Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Bachelor Thesis

Cyber security awareness: Public and security professional perspectives

Grace Zita Zavrel

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Grace Zita Zavrel

Economics and Management

Thesis title

Cyber security awareness: Public and security professional perspectives

---

Objectives of thesis

The primary goal of this thesis is to analyze cyber security awareness in a sample of regular users.

The particle goals are:
- Create an overview of the current cyber security awareness and issues based on the literature.
- Analyze and compare the perspectives of the public and cybersecurity professionals.
- Interpret the results and discuss findings in contrast with the literature.

Methodology

The theoretical part of the thesis concentrates on analyzing scientific sources and refining the information assembled to define the research question further. The practical part will comprise data collection through interviews and surveys. Survey data will be analyzed with descriptive statistics. Interviews go through transcription, and the content will be analyzed. The conclusion will summarize all the composed data.

The proposed extent of the thesis

40-50 pages

Keywords

Cyber security, Hacking, Awareness, Human error, Measures, Survey, Interview

---

Recommended information sources

Aldawood, H., Skinner, G., 2019. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet 11, 73.

Evans, M., He, Y., Maglaras, L., Janicke, H., 2019a. HEART-IS: A novel technique for evaluating human error-related information security incidents. Computers & Security 80, 74–89.

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Security Awareness: The First Step in Information Security Compliance Behavior. Journal of Computer Information Systems, 61(4), 345–356. https://doi.org/10.1080/08874417.2019.1650676

Chua, H. N., Khor, V. V., & Wong, S. F. (2023). Examining the effect of different knowledge aspects on information security awareness. Information and Computer Security, ahead-of-print(ahead-of-print). https://doi.org/10.1108/ICS-11-2022-0183/FULL/PDF

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers and Security, 106. https://doi.org/10.1016/j.cose.2021.102267

Expected date of thesis defence

2023/24 WS – PEF

The Bachelor Thesis Supervisor

doc. Ing. Miloš Ulman, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 26. 10. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 20. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Dean

Prague on 24. 11. 2023

Declaration

I declare that I have worked on my bachelor thesis titled "**Cyber security awareness: Public and security professional perspectives**" by myself, and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break any copyrights.

In Prague on 30.11.2023 _____

Grace Zita Zavrel

Acknowledgment

I would like to thank Ing. Miloš Ulman, Ph.D., John Phillip Sabou, Ph.D., my family, friends, and interviewees, for their advice and support during my work on this thesis.

Cyber security awareness: Public and security professional perspectives

Abstract

This thesis characterizes different cyber security measures used to prevent hacking. The primary goal of this thesis is to analyze cyber security awareness in a sample of regular users. Other objectives include determining the common causes of cyberattacks and which measures best suit everyday computer users.

The theoretical part of the thesis concentrates on analyzing multiple scientific research papers, articles as well as countless books written by specialists and or former hackers. This thesis will then refine the information assembled to further define the research questions. The practical part will comprise qualitative data collection methods, such as semi-structured interviews and convenient sampling, to construct a conventional content analysis in addition to establishing a grounded theory. The conclusion will summarize the level of awareness the public has as well as determine which measures are most prevalent from all the composed data.

Keywords: Cyber Security, Hacking, Awareness, Human error, Measures, Survey, Interview

Povědomí o kybernetické bezpečnosti: Pohled veřejnosti a bezpečnostních profesionálů

Abstrakt

Tato práce charakterizuje různá opatření kybernetické bezpečnosti používaná k prevenci hackerských útoků. Hlavním cílem této práce je analyzovat povědomí o kybernetické bezpečnosti na vzorku běžných uživatelů. K dalším cílům patří zjištění běžných příčin kybernetických útoků a toho, která opatření nejlépe vyhovují běžným uživatelům počítačů.

Teoretická část práce se soustředí na analýzu mnoha vědeckých výzkumných prací, článků a také nesčetných knih napsaných odborníky a nebo bývalými hackery. Tato práce pak shromážděné informace upřesní a dále definuje výzkumné otázky. Praktická část bude zahrnovat kvalitativní metody sběru dat, jako jsou polostrukturované rozhovory a vhodný výběr vzorků, aby bylo možné kromě vytvoření zakotvené teorie zkonstruovat i konvenční obsahovou analýzu. Závěr shrne úroveň informovanosti veřejnosti a také určí, která opatření jsou ze všech sestavených údajů nejčastější.

Klíčová slova: Kybernetická bezpečnost, Hacking, Povědomí, Lidská chyba, Opatření, Průzkum, Rozhovor

Table of content

List of figures

List of abbreviations

SQL - Structured Query Language - a widely used programming language for managing relational databases and carrying out different operations on the data they contain.

USB - Universal Serial Bus - a standard interface that makes it possible for devices to communicate with a host controller, like a computer.

LAN - Local Area Network - a computer network that connects devices within a single building or a collection of related buildings, particularly one with a less than one kilometer radius.

WLAN - Wide Local Area Network - a vast information network unconnected to a particular site. Through a wide-area network (WAN) provider, WANs can make it easier for devices all across the world to communicate, share information, and do a lot more.

IT - Information Technology - the creation, upkeep, or usage of systems for storing, retrieving, and delivering information, particularly computer systems, software, and networks.

CEO - Chief Executive Officer - the person with the highest position in a corporation. They oversee a company's overall operations.

CD - Compact Disk - a small plastic disc with a pattern of metal-coated pits where music or other digital data is stored, readable with laser light reflected off the disc.

G8 summit - The Group of Eight Summit - is an annual gathering of eight of the world's most powerful nations' leaders. The goal is to promote agreement on international issues like terrorism, energy, global security, and concerns relating to economic growth and crisis management.

ICT - Information and Communications Technology - focuses on the importance of unified communications and the integration of telecommunications (telephone lines and wireless signals) and computers, as well as the essential enterprise software, middleware, storage, and audiovisual, that allow users to access, store, transmit, understand, and manipulate information.

VPN - Virtual Private Network - an online privacy protection service. In order to protect your data and communications while using public networks, a VPN creates a secure, encrypted connection for your computer to the internet.

