in-dicate what we need to take away from this experience, so that if this pandemic or an-other situation takes us all back home to conduct our work and life remotely, we can make sure that we will be prepared this time.

The pandemic served as a wake-up call for schools. With restrictions forcing schools to adopt unorthodox teaching methods, attackers took it upon themselves to cause as much disruption and damage as possible. Due to the sudden change of cir-cumstances, we witnessed new threats hit the Education sector, which were never be-fore seen. Data Breaches continued its upwards tendency of being the most hard-hitting threat to schools, but uncommon threats caused by the new means through which schools held synchronous classes created a surge in class and meeting invasions. Other threats still loomed behind, not as reported on, due to the influx of new threats, mixed with the world's attention being on the pandemic.

Above all, with this collection of knowledge, there are some takeaways that are crucial to be made. As it currently stands, no one knows if there'll be a situation in the future that'll force the population indoors for an extended period of time, but if there is a situation like it, it's very important that schools will be prepared to deal with the sit-uations head-on and be able to avoid the mistakes and mitigate or prevent the conse-quences of previous years.

Going forwards, schools should make it a priority to identify what can be done to better protect the data of their employees and students, as well as continue investing in Information Technology Security.

Starting off, there should be an assessment of the current security policies, as the pandemic came and there was much left to be desired, creating a need for contingency plans for emergency situations and, going forwards, there should be plans to deal with the sudden shift from in-person to remote learning.

The pandemic also showed a glaring issue with the lack of training and awareness raising practices, as schools had to resort to making documents to help teachers set up their synchronous online lessons in ways that would allow the ceasing of class and meeting invasions. It elevates the point of awareness in general, regarding cyber secu-rity, as well as implementing ways for students and staff to learn the essential basics, securing both the users and the whole school IT infrastructure from potential threats.

Besides that, it's important for schools to have a predefined list of tools that have been vetted from a security standpoint.

The year of 2020 displays that schools are not prepared for such a shift in their regular activity and that cyber security needs to be a topic that is considered more im-portant than it currently is. With the array of threats that target schools and the aca-demic communities around the world, it's important to take a stand with Cyber Secu-rity and make a push for awareness and training, to share the knowledge and to provide future adults with all the tools and knowledge they'll need to protect themselves in the cyber space.

4 Analysis of the Case Study

Regarding the theme of this paper, a case study was conducted, in the form a sur-vey 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 discerni-ble 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 inte-grated 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 de-tails. The following figures present the results of the population analysis.

The target demographic were teachers, students and non-teaching staff. Parents were not targeted in this survey for the simple reason that, although they're part of the academic community, they rarely interact with any of the school's IT infrastructure or devices. The only, less likely way, would be the sharing of devices at home, which could result on a threat, but those are impossible to examine while attempting to keep each participant's answers and identity private and secure.

As for the targeted demographic they've been chosen because they all interact with electronic devices, both personal and the school's, on a daily basis. Teachers use them to teach, students to learn and the non-teaching staff for all other types of needed function, such as the reception, the printing room, the school's software for the bar and others, making them an also interesting target for this survey.

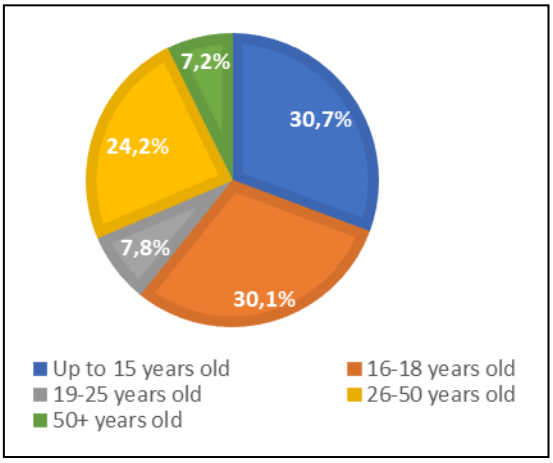


Fig. 2. Survey Participants' Age Distribution

Analyzing the results of the participants' age, it's clear that the biggest portion of the population is of individuals that are up to 18 years old, which indicates students up to 12th grade. This can be better perceived with the chart that analyzes the participants' occupation. The second biggest group is of individuals between 26-50 years old, which indicates teachers of the same grade range as the students or the schools' non-teaching staff. The remaining 2 smaller groups represent individuals between 19-25 years old, the smaller of these two being the participants over 50 years old.

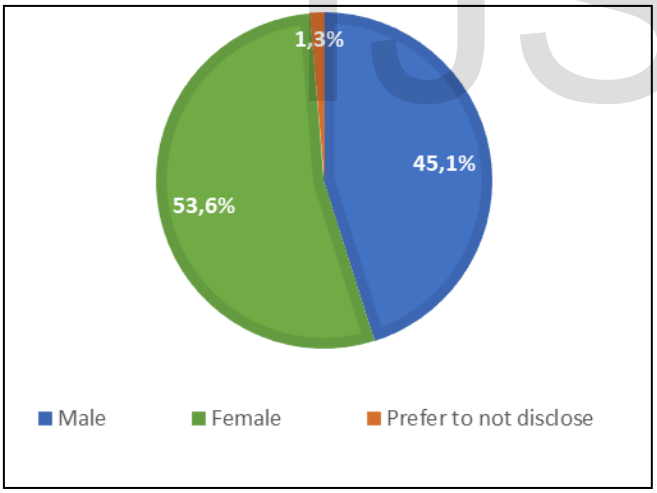


Fig. 3. Survey Participants' Gender Distribution

As for gender, a closely matched distribution between female and male partici-pants can be identified, with female participants edging out male participants by 82-69 in a total of 153 participants, with two individuals preferring not to disclose their gen-der. Altogether, this is a good distribution, with no gender having a clear majority over the other, in terms of participation.

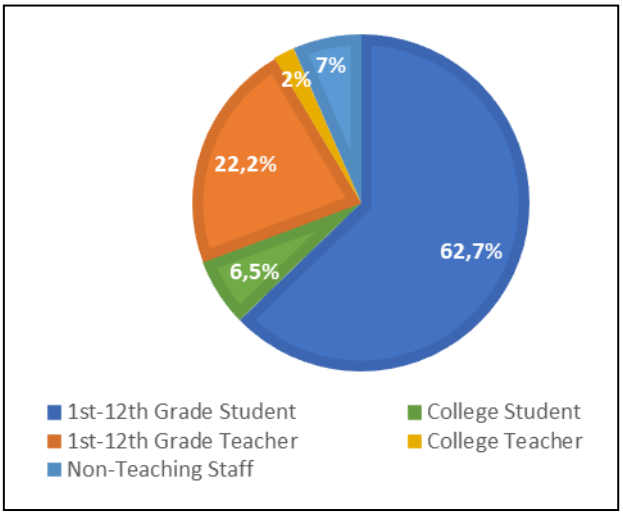


Fig. 4. Survey Participants' Occupation Distribution

This chart corroborates what can be implied from the age distribution chart dis-played above. Over 60% of the participants are students between 1st and 12th grade, with the second biggest group, with a little over 20%, being teachers of the same grade range. The three smaller groups are college students and teachers and non-teaching staff. With this chart and the age chart, we can understand who the participants are.