DDOS - Distributed Denial of Service - is an attack where multiple hacked systems are made to attack a single target, overloading server resources and preventing legitimate users.

AIDS - acquired immunodeficiency syndrome - is a persistent, perhaps fatal condition brought on by the human immunodeficiency virus (HIV). HIV interferes with your body's capacity to fight infection and disease by weakening your immune system.

MS Windows - Microsoft Windows - is a set of operating systems made by Microsoft. Windows has a graphical user interface (GUI), multitasking features, virtual memory management capabilities, and compatibility with several peripheral devices. It is available in 32- and 64-bit versions. Server and client versions of Windows OSs exist.

1 Introduction

The primary aim of this thesis is to analyze cyber security awareness and determine how much the public knows about the defense against hackers. The theoretical portion focuses on analyzing scientific sources that elaborate on different types of cyber security measures and their usage in a worldwide practice. It also covers the usage of cyber security measures by professionals to discover the best way in which everyday users can protect themselves and their data.

The practical portion is built from research questions and qualitative data based on collection methods, such as interviews and convenient sampling, which will be analyzed to confirm the theories laid out in the former portion. The first method utilized is a convenient survey which aims to uncover what the average computer user employs as cyber security protection. The survey is conducted under the assumption that our participants are answering truthfully based on their personal experience and knowledge.

The second method relies on semi-structured interviews to evaluate how the cyber security world functions. Interviews were conducted to discover which methods are applied in the real world in real-life situations and to find out which of them bring the most benefit and which are not as beneficial to the end user. The questions in the survey and the interviews are intertwined, allowing for some overlap in data; however, the interviews are far more in-depth than the surveys. The surveys are built on specific research questions regarding things such as the participants' experiences as the target of a cyber-attack or hacker, how to react and proceed, computer protection, company computer protection, education on cyber security, breach/attack protocols, phishing, viruses, scams, and hacking. Every interviewee is an employee of a larger IT firm and is somehow connected to cyber security.

2 Objectives and Methodology

2.1 Objectives

This thesis aims to seed through various cyber security measures and try and determine which of these are best for the protection of computers, data, and systems. Which strategies best safeguard people from malevolent hackers. In this consideration, the literature review and thesis will aim to cultivate and articulate the research question. This will then cast a light on a deeper understanding of how users operate and how security measures can be refined.

While focusing on the measures themselves is crucial to understanding this topic, establishing what everyday users know is also a significant part of the study itself. Determining the level of knowledge and which cyber security measures individuals use actively to protect their desktops and laptops is essential to debunking what the best approaches generally are. Subsequently, discovering what experts in the cyber security field utilize to safeguard themselves and their firms may reveal some secret algorithm that is not known to the public or just so lost in translation that people do not benefit from it.

2.2 Methodology

To achieve the objectives mentioned above, this thesis employed two methodology types. The first method employed was a convenient survey to assess what the average computer user uses as cyber security protection. This method should allow us to reach out to a diverse range of people from various backgrounds and learn about their personal experiences. With this, we can figure out how deep their understanding of cyber security is. The second method employed was semi-structured interviews. These were to evaluate how the cyber security world works. Each interview was conducted individually with the same set of questions. The grounds for selecting interviews as the second methodology utilized was to have a way to evaluate if what everyday users knew was enough and if they did enough to protect themselves virtually. Later these two methods are evaluated and compared to find where information overlaps and where information is lacking.

3 Literature Review

3.1 Cyber Security

Cyber security means protecting systems, networks, and programs against digital attacks. Accessing, altering, and destroying important information, extorting money from users, and disrupting business processes (Ma 2021). Enforcing cyber security effectively and accurately is one of the challenges of today's world; because the number of devices has grown, and hackers have become more ingenious (Katsantonis, Mavridis, Gritzalis 2021).

Security risks are rising due to the development of communications on an international scale and cloud services to store sensitive and private data (Alhayani et al. 2021).

Cyber security threats are generally divided into three categories:

(a) Cyber-crime: A individual or party that targets systems to monetize, restrict, intimidate, or sabotage.

(b) Cyber-attack: Usually politically motivated with the objective of intentionally accumulating information.

(c) Cyber-terrorism: Desires to intimidate by destroying electronic systems or altering their function, or simply taking it out of service.

In addition, the most common techniques of threatening cyber security comprise malware (viruses, Trojans, ransomware, spyware, Adware, and Botnets), SQL injection, Phishing, Man-in-the-middle attack, Denial-of-service attack, and Social engineering (Ma 2021). For better protection from these threats, knowing the different types of cyber security is necessary.

Network Security aims to protect computer networks from disruptors, malware, or hacking. It is a collection of solutions that enables organizations to keep their computer networks out of the reach of hackers, organized attackers, and malware (G. A. 2005).

Application security incorporates the use of antivirus programs, encryption, and firewalls to protect the system against external threats that may interfere with application development (Alkatheiri, Chauhdary, Alqarni 2021). Lately, it is also about preventing in-house programmers from inserting code into existing software that has the effect of enriching, abusing, or taking over permissions.

Information Security protects physical and digital data against unauthorized access, disclosure, misuse, unauthorized changes, and deletion (Li, Liu 2021).

Operational security comprises methods and decisions constructed to manage and protect data, preventing misuse (Ogbanufe 2021).

Cloud Security protects data in the cloud (based on the software) and monitors it to remove the risks of the on-site attack (Krishnasamy, Venkatachalam 2021).

End-user training refers to unforeseen aspects of cyber security, namely individuals. Anyone can unintentionally get a virus into the security system. Teaching users to remove suspicious attachments in emails, not connecting to anonymous USBs, and other critical issues should be part of any corporate security plan (Li, Liu 2021).

Cyber security is an essential issue in the infrastructure of every company and organization. Cyber security oriented companies or organizations can achieve high status and countless successes because this success results from the company's capability to protect private and customer data against a competitor. Practical measures protect the information, networks, and data against internal or external threats. Cyber security professionals protect networks, servers, intranets, and computer systems. This security ensures that only authorized individuals have access to that information (Li, Liu 2021).