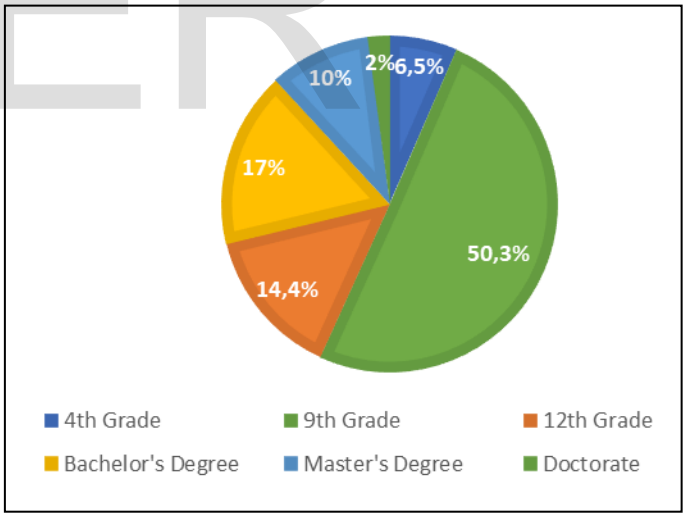


Fig. 5. Survey Participants' Academic Studies Completed

It is important to note that these academic levels are presented in relation to the Portuguese education system. Providing a translation for the American education system, 4th, 9th and 12th Grades can be directly translated to Elementary School, Freshman Year and Senior Year, respectively. The remaining academic levels are equivalent. This chart further improves the understanding of the population involved in this survey, with just over 50% of the students being between 10th and 12th grade; 14% graduated from high school and now in college; 17% having completed a bachelor's degree and being a teacher and the remaining three smaller groups being students

between 5th to 9th grade, teachers that achieved a master's degree and the smallest group being teach-ers that achieved the highest academic level of a doctorate.

Regarding the very few participants that hold a doctorate, it's important to note that a very small portion of the population holds such a high level of academic excel-lence and, when it comes to 1st to 12th grade teachers, this number is much smaller than college teacher; therefore, while making an effective analysis for this group of people may be impossible in this study, it's important to note that the distribution of teachers with a doctorate in this level of teaching is very low, hence the results obtained in the survey [73].

It is important to note that these academic levels are presented in relation to the Portuguese education system. Providing a translation for the American education system, 4th, 9th and 12th Grades can be directly translated to Elementary School, Freshman Year and Senior Year, respectively. The remaining academic levels are equivalent. This chart further improves the understanding of the population involved in this survey, with just over 50% of the students being between 10th and 12th grade; 14% graduated from high school and now in college; 17% having completed a bachelor's degree and being a teacher and the remaining three smaller groups being students between 5th to 9th grade, teachers that achieved a master's degree and the smallest group being teach-ers that achieved the highest academic level of a doctorate.

Regarding the very few participants that hold a doctorate, it's important to note that a very small portion of the population holds such a high level of academic excel-lence and, when it comes to 1st to 12th grade teachers, this number is much smaller than college teacher; therefore, while making an effective analysis for this group of people may be impossible in this study, it's important to note that the distribution of teachers with a doctorate in this level of teaching is very low, hence the results obtained in the survey [73].

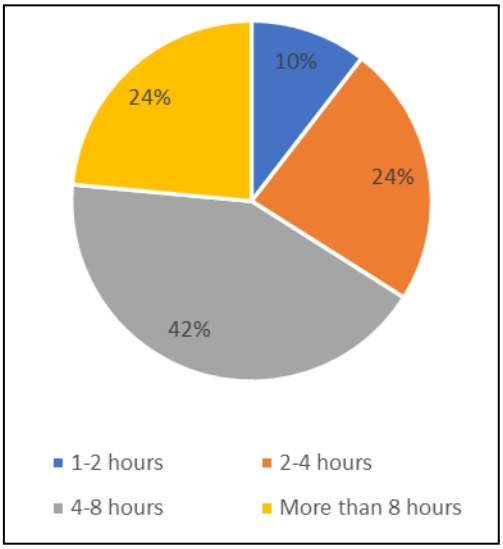


Fig. 6. Survey Participants' Number of Daily Hours Spent Using Electronic Equipment

This penultimate chart allows for an understanding of how much time is spent by the participants of the survey using electronic equipment, such as computers, smartphones, tablets or others throughout their day-to-day lives. Obviously, the more time spent using electronic equipment, the more likely to commit mistakes for the not so careful users and the window of opportunity for attacks is bigger. As the data shows, the majority of users will spend a sizeable chunk of time throughout the day using electronic equipment, with 42% spending anywhere between 4 and 8 hours and an even 24% split spending either 1 and 2 hours or 2 to 4 hours daily. The smaller split of only 10% of participants spends between 1 and 2 hours using this type of equipment. While this chart depicts a good picture of the average, daily usage of electronic equipment by the survey participants, the final demographic information chart will be linked to this one, as it inquired the participants about the purpose of the usage of the equipment.

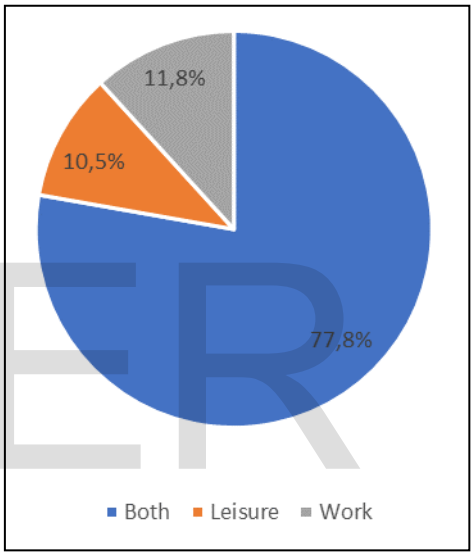


Fig. 7. Survey Participants' Purpose of the Usage of the Equipment

The figure above presents the distribution of the finality of the usage of the men-tioned equipment. The way this links up with the previous chart is that the purpose is very important, especially when considering device management. While some partici-pants may have different devices for work and leisure, most will either not feel the need for the separation or not be able to afford to do this.

The data received from the 153 participants shows that the majority, 77.8% (119), will use phones, computers and other equipment for both leisure and work. As men-tioned above, device management is crucial, thus, this is an important piece of infor-mation, especially to pair from the results of the questions below that hit on device management. Separating the usage of equipment between work and leisure is crucial, especially if users aren't aware or don't practice safety measures, such as not accessing personal accounts in the institution's devices and not accessing unprotected wireless networks on devices that contain private or confidential information.

While the charts above provide a good understanding of the participants, as men-tioned above, the participants replied to a total of 14 questions. The format of the questions besides

the ones presented in the charts above was yes/no regarding the in-dividual's online habits and current cyber security themes, such as the reuse of passwords, and access to unprotected public wireless networks, and multiple-choice questions with an emphasis on more common technical terms that every user should pos-sess some knowledge of, even if superficial.

The following two subsections contain the charts with the data regarding the in-dividual questions and the third subsection contains charts that establish a link be-tween the questions and some of the demographic data analyzed above. A third sub-section will cross-reference different demographic factors with the results of the vari-ous questions, presenting the most relevant ones.

4.1 Online Security Habits Question Analysis

In this subsection, there's all the relevant data regarding the yes/no questions pre-sent in the survey. First, there's table 1 that contains the questions mentioned and the associated number. The table will act as a reference board for the chart that follows it, as well as the ones in a subsection below that'll go over some of the more important links between the demographic data and the questions about Cyber Security. The table is composed of the number, as the charts regarding any yes/no question will follow the same numbering present in it. To minimize the amount of charts present, the data from all binary answer questions were condensed into one.