3.2 Hacking

The essence of hacking is finding unintended or overlooked uses for the laws and properties of a given situation and then applying them in new and inventive ways to solve a problem (Erickson 2008). It is the unauthorized use of computer and system resources. Computer hacking is the act of modifying computer hardware and software to achieve a goal other than the maker's intended purpose (Kumar, Agarwal 2018).

Hackers are progressively prevalent and skilled in their assaults on social engineering. They will collect diverse information from different outlets, including social media, personal blogs, and data, and carefully collect important key data from well-meaning workers, who are used by such cybercrimes to target networks, capture valuable information, and even ransom companies and, in some cases, harm objects (Alghamdie 2021). If you were lucky enough to consider a career as a computer hacker, you will have to decide if you will aspire to safeguard the common good or settle for pettier goals. Do you want to be a mischievous criminal hacker or a righteous powerful defender? (Grimes 2017) The only way to become skilled at hacking is to practice, not by reading the language of a few manifestos or following instructions discovered in files (Gunkel 2001). Because of this, the hacker has played—and still plays—both the hero and the villain in many cyber reports (Gunkel 2001).

Proof plays a more contributing part, and failure to successfully punish cyber criminals' results from a lack of evidence to be presented in court. Two main variables contribute to the fulfillment of testimony, such as receiving proof valid for the responsibility of persons. Secondly, few organizations in cybercrime situations that are planned, committed, and resource-based have legal knowledge. Those challenges reduce the likelihood of prosecution and detention of a suspect, even if arrested (Alghamdie 2021). Like any parasite, hacking operates within its host country in a way that protects and supports the environment on which it depends. Its goal is not to destroy the host system but to simply use it (Gunkel 2001).

3.2.1 Cyber security measures

Cyber security has always been a specialized area, with only the cyber community understanding the need to safeguard itself from cyber threats. However, the recent rise in cybercrime affecting end users has changed this perspective (Al-Sharif et al. 2016). Companies will often invest in preventative controls and safeguards to avoid or minimize the possibility of cyber security attacks and measures to identify, manage, and reduce net losses from cyber security attacks. Measures used by corporations to prevent intrusions include firewalls, software encryption, and virus detection. Other corporate options include computer security investments, incident response teams, and cyber-insurance products (Jeyaraj, Zadeh 2022).

Technical Security Measures

Firewall

Firewalls have become the fundamental source of protection against large cyberattacks, impacting both conventional and contemporary networks and ensuring the security of internal networks from exterior (and potentially malicious) networks. Firewalls play a significant role in guarding, filtering, and managing all traffic transmitted and received from any computer, Local Area Network (LAN), or Wide Local Area Network (WLAN) internal networks from unauthorized intrusions or external assaults. Firewalls are either hardware or software devices that filter and regulate information flowing from the internet to one's private network or individual computer. They allow only data that is regarded safe and harmless to pass in and/or out (Anwar, Abdullah, Pastore 2021).

Antivirus software

To secure IT assets, end users are frequently presented with various classes of fundamental security measures based on their usage situation. However, the first security suggestion offered to all users is installing an antivirus on their devices. In fact, antivirus software is widely regarded as one of the most effective anti-malware solutions. They are installed in most users' personal computers and businesses and are implicitly trusted by the vast majority of users. They are also part of the trusted computing base (Genç, Lenzini, Sgandurra 2021). Antivirus software is the primary detection and classification program for malware, and it has progressed in tactics, employing processes based on signatures, heuristics, rules, and, most recently, artificial intelligence. The typical approach used by

antivirus programs is Signature detection, which is based on a vendor-generated database. Any file that is downloaded to the machine is compared to the database, and if a match is found, it is malware. The issue with signature-based detection is that it will only identify samples that have already been recognized and whose signature has been saved in the antivirus system database. Heuristic detection approaches were developed to supplement signature-based detection and address its shortcomings. The functioning of heuristic algorithms is based on several factors, each with a score, which decides whether a file is dangerous. The three most frequent methods for doing this analysis are:

Generic: Compares the activities of one file to those of another that have already been flagged as harmful.
Passive: Examines each file independently to discover how it operates.
Active: Runs the sample in a safe environment (sandbox) to determine whether its activity is harmful. This approach is difficult to execute and results in considerable delays; however, it may be avoided by introducing payload activation delays (Pérez-Sánchez, Palacios 2022).

Antispyware

Antispyware tracks attacks, detects dangerous spyware and clears it from the system (Lee, Kozar 2008). There are several antispyware programs available on the market. These antispyware programs' mechanisms may be divided into two groups Signature scanning and Network filtering (Chow et al. 2005). The signature scanning approach is like that used in antivirus software. Essentially, for each known spyware, a combination of bytes known as the spyware signature is discovered. These signatures are saved in a database. The antispyware tool compares the suspected software to this database. If the software fits any signature, it is classified as spyware. Signature scanning can only detect known spyware, and users must often update the database (Chow et al. 2005). Network filtering can only check for the presence of known spyware. It is difficult to restrict just spyware-related Internet access activities from the application in which the spyware is contained. Some antispyware software just deletes apps with spyware attached from the system, causing users to lose the program's original "useful" functionality (Chow et al. 2005).

Encryption

Cryptography and cryptographic techniques are particularly essential for ensuring network and computer system security. The two most used encryptions used to safeguard the privacy of communications in transmission are link encryption and end-to-end encryption. Link encryption encrypts a single link in a communication network, and end-to-end encryption encrypts a path in a communication network from beginning to finish. Cryptography may be used in computer systems to offer access control and prevent unauthorized users from reading, modifying, or accessing resources (Wright 2003). Cryptography is also utilized in electronic commerce as an essential security feature. One well-known example is the use of cryptography to verify a seller and encrypt a credit card number during the process of purchasing products on the internet. Another place it may be found is in the arts. When a creator of digital content posts a video or audio file online, encryption can safeguard the material and prevent extensive redistribution of the content without being noticed (Wright 2003). Encryption ensures the confidentiality and privacy of customer data and the security of sensitive information. Encryption protects data in the event that malevolent individuals or administrators get access to information and promptly check out documents, rendering stolen files or duplicated disk photos unreadable. Data-layer encryption provides consistent safety across several systems, regardless of the operating system type. Encryption satisfies our requirements for large-scale data security (Kashyap 2019).

Two-factor authentication

Strong authentication and restricting access to a network and resources are an important security need for electronic devices connected to the internet. Passwords, tokens (chip card, smartphone,...), and biometrics (fingerprints, etc.) are three typical authentication elements (Aman, Basheer, Sikdar 2019). An account being compromised is avoided by using two-factor authentication. A two-factor authentication protected account often requires an individual to verify with something they know (typically a password) as well as something they possess, such as a mobile phone or hardware token (Reese et al. 2019). Two-factor authentication is frequently used to strengthen security (Aman, Basheer, Sikdar 2019). An issue with many electronic devices is that they are physically unprotected. They are usually in easily accessible areas to anyone, including people with malicious intent. As a result, an attacker may effortlessly seize and use these devices to

carry out physical and side-channel attacks. Attackers may be able to successfully acquire passwords from the device's memory and perform a spoofing attack. In such exploitations, the attacker poses as an internet node and may acquire remote access to vital network resources. These problems can be minimized with two-factor authentication (Aman, Basheer, Sikdar 2019).

Automatic logout – secure login

Desktop computers are still widely used in offices and households, typically by numerous users. Users authenticate themselves before using the computer (e.g., by signing in with a username and password) and de-authenticate (i.e., log out) after usage to prevent unwanted access. Most authentication techniques, however, miss this critical de-authentication phase (Mare et al. 2014). The consequences of failing to log out of a computer can be severe: a malicious attacker with access to your desktop might rummage through your personal information, edit, or destroy your data, or steal your credentials to act on your behalf. Even in a non-adversarial environment, other authorized users may exploit your account if you fail to log out (Mare et al., 2014). The most popular solution to the de-authentication issue is 'timeouts,' or executing an automated logout after a period of inactivity (Mare et al. 2014).

Back up data/computer

Data and information backup is a crucial responsibility of the company's employees. It is widely known that data and information backup is critical for future operations. People and workers do not perform data backups due to the absence of information, equipment, and carelessness, and they are unaware of the importance and effect of data loss. There are several data backup techniques and technologies available on the market today. Major information and data security tools include antivirus, firewalls, passwords, digital signatures, and encryption technology. The automated electronic system requires backup security, including password security and power backup security, as well as maintenance and protection against threats such as theft, damage, or loss of data and databases. An online security system, as well as manual security mechanisms, must be carefully controlled. In government institutions, businesses, personal life, data, and information are saved in many ways. It is reported that the most common data backup method (50.7%) is using a hard disk. Other techniques include utilizing a pen drive (40%), entering the password into a

workstation computer (35%), using an external hard disk (27.9%), servers (22.1%), and Google Drive/ Sky Drive (6.4%). Cloud computing is becoming increasingly popular for data backup and access. Because of the lack of security in the networking system and the internet, Google Drive and servers are unsafe. Memory cards, CDs, USB drives, and floppy disks can all fail and lose data. At least two or three backups should be created in a company, person, and government offices. It is preferable to keep the server in the user's country rather than in another's (Giri, Shakya 2019).

Organizational Cyber Security Measures

Complex passwords

The ability to identify oneself and what one is allowed to access is crucial in the virtual world, just as having a safety deposit box to protect what is valuable in the physical world and identification cards to prove one's identity. Authentication is used to establish one's identity online and prove an account's ownership. Passwords are probably the most prevalent form of authentication. While many actors encourage using strong passwords, users commonly adopt methods to make their passwords simpler to remember. A password is computationally secure if it can withstand attacks for an extended period or is difficult to guess using a dictionary or brute force attack. This attribute is often attained by using lengthy passwords with a variety of characters (Kävrestad et al., 2020).*Educating users*

Social engineering is described as a means of exploiting a flaw in human nature and taking advantage of the typical person's ignorance. Although social engineering approaches have changed over time, the effectiveness of such attacks continues to rely on contemporary preventative tools and security measures and the availability of educated and professional employees dealing with sensitive data in businesses. Corporations aim to prepare their employees for social engineering dangers by providing creative and engaging education, training, and awareness programs (Aldawood, Skinner 2019). This includes training materials, legislative and legal frameworks, and instruction on safety measures to be done before and after attacks. Aside from regular training, firms may run timely information security awareness campaigns to emphasize the significance of keeping ongoing alertness (Aldawood, Skinner 2019). Defense methods for social-engineering attacks include security education and training, increasing societal awareness of social-engineering attacks, equipping people with the tools they need to recognize and prevent these threats, learning how to protect sensitive information, notifying the security service of any suspicious

behavior, arranging new hire security orientations, and educating all staff members about the potential for attacks (Salahdine, Kaabouch 2019). To identify phone-based attacks, it is crucial to confirm the source of calls using a contacts list that has been recorded, to be vigilant of obtrusive and unwanted calls, to request a callback, or to pose questions with private responses to the caller in order to establish their identity. Refusing to take these calls is the best way to stop these attacks. Attacks on the help desk can be prevented by giving PINs to recognized callers. When responding to a call request, the help desk must adhere to the script (Salahdine, Kaabouch 2019). When email-based attacks occur, some companies use honeypot email addresses, sometimes referred to as spam traps, to collect and send spam to employees. The server marks emails coming from spam trap lists as harmful and temporarily bans them. Other safety measures include verifying the sender of emails before clicking on a link or downloading an attachment, looking at the email header, getting in touch with the known sender if in doubt, and deleting messages that contain quick money or exciting news (Salahdine, Kaabouch 2019).

3.2.2 Exploitation

“There's nothing good or bad about knowledge itself; morality lies in the application of knowledge” (Erickson 2008).