TABLE 1

QUESTIONS ASKED TO THE SURVEY PARTICIPANTS REGARDING THEIR ONLINE SECURITY HABITS.

Question No.	Question
1	Do you possess any knowledge in Cyber Security?
2	Do your passwords include numbers and special characters (e.g.,.+*!-<>)?
3	Do you use the same password for different services (e.g., email, social networks, etc.)?
4	Do you access your personal accounts on your institution's devices?
5	Do you access the Internet through public wireless networks (e.g., cafés, shops, etc.)?

There are 5 total yes/no questions. They inquire the participants about their daily habits, more specifically, about passwords and device management. These questions aim to obtain an interpretation of the participants' day-to-day habits, as some of them can prove quite risky if there's a lack of awareness regarding these habits.

Question 1 is very broad and doesn't allow for specific conclusions, but it's im-portant, nonetheless, as the habits and technical terms present in these survey ques-tions are quite basic and lack of knowledge or, in some cases, the practice or not prac-tice of the habits present in them, can be dangerous for the individual and their insti-tution. The overall aim of this question is to evaluate how many users feel like they're knowledgeable, up to a certain point, in cyber security, setting an initial mental note for the next questions.

Questions 2 and 3 are directed at passwords, more concretely, password reuse and weak and strong passwords. Nowadays, strong passwords are a must. Simple passwords with no numbers or special characters can be cracked very fast. To counter this, it's important to make passwords that are strong. There are many ways that password strength can be improved, such as, its length, the use of special characters, like the ones present in the question itself, and numbers. Web browsers like Google Chrome also suggest very strong passwords and can store them, but a safer way is to use a password manager, which can make the process of creating and remembering strong passwords easier. Password reuse is, unfortunately, a very big problem. Reusing passwords is a very dangerous practice, as most people possess access to many ser-vices, multiple email accounts, social media networks, and the reuse of the same password or making only little adjustments can prove to be a very dangerous practice, be-cause if one password is cracked, all other accounts that can be accessed with the same password are in equal danger.

Questions 4 and 5 aim towards device management, more specifically, accessing personal accounts on the institution's devices and accessing the Internet through pub-lic wireless networks, like the ones often present at coffee shops and malls. These two questions are related in the way that they represent an often-overlooked issue. Device management, if mishandled, can be very dangerous. On one hand, accessing a personal account through an institution's device, such as a computer or maybe a phone pro-vided/reserved for work, can have consequences. These consequences normally stem from possible phishing attacks, particularly through email accounts. If an individual accesses their personal email account and accidently or because they're not aware, click on a Phishing link, all types of threats can be unleashed, such as Malware, Ransomware, Keyloggers, Spyware, and other threats. On the other hand, accessing a wireless unprotected network like the ones mentioned above can be very dangerous, as attackers tend to prefer this type of networks to infiltrate and, for example, watch the network traffic and even try to unleash threats upon the users connected to the network. This type of network tends to be preferred by attackers because they're normally not password protected, because that entices the regular users to connect and, with that in mind, these users can become easy prey to hackers if not protected properly.
These factors are important to inquire the participants about, as these are very dangerous practices, that they should be aware of and potentially change their habits, if in the wrong. The figure below represents the data to each of the questions described above.

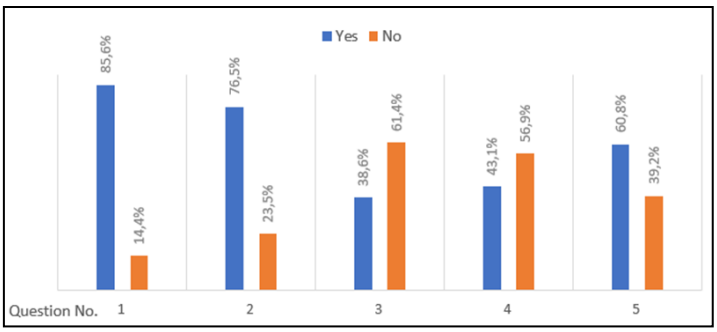


Fig. 8. Results of the online security habit questions presented to the participants.

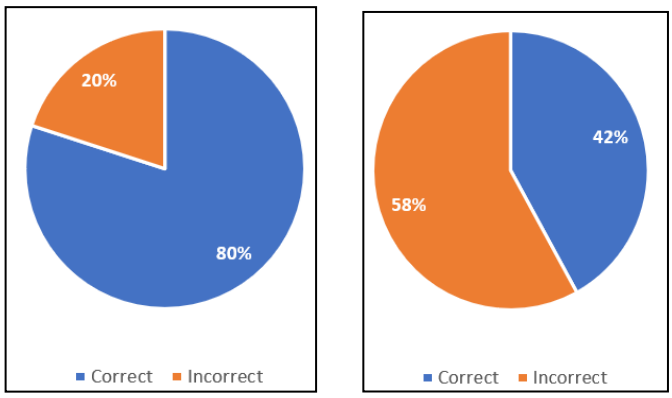
Starting with the first question, as described above, not a lot can be concluded about its results, but that's not the intention regarding its existence. It is helpful because it helps shape a view of our participants' confidence towards their knowledge of the domain in which they were surveyed. An encouraging 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' online security habits, showed that a significant amount of the participants doesn't know one or more of the basic questions or the consequences to their bad habits that followed in the sub-sequent questions.

In questions 2 and 3, 76,5% (117) of participants reported that they include spe-cial characters in their passwords and 61,4% (98) report that they don't reuse the same password. When it comes to 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 [74]. As for the reuse of passwords, 38,6% (55) of participants report reusing passwords, representing over a third of the total participants that report to having a very dangerous habit in their daily online lives. 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 compro-mising an entire network [75]. Even more worrisome is the 9,8% (15) of participants that reported reusing passwords, while at the same time, not including any measures to ensure a strong password. While these users are a minority, they represent a very big threat to themselves and to their institution.

In questions 4 and 5, 43,1% (66) of participants reported to accessing personal accounts on their institution's devices and 60,8% (93) of participants report to access-ing unprotected wireless networks. Question 4 shows a lack of proper device manage-ment, since these are not institutional accounts, these are personal ones that can be-come a vulnerability for both the users and the network, as the user may leave the ac-count connected and not end their session and through that account, infect the net-work as computers in schools tend to be directly connected to the internal network, not a peripheral one [76]. As for question 5, it relates to an equally dangerous issue, as connecting to public wireless networks and possibly dealing with sensitive information in the process may prove costly, as hackers may be able to gain access to the wide array of private information stored in mobile devices [77].

4.2 Technical Term Question Analysis

This second part, while shorter, possesses worthwhile data regarding the knowledge and awareness of the participants. The first question approaches 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 dif-ferent definitions of unrelated terms and only one definition of the term Ransomware, for a total of 4 options.



a) b)

Fig. 9. (a) The chart represents the results of the question regarding a multiple-choice question that asked the users to complete the phrase "Phishing is…"; (b) The chart presents the results of the technical question regarding multiple-choice question that asked the users to indicate which Cyber Threat was a better fit for the sentence displayed.

These two questions worked towards the same goal, but the first one being Phish-ing 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 [78]. The vast 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 what this term refers to and entails.