When diving in deep and studying this quote, we can understand the root of exploitation, for exploitation is the art of using someone else’s work to our own benefit. A hacker takes a program or code, then finds its weakness. A hole in the program, if you will, and uses it against the original program. It is the staple of hacking (Erickson 2008). An easy way to bring a better understanding to this phenomenon is through a simple joke.
A man is out wandering in the woods when he comes across a magical lamp on the ground. He instinctively picks up the lamp, rubs the side with his sleeve, and a genie emerges. The genie expresses gratitude to the man for releasing him and offers him three wishes. The man is overjoyed and knows precisely what he desires. "First and foremost," the man declares, "I want a billion dollars." A briefcase full of money appears out of thin air when the genie snaps his fingers. "Next, I want a Ferrari," the man says, his eyes wide with wonder. A Ferrari rises from a cloud of smoke when the genie flicks his fingers. "Finally, I want to be irresistible to ladies," the man says. The genie transforms the man into a box of chocolates with a snap of his fingers.

A program will follow its instructions exactly, and the consequences aren't necessarily what the programmer meant, just as the man's final request was fulfilled based on what he said rather than what he was thinking. The consequences can be disastrous in some cases (Erickson 2008).

There is no question that the concept of exploitation is deeply tied to one or more concepts of use; therefore, exploitation is the same as utilizing someone. Generally speaking, you are more susceptible to exploitation if you are less wealthy, educated, crafty, or ruthless than another company or have any other vulnerability within your system. One's vulnerability is exploited when a hacker utilizes this weakness to gain access to a system or company and uses it against the hacked entity. As Kant defines, exploiting someone is viewing them just as a means to an end rather than as an "end in themselves." (Mitnick, Simon 2002)

3.3 Cyber security awareness

The concept of cybersecurity awareness is generally understood as the knowledge and understanding that individuals, organizations, and the public have about the risks and threats related to cybersecurity. It involves being conscious of potential cyber threats, understanding best practices for securing information and systems, and being vigilant about maintaining a secure online environment. Cybersecurity awareness often includes education and training programs to help individuals recognize the importance of information security, understand common cyber threats, and adopt good cybersecurity practices. These programs aim to create a culture of security within an organization or community (ISO 2022) (ISO 2023). While there is no standard for cybersecurity awareness, there is an information security management system standard that organizations can use to establish, implement, maintain, and continually improve an information security management system. It includes a focus on creating awareness among employees and stakeholders about information security risks and responsibilities.(ISO 2019)

At this current point in time most people know they need to be vigilant while browsing the internet. That doesn't always mean they are fully aware of the dangers that lurk on the world wide web. In an era where the digital realm intertwines with nearly every facet of our lives, cyber security awareness stands as a critical shield against the evolving landscape of cyber-attacks.

Cybersecurity Awareness in the Workplace

As previously mentioned, the surge of cyber-attacks has posed a formidable challenge. Ransomware attacks, phishing schemes, and data breaches have become prevalent, targeting individuals and organizations with increasing sophistication. These threats demand an informed populace capable of recognizing and thwarting potential risks. Moreover, the global shift toward remote work, accelerated by the COVID-19 pandemic, has amplified the need for cyber security vigilance (Zwilling et al. 2022). In the dynamic landscape of cybersecurity, the confluence of technical intricacies and the pivotal role played by non-expert end-users in online interactions presents a difficult challenge. As custodians of decisions regarding privacy settings, password robustness, and adherence to security policies, users are at the forefront of ensuring cyber resilience through informed decision-making. Acknowledging a discernible knowledge gap among non-expert users (Zhang-Kennedy, Chiasson 2022). Employees accessing sensitive information from various devices

outside the secure confines of their offices call for heightened awareness to mitigate vulnerabilities arising from this shift. Smart devices, often lacking stringent security measures, expand the attack surface for hackers, necessitating a well-informed populace to safeguard against potential breaches (Zwilling et al. 2022). Employees' information security awareness is highlighted as a critical factor influencing information security behaviors and policy compliance. Lack of information security awareness is identified as a major cause of mishandling sensitive information. Unaware employees are identified as a significant vulnerability for organizations. This vulnerability can result in substantial financial losses and reputational damages, particularly with the enforcement of data protection laws like GDPR (Khando et al. 2021).

Perceptions of Cybersecurity Awareness in Everyday Users Lives

In parallel, the concerning escalation in data breaches and privacy infringements underscores the need for robust cyber security measures. Individuals' heightened awareness is vital in safeguarding their personal information against unauthorized access and exploitation. (Zwilling et al. 2022) Personal experiences with cyber threats, such as falling victim to scams or identity theft, can significantly impact how individuals perceive the importance of cybersecurity. Those who have encountered such incidents may be more vigilant and proactive in their online behaviors. (Dhillon et al. 2019) Cyber security awareness also confronts the growing threat of social engineering tactics and misinformation. Hackers skillfully exploit human psychology to manipulate individuals into divulging sensitive information (Smith, Ali 2019). Individuals may recognize the importance of cybersecurity awareness in safeguarding their personal information. This could involve using strong and unique passwords, being cautious with sharing sensitive details online, and regularly updating software for security. Furthermore, the propagation of misinformation and fake news can serve as a conduit for social engineering attacks or breaches, underscoring the need for informed and vigilant individuals. Younger generations, who have grown up in a digital age, might be more accustomed to online security practices, while older individuals might be learning and adapting to new cybersecurity norms. This era also witnesses the rapid evolution of technology. Emerging innovations, from AI to cloud computing, offer unprecedented opportunities while simultaneously presenting new challenges in securing these advancements. A comprehensive understanding of cyber security becomes indispensable to navigate these complexities (Zwilling et al. 2022). Public awareness

campaigns, government initiatives, and regulatory requirements related to online safety can also shape individuals' perceptions of cybersecurity outside of the workplace (Dhillon et al. 2019).

3.4 Identifying the problem

In today's age, the finest techniques in cyber security exist. Yet there are endless cyberattacks daily. So, what is the issue? Is it the technological improvements that evolve every day, producing never-ending loopholes that may be exploited. Or is there a lack of understanding and knowledge of these measure? How many people know how to defend themselves and their companies? Is simply knowing of these measures and being able to utilize their basic functions enough or does one need to fully understand what he or she is doing to make their devices "safe"? Is just being aware of the existence of hackers enough? Given the current state of affairs, people would be tempted to say no, and they would be correct. Yet when it comes to cyber-attacks the story tends to be how it happened to someone else. Not often do we hear "You won't believe what happened. Yesterday I got hacked.". With this people tend to grow less vigilante, they trust more. So how can we safeguard ourselves better in order to not become one of those stories?

The unregulated use of devices by individuals is one of the most serious information security issues that many firms face (Al-Sharif et al., 2016). Many breaches have been discovered to be the result of some type of human mistake. Six hundred twenty-eight examples of inaccurate or improper data being shared through emails, letters, and faxes, four hundred and one cases of data loss or theft, one hundred fifty-nine cases of information being exchanged with a third party, and ninety-nine cases of unauthorized individuals accessing or exposing data were among the breaches (Evans, He, Maglaras, Yevseyeva, et al. 2019). According to studies, organizations typically neglect human error as a key source of security breaches and instead focus on their technical measures. Human mistake or behavior is responsible for over 90% of cyber-attacks (Evans, He, Maglaras, Janicke 2019).

Human error may be classified into two types: person approach and system approach. The person approach focuses on errors made by individuals at the front lines, a person executing the work, and considers these errors to be the result of recklessness, negligence,

carelessness, inadequate motivation, inattention, and forgetfulness. This approach supports the notion that mistakes are moral concerns (Evans, He, Maglaras, Janicke 2019). The system approach recognizes that humans are flawed and that mistakes will occur even in the finest organizations and to the most diligent people. The system approach can be subdivided into 'active failures' and 'latent failures.' Active failures are characterized as errors or procedural breaches committed by individuals executing the work in the form of slips, lapses, and blunders that are difficult to anticipate. Whereas latent conditions are characterized as the inherent defects or vulnerabilities inside the system that originate from individuals creating everything, such as designers, procedure authors, and top-level management (Evans, He, Maglaras, Janicke 2019). Through the ages, people and companies have learned that there are ways to protect themselves against malicious hackers. Yet studies have shown us that countless cyberattacks still happen daily.

3.5 Summary

The literature review contributes valuable insights into the multifaceted realm of cybersecurity. It explores the definition of cybersecurity, emphasizing the protection of systems, networks, and programs from digital attacks that target critical information, finances, and business processes. The escalating security risks are attributed to the global expansion of communication and the adoption of cloud services. The review identifies cybersecurity threats, encompassing cyber-crime, cyber-attacks, and cyber-terrorism, employing techniques such as malware, SQL injection, phishing, and more. Different cybersecurity domains, including network security, application security, information security, operational security, and cloud security, are discussed as measures against diverse threats. End-user training emerges as a crucial aspect, addressing human factors and preventing unintentional security breaches. Cybersecurity awareness, both in the workplace and in individuals' lives, is underscored as pivotal in countering the evolving landscape of cyber threats.

In the relentless landscape of cybersecurity, where cutting-edge techniques coexist with persistent cyber threats, a critical question arises: are the incessant cyberattacks a result of ever-evolving technological vulnerabilities or a lack of understanding and knowledge of security measures? This narrative delves into the duality between advanced cybersecurity measures and the human factor, questioning whether mere awareness of security measures suffices or if a deeper comprehension is essential for true digital safety. Despite the

prevalence of cyber threats, individuals often perceive these incidents as distant tales, leading to a sense of complacency and trust.

RQ1: How much cyber security awareness do people have and how can everyday users better protect themselves virtually?

4 Practical Part

4.1 Research methods

This thesis employed two research methods: a convenient survey and semi-structured interviews. These methods were chosen because they were the best way to gain real-time information on how much knowledge everyday computer users actually possess regarding cyber security. In order to avoid any prejudice a general set of questions was asked in both research methods. When utilizing a survey, the work is conducted under the assumption that our participants are answering truthfully based on their personal experience and knowledge. In relation to the interview, we can figure out how things are applied to the real world in real-life situations. Find out what works and what is not as beneficial as we thought.

4.2 Survey distribution

The survey was conducted in two languages using an online platform for participants to fill out. The online platform chosen was google forms. Google forms is a platform that lets a person create a survey in an easy, quick, user-friendly way and analyzes data collected in real time. Creating the survey this way made putting all the questions together and later analyzing them less time taxing. Distribution of the survey was simple as well, thanks to the platform providing a link which was then sent out via email, Facebook and other communication platforms to people of convenience, who then sent it to others in order to spread the survey further. The survey was created on google forms in view of the fact that individuals would have easy access to the survey form, and the way the platform has their forms set up allows convenient evaluation of not only participants solo responses but also questions that were grouped together. As mentioned before said survey was put together in two different languages. The chosen languages were English and Czech. Both surveys had the same number of questions and the same answers. Both were then thoroughly evaluated and combined into an excel spreadsheet to create one single string of results for easier assessment. The Czech survey consisted of 93 participants, and the English survey consisted of 28 participants, bringing us to a total sample size of 121 participants.

Four sections make up the entire survey. The first part was meant for all participants, the second for individuals that use a computer for personal use, the third was for individuals who use a company computer, and the last part was a set of four scenario questions for each

participant to answer. Each question was then evaluated separately and calculated based on the number of participants that answered. The survey on its own took approximately ten minutes to complete and consisted of 38 questions. The questions were constructed with the goal of gaining as much information as possible about the amount of knowledge people have about cyber security. We wanted to find out if people know what is on their computers and how to protect them. We asked about different security measures and which they utilize.

Survey Target Group

We wanted to make our target group as wide as possible but not so far off that the results would become invalid. In order to achieve that, people who actively use computers every day for work or personal use were targeted. Individuals who utilize tablets or phones as their primary connection to the cyber world were not taken into account. During the distribution of the survey, it was important to spread it in groups and to individuals who actively used computers. When scaling down the sample pool, the main age group ranged from twenty to forty years old. Further, the survey was aimed towards people working in different sectors other than internet and computer technologies. This was done for the fact that the goal was to obtain knowledge on how people not actively connected to the cyber world would react in different situations and what they have experienced.