As for the last question regarding Ransomware, this one was a bit more compli-cated 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.

4.3 Key links between demographic factors and the questions

This section covers the data from demographic factors and the questions, both present in the survey. While each question presents valid data on itself, combining the data between the demographic information gathered and the results obtained from the questions related to Cyber Security will allow for a more profound analysis and grant us the possibility for better conclusions.

There are 3 different links presented in this section: Academic studies completed and the online security habits questions, studies completed and the technical term questions and lastly, purpose of usage of electronic equipment with access to personal accounts on the institution's devices and accessing unprotected public networks.

Starting with the first connection, the combination of the academic studies com-pleted from the demographic information gathered and the results from the online se-curity habits questions that revolved around the daily online security habits of the participants. This connection was created with the intention to examine if different levels of education influenced the results and if so, how did those levels influence the overall

results.

TABLE 2

LINK BETWEEN THE DIFFERENT ACADEMIC LEVELS ACHIEVED AND THE QUESTIONS REGARDING THE ONLINE SECURITY HABITS OF THE PARTICIPANTS.

Question No.	4th Grade	9th Grade	12th Grade	Bachelor's	Master's	Doctorate
2	Yes (8)	Yes (59)	Yes (16)	Yes (18)	Yes (13)	Yes (3)
	No (2)	No (18)	No (6)	No (8)	No (2)	No (0)
3	Yes (2)	Yes (28)	Yes (13)	Yes (11)	Yes (4)	Yes (1)
	No (8)	No (49)	No (9)	No (15)	No (11)	No (2)
4	Yes (5)	Yes (38)	Yes (10)	Yes (9)	Yes (3)	Yes (1)
	No (5)	No (39)	No (12)	No (17)	No (12)	No (2)
5	Yes (4)	Yes (49)	Yes (16)	Yes (18)	Yes (5)	Yes (1)
	No (6)	No (28)	No (6)	No (8)	No (10)	No (2)

There is a lot of data present in the table but only a few outliers are key points that need to be mentioned. It's worthy to note the following: for 9th grade, 28 out of 77 par-ticipants that reported having 9th grade completed actively reuse the same password for different services, 38 of those same participants also report to accessing personal accounts on their institution's devices and 49 access public wireless networks.

This denotes the need for better awareness raising between 5th and 9th grade, and the same point can be made about the 12th grade level, as the numbers observed on participants that reported having completed 12th grade, paint a similar picture as the previews level, with 12 of the 22 reusing passwords for different services, 10 of the same group accessing their personal accounts on their institution's devices and 15 ac-cessing unprotected wireless networks.

With this data, it can be concluded that there is a lot of uninformed students from 5th grade to 12th grade (middle and high school) that present very bad habits con-cerning their online security. It indicates that schools that teach at these grades need to present students with opportunities of learning Cyber Security and actively encourage them to internalize the basic concepts and good practices, because the world is more and more dependent on information technology, making the need for well-informed students ever more present and crucial, as many won't choose a career linked to Cyber Security, engineering, or the sciences. In Portugal, as of 2021, only around 20% of stu-dents enrolled in universities are in the Engineering, Industry and Construction area and less than 10% pursue Sciences, Maths and IT, which implies that only a small per-centage of college graduates will be fully aware of the dangers of lackluster online se-curity and good Cyber Security practices, if schools don't teach cyber security or pro-vide access to learning it at the middle-high school level [79].

The second link combines the data from the academic studies completed and both the technical questions. Once again, presented in the table below, are the results from combining the data between a demographic factor and the results from Cyber Security related questions. These have been divided into each of the academic levels present in the survey and, for simplicity, they've been identified with Cor (correct) and Inc (incorrect), as to identify the number of participants that answered correctly and incor-rectly to each.

TABLE 3

LINK BETWEEN THE ACADEMIC LEVELS ACHIEVED AND THE TECHNICAL TERM QUESTIONS.

Question	4th Grade	9th Grade	12th Grade	Bachelor's	Master's	Doctorate
Phishing	Cor. (7)	Cor. (64)	Cor. (16)	Cor. (22)	Cor. (12)	Cor. (2)
	Inc. (3)	Inc. (13)	Inc. (6)	Inc. (4)	Inc. (3)	Inc. (1)
Ransomware	Cor. (7)	Cor. (29)	Cor. (8)	Cor. (11)	Cor. (8)	Cor. (1)
	Inc. (3)	Inc. (48)	Inc. (14)	Inc. (15)	Inc. (7)	Inc. (2)
Both Incorrect	1	12	4	4	3	1

As previously analyzed, the results are more positive in the question about Phishing than the question regarding ransomware, but from this table, a few key points are worthy of mention: as with the previous questions, the most worrisome groups are middle and high school, but other groups also display lack of awareness, more evidently in the question about Ransomware. Phishing is a very dangerous form of attack, as it attacks the most vulnerable part, the user, and it has been a very popu-lar tool for attackers in recent years. As such, it has gained the attention of all kinds of media and news outlets, which may be able to explain the more positive responses.

In terms of the Ransomware question, it's hard to explain its way lower results, because this threat has been prevalent for years and has been the theme of many arti-cles and news pieces. These numbers are particularly worrisome, as not even half of the participants were able to answer this question correctly, compared to the over 80% correct answers in the Phishing question.

The last comparison in this table accounts for the participants that didn't answer correctly to neither of the questions and this is the most alarming comparison, as an-swering both correctly would be ideal, answering one correctly and the other incor-rectly could still be considered good, but answering both incorrectly nears on unac-ceptable, and it allows for the best insight into the knowledge of the represented stud-ies level groups. The more participants that answer both questions wrong, the more se-rious are the conclusions regarding the need for more awareness raising.

As the data shows, there's still a significant portion of participants (25) that an-swered both questions incorrectly. The more notable results are 9th grade, 12th grade, bachelor's and master's degrees graduates. While these numbers come from a small sample of participants, of only 153, 25 participants who incorrectly answered both questions, stands for roughly 16% of the total sample. While this number may seem small when compared to the total number, it is still a very bad outlook, as it shows that students who complete 9th and 12th grade aren't knowledgeable of these basic technical terms and that teachers who have achieved a bachelor's or master's degree may also not possess this basic knowledge, which drives the point that Cyber Security should have a reinforced focus in schools.

While only three participants achieved a doctorate, it's important to highlight that one of those participants failed to answer any of the two questions correctly, demonstrating that despite achieving the highest level of academic excellence, these users aren't exempt from the lack of awareness talked about throughout this paper, which can lead to bad situations for both the users and their institutions.

This final link combines the purpose of usage of electronic

equipment and the re-sults from the two yes/no questions regarding device management. These questions, in their own regard, were informative, but together allow for a deeper understanding of the participants. The table below presents 3 combinations. These combinations are all similar but all important to mention. The first two combine the participants that have reported using electronic devices for both work and leisure and that answered yes to each of the questions; the last combination only changes the questions from one incor-rect habit to both.

TABLE 4

LINKS BETWEEN THE PARTICIPANTS' PURPOSE FOR USING ELECTRONIC EQUIPMENT AND THE DEVICE MANAGEMENT HABITS QUESTIONS.