4.3 Semi-structured interviews

The second research method selected, were semi-structured interviews. A group of computer specialists from various companies were chosen for these interviews. This selection was made based on connections made through networking and then refined based on the positions of the specialist and the company they worked for. It was imperative that each specialist had a different position and company for there to be a wider array of viewpoints. Each of these interviews were conducted separately at different points in time over the course of a few months. Every meeting was carried out face-to-face in an inviting setting. These interviews had a set of premade questions, and the interviewer had a notebook and pen to jot down notes as well as write down any extra questions or topics that may have come up during the meeting. Each interview was recorded with the consent of the interviewees so that it would be possible to return to the given information at any time. Since the specialists are of Czech descent, the interviews were conducted in the Czech language and then translated to English and converted to transcripts. The individual meetings took

approximately 60 min and consisted of 32 preset questions, not including any extra questions that came up during the conversation. Questions ranged from personal opinions about cyber security to company-based ones as well as questions about today's innovations that revolve around the cyber world. Some questions were similar to those that appeared in the convenient survey; however, the greater amount was in mere correlation with the survey. Since cyber security not only as a whole but within corporations is being discussed, after each interview, all identifiers were removed from the record to keep animosity and protect each individual's information, including their firms. This way, interviewees felt more comfortable sharing information that could be a little more revealing to an individual with sinister intentions.

4.4 Study limitations

Like with every study, constraints developed during the process of evaluating and acquiring data, and this study was no exception. Overall, there were two main limitations: (1) in retrospect an insufficient sample size, (2) the inability to convey and gather information in depth. The first constraint emerged during survey distribution. One would think that because the survey took place online, it would be easier to reach a bigger number of people, which is usually true in principle and practice. However, when a large number of people were asked to do a survey on cyber security for a bachelor's thesis, some questioned the survey's credibility. With the prevalence of phishing attempts in today's world, it's reasonable that some questioned whether or not this was a genuine study. This, however, provided insight into how people handle dubious links. This, in and of itself, aided in establishing how participants saw cyber security. Nonetheless at the end of the survey period the study had sufficient results.

The second constraint was also a result of the initial study method. Despite the survey yielded a large number of responses and provided the figures needed to compare with what IT specialists say, certain questions might have benefited from more in-depth follow-up questions in retrospect. Some participants provided only one-word responses, which was sufficient to acquire the necessary data, but it would have been more enlightening to have more information on the individuals' cognitive processes.

5 Results and Discussion

5.1 Survey

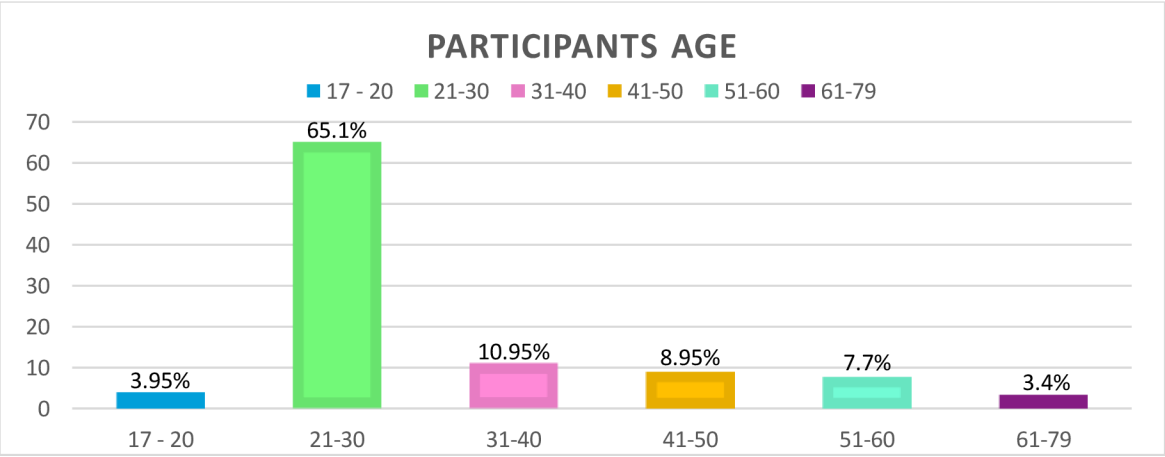
Participants

Within the survey, there were four questions to help identify who a part of the sample was. Firstly, age. Secondly, type of work. Then, what type of computer they had, either laptop or desktop. Last, if they use a personal or company computer. The highest-ranking number of participants were from ages twenty-one to thirty. They made up 65% of our sample. From there on out, we had smaller samples from different age categories. People aging from thirty-one to forty made up 11% of our sample, forty-one to fifty were 9%, fifty-one to sixty 8%, seventeen to twenty 4%, and lastly, sixty-one to eighty made up 3%. Age isn't as big of a contributor as one would think. However, it does still play a role in cyber security. The reason for that is the older an individual is, the more difficult it becomes to keep up with the growing innovations and threats in the cyber world. On the contrary to this, the younger an individual is, the less they pay attention to what could be malicious and rather focus on their goal, whether that be obtaining the newest video game that hasn't come out yet or just downloading a cheat sheet for their homework.