Link	Results
Both and Answered Yes to the Access to Personal Accounts Question	50
Both and Answered Yes to Accessing Unprotected Public Networks	67
Both and Answered Yes to Both Questions	28

These results corroborate that there's a lot of users with bad habits, like previous data presented had suggested. All three connections present in the table above display bad and possibly dangerous habits. First, just using electronic equipment for both work and leisure, especially if not given the needed care, can be dangerous for both the user and the institution. Second, answering yes to any of the two questions also poses a bad practice, as accessing personal accounts in the institution's devices is dangerous, espe-cially when considering Phishing emails or links, present in sketchy ads or emails that got through the spam filter and accessing public and unprotected wireless networks is a generally bad habit, as it can be a very good opportunity for an attacker to retrieve private or confidential information.

When the dual purpose of using the electronic equipment is paired with either or both the habits present in the questions, the users can put themselves in danger with-out realizing it, and so can their institutions. If there are not different devices for work and leisure, accessing personal accounts or accessing public wireless networks may be seriously harmful when considering that teachers may have students' or the school's private or confidential information, as well as their own in their computers or smartphones.

With the data collected, we can analyze that around a third of the users either answered one question or the other with Yes, validating the data presented above, but what's more worrisome is the fact that 28 participants possess both of the bad habits represented by the two questions.

4.4 Concerns about Cyber Security from the Survey Participants

This last section regarding the survey directed tackles the last question, charac-terized by being optional, but that hopefully would let users share their mind, in re-spect to their cyber security concerns and worries. Unlike all other questions, this one didn't have any parameters or choices for the users to make. The question was com-pletely open, and each participant was free to write any concern they might have re-garding online security, digital safety, or anything other topic related to Cyber Securi-ty, or opt just leave it blank, indicating they didn't know or didn't have any.

Since there weren't any parameters or choices, to compile the results, each answer had to be analyzed. Some users would leave this question blank or with some kind of punctuation to indicate that they didn't have any concerns, others would write none and the remaining participants writing a concern of theirs, with a few writing multiple concerns that would fit into different categories. In total, 14 different categories were identified, some occurring more often than others, with a few categories taking the spotlight.

After identifying the different categories, the answers to each question were equated to see in which category they'd fit and so that each could be tallied up and examined, as to allow for conclusions.

With this in mind, the following list contains the results of each of the categories, in order of frequency of appearance:

- Unauthorized access - 46
- Doesn't have any concern/ Left the answer blank – 44
- Loss of personal data - 25
- Identity theft – 23
- Improper use or sale of personal data - 10
- Bank account related threats – 6
- Digital Privacy – 5
- Cyber Bullying (stalking) – 4
- Cyber threats – 4
- General lack of awareness and knowledge by regular users - 3
- Cyber war - 1
- Ransom of personal data - 1
- Online safety measures for underage users - 1

As we can observe, there's a wide range of different concerns, some are similar to others, but each category possesses a different type of concern that deserves analysis. The data presented shows a distinguished category from all others: unauthorized access. By far, the biggest concern for the participants of this survey was unauthorized access of some sort.

These threats are also somewhat similar to what has been seen in other studies, that reported concerns regarding Cyberbullying, Privacy, Financial Scams and Tech-nical Threats (such as the Cyber Threats reported in this paper) [80].

Participants that reported to being concerned about this type of threat reported it in different ways, some would be concerned that attackers would get access to their accounts, like email or social media accounts being the most frequently mentioned, some being concerned about unauthorized access to their personal devices, others by having a hacker getting a hold of their passwords and others would be afraid of unauthorized access to their bank accounts and, as a consequence losing their money.

Unauthorized access is a very valid concern, especially for users that may not possess much knowledge of good practices or essentials regarding Cyber Security. One very simple, but important step would be to create different passwords for every dif-ferent account or service that they have or use, turning on 2 factor authentication when available.

The second most frequently seen concern was loss of personal data and a very close third was identity theft, both simi-

lar in the sense that an attacker would need to get access to the data, so that they could proceed with stealing the identity of the user, for some nefarious act or just to steal it. In any situation, it's an awful situation for any user that gets their identity stolen or that loses any sort of personal data, to the hands of an attacker.

As mentioned above, good ways for a user to prevent this sort of situation and protect their personal data, there's a few key things to keep in mind: strong authenti-cation is key, device management is very important, not accessing any unprotected public wireless network and logging out of accounts and shutting down their comput-ers, personal or work devices, can go a long way in preventing this sort of threat.

Next came the improper use or sale of personal data, which also ties in with the ransom of personal data. Both of these concerns come as a further consequence of the loss of personal data. As such, the user loses some or all personal data, at the hands of a Cyber Attack and it's through said attack that the attacker will steal and gather the data and either use it to obtain a ransom, often seen through the use of ransomware or will just sell it or use it for nefarious activities. The act of selling this data can be harmful in the education sector, as a lot of information is stored in schools, making it a prime target for attackers that wish to use this data for selling purposes. As for the im-proper use of said data, it can be used for various situations, but it's normally identi-fied as individuals or organizations that'll use personal data beyond the stated intentions.

Bundled with these concerns is also the bank account related threats, as it still constitutes a concern that relates to unauthorized access, but instead of losing personal data, the user will lose money. Although this concern isn't nearly as frequently men-tioned as the previous ones, mainly because of the age demographic of this survey, it's very important and linked to the previous ones. The participants reported different types of bank account related threats, some related to home banking and others more directly to the unauthorized access to their bank accounts and usage of their funds. Home banking has become a very key tool for people, as it allows for everything or al-most everything that a person can do at a bank, to be done at home or anywhere, with the use of a device connected to the Internet.

The remaining few concerns have all shown up less than 10 times each and aren't directly linked to the previous ones, but they are valid and deserve a closer look. The first noteworthy one comes in the form of cyber threats in general. This one showed up 4 times in total and 3 of those times, it came in the form of Phishing. Users concerned about cyber threats and particularly phishing have simple but effective ways to deal with them, such as keeping the devices up to date, installing security patches when available and not clicking on sketchy links or visiting suspicious websites or emails.

The next two are closely related to each other and they're Cyberbullying and online safety measures for underaged users. It's obvious that Cyberbullying isn't only for underaged users, but it occurs too often in the teenage years, as a 2018 survey by the Pew Research Center found that 59% of teens from the United States. have experi-enced some form of Cyberbullying. Connected to this topic is the safety measures for underaged users, because most social media platforms only require users to be 13 years of age or older, as a minimum age requirement. These are two very important con-cerns, as teens believe that teachers and schools are failing to tackle this major issue [81].

The following concern is digital privacy and, although, it wasn't mentioned a lot, it's a very important and sensitive topic. In the broad spectrum, it means protect-ing the more private information about a user. Information such as the user's name, home address or date of birth. This is a very recurrent topic, especially considering cookies that are widely used today by web developers to track the users' behavior [82]. Fortunately, there are some easy steps that users can take to protect their online pri-vacy, like using a virtual private network, using antivirus software, and limiting the amount of personal information shared on social networks.

Cyber Warfare only had one participant mention it as a concern, and it is defined as a Cyber Attack or a series of attacks that normally target countries. There are dif-ferent types of Cyber Warfare attacks, such as espionage, DoS attacks, attacks to criti-cal infrastructure (e.g. hospitals, power grid) and economic disruption. What sets these attacks apart is that they involve nations launching Cyber Attacks on other nations, with some cases having these attacks orchestrated by terrorist organizations [83]. There isn't much the users can do as to protect themselves directly against this type of attacks other than adopting good online security and privacy practices and staying up to date on news regarding these attacks.

At last, we have the final two categories: the users that either didn't have any concerns or left the answer blank and the users that were concerned about the general lack of knowledge in this area, not only for themselves, but the general population. These two categories can somewhat be referenced together, since there was a total of 44 different participants that reported not having any concerns. These users stand for almost 30% of the total number of participants, and this number is alarming, while al-so making the concerns of the participants who reported worries about the general knowledge of the population lacking well founded.

What is crucial to understand is that, with the data presented above, it's clear that these participants either do not possess any concerns because they are not aware of any cyber threat or how these could impact them or are extremely confident about their knowledge in cyber security, hence the non-existence of any concerns. The results of the survey create an inclination towards the first, rather than the latter, but this can be fixed, especially in the sector of Education. Schools should provide solutions and answers to these worries, as well as encourage students to take an interest in their online safety, just like their physical safety. Some examples of how this could be achieved are lectures, seminars, talks with Cyber Security professionals, workshops and interactive activities.

Just like any other subject taught at schools, institutions should make it a priority to stoke the interests of young students and, for that matter, the whole academic community, including teachers, parents and staff, because as the world keeps evolving and the dependence on the Internet and Information Technology grows every day, so do the Cyber

Threats.

5 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 possibili-ties in which this objective can be reached, like lectures with experts, updating the cur-riculum 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.

This paper covers the major Cyber Threats that plague the Education sector and how these can impact not only the IT infrastructure present in schools, but also its stu-dents and staff alike. The survey conducted allows for an insight into students and teachers of different ages and academic levels, with different online security habits and knowledge, as to examine how these members of different academic communities behaved in an online setting, as well as inquire them about their knowledge.

The results were varied, but they showed a tendency with the 2 bigger groups; participants that had completed 9th and 12th grades demonstrated a worrying lack of knowledge and alarming online security habits. Besides these two groups, the others presented a much smaller sample, but a key takeaway comes from the participants that had achieved a doctorate, who demonstrated that they had a lack of awareness towards Cyber Security, when they failed technical questions and exhibited trouble-some habits.

Above all, this paper aims to demonstrate that schools need to make a significant effort when it comes to Cyber Security. These efforts range from taking a more proac-tive stance regarding Cyber Security, aiming to make it a priority and secure the data, rather than only acting when there's been an incident; Highlight the importance of awareness by implementing talks with experts or professionals and introducing game-based education for both students and staff alike; Invest in secure infrastructure and network solutions; Implement the techniques and best practices approached by this paper and try to gather the academic communities concerns and worries so as to address them and teach them how to engage with their own digital security.

With the world more and more dependent on IT, situations like the pandemic highlight this overwhelming dependence on these tools and how unprepared most in-stitutions were when faced with a dire situation that ensnares schools into a poor situ-ation. And schools need to try and implement further ways to introduce students to the basics and essential knowledge of Cyber Security, starting off providing students with lectures or talks, game-based experiences and challenges, and showing them the con-sequences in a test environment so that everyone in the academic community can learn from these important concepts, and monitor the learning through quizzes or surveys, addressing the major concerns and bad habits as to facilitate the learning process.

The key is to attempt building up the education of students of all ages in these matters, which may turn out to be the difference between a well-prepared individual and a victim of one of the countless consequences of the lack of awareness and knowledge in this very important topic of Cyber Security in Education.

7 End Sections

7.1 Appendix A. Survey Questionnaire

This survey was conducted through the means of Google Forms. The questions con-tained in this appendix are the ones present in the survey. To conduct this survey, an email was sent out to various schools around the country containing the link.

The survey is divided into 4 parts; The first aims to gather some demographic infor-mation from the participants; The second part questions the participants on their daily online security habits; The third part questions the participants on technical terms and the final part asks an optional question that inquires the participants on their main concerns regarding their digital security and privacy.

Survey Participant's Information

1. Indicate your age range:
   Up to 15 years old ☐
   16 -18 years old ☐
   19-25 years old ☐
   More than 50 years old ☐
2. Indicate your gender:
   Male ☐
   Female ☐
   Prefer to not disclose ☐
3. Indicate your occupation:
   1st to 12th grade student ☐
   1st and 12th grade teacher ☐
   College student ☐
   College Teacher ☐
   Non-teaching staff ☐
4. Indicate the highest academic studies level you've achieved:
   4th grade ☐
   9th grade ☐
   12th grade ☐
   Bachelor's degree ☐
   Master's degree ☐

Doctorate ☐

5. Do you possess any knowledge in Cybersecurity?
Yes ☐
No ☐

Daily Online Security Habits

1. Do your passwords contain at least 9 characters and include numbers and special characters? (e.g., +*!-<>)
Yes ☐
No ☐

2. Do you use the same password for different services? (e.g., email, social networks, etc.)
Yes ☐
No ☐

3. Do you access your personal accounts on your institution's devices?
Yes ☐
No ☐

4. Do you access the Internet through public wireless networks? (e.g., cafés, shops, etc.)
Yes ☐
No ☐

5. How much time do you spend using electronic equipment every day? (e.g., comput-ers, smartphones, tablets, etc.)
Less than 1 hour ☐
1 to 2 hours ☐
2 to 4 hours ☐
4 to 8 hours ☐
More than 8 hours ☐

6. To what end? (Follow-up from the previous question)
Work ☐
Leisure ☐
Both ☐

Technical Terms

1. Phishing is…
Independent program that replicates itself with the purpose of spreading to other devices in the network. ☐
Act of deceiving users to attempt stealing confidential information. ☐
Program that automatically executes and displays advertisements without the user's permission. ☐

2. Select the term that better suits the following sentence: "Software that restricts the access to the infected system, encrypting system files and demanding a ransom in re-turn".
Spear Phishing ☐
Adware ☐
Spam ☐
Ransomware ☐

Final Optional Question

1. What are your concerns regarding your digital security and privacy?

REFERENCES

[1] Richardson, M. D.; Lemoine, Pamela A.; Stephens, Walter E.; Waller, Robert E. Planning for Cyber Security in Schools: The Human Factor. Edu. Plan. 2020, 27, 23-39

[2] Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime. Available online: https://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=coms%2Fcybercrime%2Freport.htm (accessed on 13 October 2021).

[3] Jang-Jaccard, J., Nepal, S.; A survey of emerging threats in cybersecurity. J. Comput. Syst. Sci. 2014, 80, 973–993. [CrossRef]

[4] A Roadmap for Cyber Security Research. Available online: https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap_0.pdf (accessed on 13 October 2021).

[5] Breda, F.; Barbosa, H. & Morais, T. SOCIAL ENGINEERING AND CYBER SECURITY. In Proceedings of the International Technology, Education and Development Conference, Valencia, Spain, 6-8 March 2017; pp. 4204-4211. [CrossRef]

[6] Hacking the human operating system: The role of social engineering within cybersecurity. Available online: https://community.mcafee.com/nysyc36988/attachments/nysyc36988/security-awareness-documents/1068/1/rp-hacking-human-os.pdf (accessed on 15 October 2021).

[7] Prashant, K.D.; "Prashant's algorithm for password management system", Int. J. Eng. Comput. Sci. 2016, 6, 2424-2426.

[8] Arachchilage, N. A.; Love, S.; Beznosov, K. Phishing threat avoidance behaviour: An empirical investigation. Comput. Hum. Behav. 2016, 60, 185-197. [CrossRef]

[9] Mitnick, K. D.; Simon, L. W. The art of deception: Controlling the Human Element of Security. 1st ed.; Wiley: New Jersey, United States, 2002.

[10] Schuesster, J. H. Contemporary threats and countermeasures. Int. J. Inf. Secur. Priv. 2013, 9, 3-20.

[11] Alavi, R.; Islam, S.; Mouratidis, H. An information security risk-driven investment model for analysing human factors. Inf. Comput. Secur. 2016, 24, 205–227.

[12] Katzan, H. Contemporary issues in cybersecurity. J. Cybersecur. Res 2016, 1, 1-6.

[13] Cybersecurity in K-12 education: Schools face increased risk of cyber attacks. Available online: https://www.fedscoop.com/cybersecurity-in-k-12-education-schools-around-the-country-face-risk-of-cyber-attacks/ (accessed on 24 October 2021).

[14] The State of K-12 Cybersecurity: 2019 Year in Review. Available online: https://static1.squarespace.com/static/5e441b46adfb340b05008fe7/t/620d593cae830c221a2c7a8a/1645041982038/K12CybersecurityYearinReview.pdf (accessed on 02 November 2021).

[15] Report: K-12 schools experienced 122 cyber-attacks in 2018. Available online: https://www.campussafetymagazine.com/safety/k-12-cybersecurity-resource-center-cyber-attacks/ (accessed on 9 November 2021).

[16] A parent's guide for understanding K-12 school data breaches. Available Online: https://studentprivacy.ed.gov/resources/parent%E2%80%99s-guide-understanding-k-12-school-data-breaches (accessed on 17 November 2021).

[17] Beaudin, K. College and University Data Breaches: Regulating Higher Education Cybersecurity Under State and Federal Law. Journal of College and University Law 2015, 3, 657-693.

[18] Identity Theft Resource Center - 2021 Annual Data Breach Report. Available online: https://notified.idtheftcenter.org/s/2021-data-breach-report (accessed on 26 February 2022).
[19] Ransomware Protection | Kaspersky. Available online: https://www.kaspersky.com/enterprise-security/wiki-section/products/ransomware-protection (accessed on 27 February 2022).
[20] What is a Trojan Virus | Trojan Horse Malware | Imperva. Available online: https://www.imperva.com/learn/application-security/trojans/ (accessed on 3 March 2022).
[21] What is Spyware | Spyware Definition | Avast. Available online: https://www.avast.com/c-spyware (accessed on 6 March 2022).
[22] What is a Computer Virus or a Computer Worm? Available online: https://www.kaspersky.co.in/resource-center/threats/viruses-worms (accessed on 11 March 2022).
[23] Conteh N. Y.; Schmick, P.J. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. Int. J. Adv. Comput. 2016, 6, 23-31. [CrossRef]
[24] What is Social Engineering? A definition + techniques to watch for. Available online: https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html (accessed on 13 March 2022).
[25] What Is Vishing and How to Defend Against It? Available Online: https://www.kaspersky.com/resource-center/definitions/vishing (accessed on 17 May 2022).
[26] Gu, Q.; Liu, P. Denial of service attacks. In book Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications; Bidgoli, H.; Wiley, New Jersey, United States., 2007; Volume 3: pp. 454-468. [CrossRef]
[27] Understanding Denial-of-Service Attacks | CISA. Available online: https://www.cisa.gov/uscert/ncas/tips/ST04-015 (accessed on 14 March 2022).
[28] Sen, R.; Borle, S. Estimating the contextual risk of a data breach: An empirical approach. Manag. Inf. Syst. 2015, 32, 314-341. [CrossRef]
[29] Davis, D. Best practices for balancing technology use and safety in a modern school. In Proceedings of Society for Information Technology & Teacher Education International Conference, Washington, DC, United States, 26 March 2018.
[30] Goldsborough, R. Protecting yourself from ransomware. Teacher Librarian 2016, 43, 70-71.
[31] Kleinberg, H.; Reinicke, B.; Cummings, J. Cyber security best practices: What to do? J. Inf. Sys. App. Re. 2015, 8, 52-59.
[32] Humayun, M.; Niazi, M.; Zaman, N.; Alshayeb, M.; MahMood, S. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab. J. Sci. Eng. 2020, 45, 3171–3189. [CrossRef]
[33] Mell, P.; Bace, R. Intrusion Detection Systems. National Institute of Standards and Technology. 2001. [CrossRef].
[34] Gonçalves, J.; Barbosa, H. A Survey of Cyber Security Systems: Approaches for Attack Detection, Prediction and Prevention. In Proceedings of the Digital Privacy and Security Conference, Porto, Portugal, 15 January 2020. [CrossRef]
[35] Liao, H.; Lin, C.R.; Lin, Y.; Tung, K. Intrusion detection system: A comprehensive review. J. Netw. Comput. Appl. 2013, 36, 16-24. [CrossRef].
[36] Chhikara, J.; Dahiya, R.; Garg, N.; Rani, M. Phishing & Anti-Phishing Techniques: Case Study. Int. J. Adv. Res. Comput. Sci. Eng. Inf. Technol. 2013, 3, 458-465.
[37] Shahriar, H.; Klintic, T.; Clincy, V. Mobile Phishing Attacks and Mitigation Techniques. J. Inf. Secur. 2015, 6, 206-212.
[38] Phishing | 10 Ways to Avoid Phishing Scams. Available online: https://www.phishing.org/10-ways-to-avoid-phishing-scams (accessed on 20 March 2022).
[39] What is a Firewall? – Cisco. Available online: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html (accessed on 22 November 2021).
[40] Types of Firewalls. Available online: http://www.ittoday.info/AIMS/DSM/83-10-41.pdf (accessed on 22 March 2022).
[41] Anwar, R.J.; Abdullah, T.; Pastore, F. Firewall Best Practices for Securing Smart Healthcare Environment: A Review. Appl. Sci. 2021, 11(19), 9183. [CrossRef]
[42] What is a WAF? | Web Application Firewall explained. Available Online: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/ (accessed on 25 May 2022).
[43] Iglesias, F.; Zseby, T. Analysis of Network Traffic for Anomaly Detection. Mach. Learn. 2014, 101, 59-84. [CrossRef]
[44] Wawrowski, L.; Michalak, M.; Bialas, A.; Kurianowicz, R.; Sikora, M.; Uchonski, M.; Kajzer, A. Detecting anomalies and attacks in network traffic monitoring with classification methods and XAI-based explainability. Procedia Comput. Sci. 2021, 192, 2259-2268. [CrossRef]
[45] Han, W.; Xue, J.; Yan, H. Detecting anomalous traffic in the controlled network based on cross entropy and support vector machine. IET Inf. Secur. 2019, 12, 109-116. [CrossRef]
[46] SIEM Tools - Security Event Monitoring Software Guide | SolarWinds. Available Online: https://www.solarwinds.com/pt/security-event-manager/siem-tools (accessed on 25 May 2022).
[47] Talal, M.; Zaidan, A.A.; Albahri, O.S.; Alsalem, M.A.; Albahri, A.S.; Alamoodi, A.H.; Kiah, M.L.; Jumaah, F.M.; Alaa, M. Compreensive review and analysis of anti-malware apps for smartphones. Telecommun. Syst. 2019, 72, 285-337. [CrossRef]
[48] Ye, Y.; Li, T.; Adjeroh, D.; Iyengar, S.S. A Survey on Malware Detection Using Data Mining Techniques. ACM Comput. Surv. 2017, 50, 1-40. [CrossRef]
[49] Arlitsch, K.; Edelman, A. Staying safe: Cyber security for people and organizations. J. Libr. Adm. 2014, 54, 46–56. [CrossRef]
[50] Using behavioural insights to improve the public' s use of cyber security best practices. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf (accessed on 25 November 2021).
[51] What is Endpoint Detection and Response? | EDR Security Definition. Available Online: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/ (accessed on 26 May 2022).
[52] What is VPN? How It Works, Types of VPN. Available Online: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn (accessed on 26 May 2022).
[53] Bulgurcu, B.; Cavusoglu, H.; Benbasat, I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Q. 2010, 34, 523–548. [CrossRef]
[54] Sommestad, T.; Hallberg, J.; Lundholm, K.; Bengtsson, J. Variables influencing information security policy compliance: A systematic review of quantitative studies. Inf. Manag. Comput. Secur. 2014, 22, 42-75. [CrossRef]
[55] Alshaikh, M.; Maynard, S.B.; Ahmad, A.; Chang, S. Information Security Policy: A Management Practice Perspective. In Proceedings of the Australasian Conference on Information Systems, Adelaide, Australia, 29 June - 1 July 2015.
[56] Aldawood, H.; Skinner, G. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet 2019, 11, 1-16. [CrossRef]
[57] Kahoot! | Learning games | Make learning awesome! Available Online: https://kahoot.com (accessed on 18-05-2022).

[58] Jigsaw | Phishing Quiz. Available Online: https://phishingquiz.withgoogle.com/ (accessed on 18-05-2022).
[59] Riskio.co.uk. https://www.riskio.co.uk/ (accessed on 18-05-2022).
[60] Pirlet, C.D. Game-Based Learning to Enhance Global Awareness. In Proceedings of International Assembly of National Council for the Social Studies, Virtual, 15-21 November 2021.
[61] Hart, S.; Margheri, A.; Paci, F.; Sassone, V. Riskio: A Serious Game for Cyber Security Awareness and Education. Comput. Secur. 2020, 95, 1-18. [CrossRef]
[62] What is Mobile Device Management (MDM) | IBM. Available online: https://www.ibm.com/topics/mobile-device-management (accessed 28 March 2022).
[63] Thanh, D.V.; Jorstad, I.; Jonvik, T. E.; Thuan, D.V. Strong authentication with mobile phone as security token. In Proceedings of the IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, Macau, China, 15 October 2009. [CrossRef]
[64] Schaffer, K. Ontology for Authentication. National Institute of Standards and Technology. 2021, 1-48. [CrossRef]
[65] Relatório Cibersegurança em Portugal - Riscos e Conflitos 2021. Available online: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf (accessed 6 April 2022).
[66] The State of K-12 Cybersecurity: 2020 Year in Review. Available online: https://static1.squarespace.com/static/5e441b46adfb340b05008fe7/t/620d58f6f14b822a371b8c7b/1645041911977/StateofK12Cybersecurity-2020.pdf (accessed on 2 April 2022).
[67] Moodle | Open Source Learning Platform. Available online: https://moodle.org/?lang=en (accessed on 2 April 2022).
[68] Classroom | Google for Education. Available online: https://edu.google.com/products/classroom/ (accessed on 3 April 2022).
[69] Video Conferencing, Cloud Phone, Webinars, Chat, Virtual Events | Zoom. Available online: https://zoom.us (accessed on 3 April 2022).
[70] Log in | Microsoft Teams. Available online: https://www.microsoft.com/en-us/microsoft-teams/log-in?rtc=1 (accessed on 3 April 2022).
[71] How to Avoid ZoomBombing. Available online: https://www.smcoe.org/employees/assets/files/Employee%20Only_FIL/Learning_FIL/ZoomBombing.pdf (accessed on 6 April 2022).
[72] The State of K-12 Cybersecurity: 2018 Year in Review. Available online: https://static1.squarespace.com/static/5e441b46adfb340b05008fe7/t/620d597eeeaef455e8c669c1/1645042048689/K12Cybersecurity-2018YIR.pdf (accessed on 7 April 2022).
[73] Call, M. K. The Impact of Teachers with Differing Levels of Degree Attainment on Student Performance in Mathematics. Doctorate, Liberty University, Virgina, United States, 2018.
[74] Das, A.; Bonneau, J.; Caesar, M.; Borisov, N.; Wang, X.F. The tangled web of password reuse. In Proceedings of the Network and Distributed System Security Symposium, California, United States, 24-26 February 2014.
[75] Spafford, E.H. Preventing weak password choices. Comput. Secur. 1992, 11, 273–278. [CrossRef]
[76] Rhee, K.; Jeon, W.; Won, D. Security Requirements of a Mobile Device Management System. J. Inf. Secur. 2012, 6, 353-358.
[77] 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. Inf. Syst. Front. 2019, 21, 1213–1229. [CrossRef]
[78] Portugal is the 2nd country in the world most affected by spam and phishing. Available Online: https://www.safecommunitiesportugal.com/cybercrimealerts/portugal-is-the-2nd-country-in-the-world-most-affected-by-spam-and-phishing/ (accessed on 2 December 2021).
[79] PORDATA - Alunos matriculados no ensino superior: total e por área de educação e formação. Available online: https://www.pordata.pt/Portugal/Alunos+matriculados+no+ensino+superior+total+e+por+%C3%A1rea+de+educa%C3%A7%C3%A3o+e+forma%C3%A7%C3%A3o-1026 (accessed on 8 April 2022).
[80] Muir, K.; Joinson, A. An Exploratory Study Into the Negotiation of Cyber-Security Within the Family Home. Front. Psychol. 2020, 11, 1-14.
[81] A Majority of Teens Have Experienced Some Form of Cyberbullying | Pew Research Center. Available Online: https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/ (accessed on 9 April 2022).
[82] Cahn, A.; Alfeld, S.; Barford, P.; Muthurishnan, S. An Empirical Study of Web Cookies. In Proceedings of the 25th International Conference on World Wide Web. Montreal, Canada, 11-15 April 2016. [CrossRef]
[83] What is Cyber Warfare | Types, Examples & Mitigation | Imperva. Available Online: https://www.imperva.com/learn/application-security/cyber-warfare/ (accessed on 11 April 2022).
[84] Gyunka, B. A.; Christiana, A. O. Analysis of human factors in cyber security: A case study of anonymous attack on Hbgary. University of West Scotland, 2017, 10-18.
[85] Aziz, A. The evolution of cyber attacks and next generation threat protection. In Proceedings of the RSA Conference, California, United States, 25 February – 1 March 2013.
[86] Blythe, J. Cyber security in the workplace: Understanding and promoting behaviour change. In Proceedings of CHItaly 2013 Doctoral Consortium, Trento, Italy, 16 September 2013.
[87] Atkinson, S.; Furnell, S.; Phippen, A. Securing the next generation: Enhancing E-safety awareness among young people. Comp. Fraud Sec. 2009, 2009, 13–19. [CrossRef]
[88] Javidi, G.; Sheybani, E. K-12 cybersecurity education, research, and outreach. In Proceedings 2018 IEEE Frontiers in Education Conference, California, United States, 3-6 October 2018. [CrossRef]