Professionals' perspectives

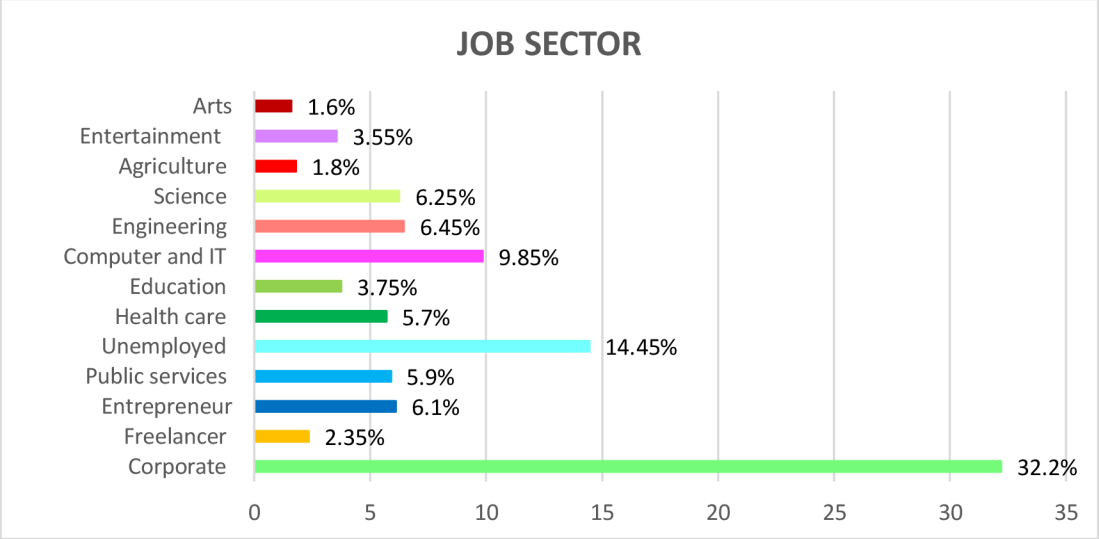
The statement above is further supported by interviewed specialists who say that younger people are more inclined to be less cautious on the internet, whereas the older generation shies away from fully educating themselves.

Figure 1 - Participant Age



When focusing on the second identifier, what job sector someone works in, it is important that they are not a part of the ICT community. If there were to be an overpowering percentage of people in this sector, the answers would no longer be valid since the goal is to gain knowledge that would potentially advise people who are not as well versed in cyber security. In the sample of 121, only 9.9% of people were from the ICT sector, which implies that 90.1% are not people well versed in cyber security. This shows that the sample is what was hoped for, meaning that the information gathered is from individuals that presumably do not have an in-depth understanding of cyber security.

Figure 2 - Job Sector



Next, what type of computer individuals use was identified. This factor is important to the study because, based on the type of computer, individuals tend to treat their devices differently. Knowing what type of computer, a user has could inform us if users treat their security differently or not. The results showed that 50% of participants use laptops, 14% use a desktop computer, and 36% use a combination of both.

Professionals' perspectives

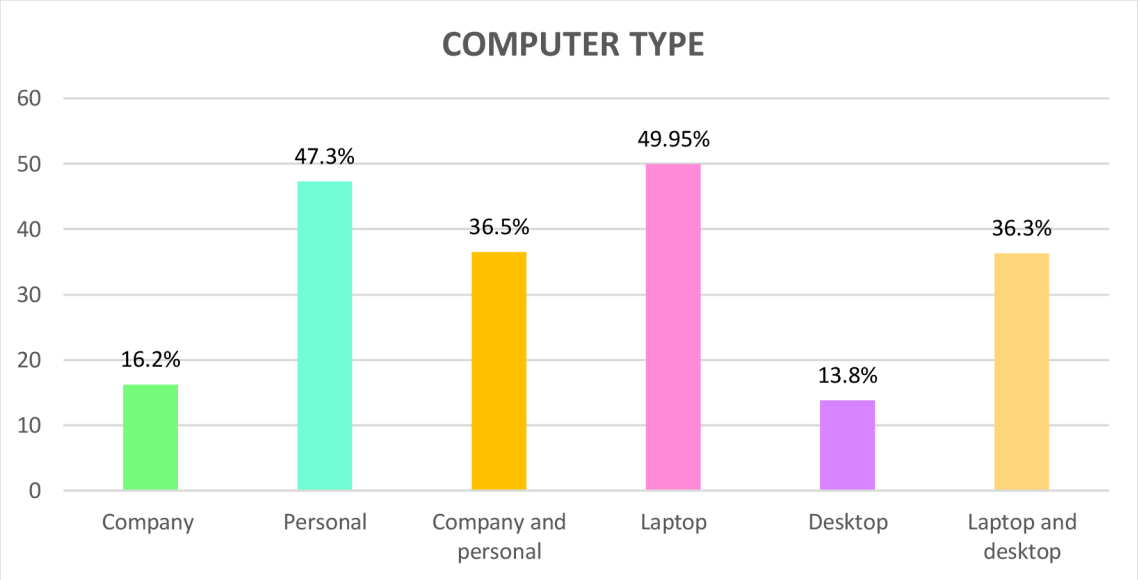
Interviewed specialist A says, a person using a desktop in a work setting will have a set defense by their company in most cases. In correlation to this, a person using their desktop at home will also have a different security system set up. Whereas laptop users need to account for connecting to multiple different internets serves, making their protection differentiate.

Finally, the last differentiator comes into play, and that is a company vs. personal computer. The survey shows that 47% of people use a personal computer and 16% use a company computer, the remaining 37% use both a company and personal computer. As briefly mentioned above, people with company computers are more likely to have a preset security system from their ICT department. Home users are more commonly less vigilant thanks to the fact that they might not feel they would be the aim of a cyber-attack. They hear of attacks happening but don't account for actually being attacked.

Professionals' perspectives

Specialist B used an in-home example to explain this. They gave an example of a child taking their parents credit card and filling out information on a video game site in order to buy something. In this scenario and most cases, it is assumed a child doesn't have their own computer but uses their parents which show cases lower vigilance in a home setting.

Figure 3 - Computer Type



Cyber Attacks

Before uncovering how many participants have fallen victim to a cyber-attack, it is important to see if they even viewed themselves as potential targets. Above, it was mentioned that a lot of the time, people do realize that they could be the victim of an attack; however, sometimes, they may feel it wouldn't happen to them. Thus, the survey takers were asked if they thought they could be the victims of a cyber-attack. Luckily most answered yes. Only 24% thought they were immune to the dangers of the cyber world. The rest of the participants, 76%, said they believed they could be attacked.

Professionals' perspectives

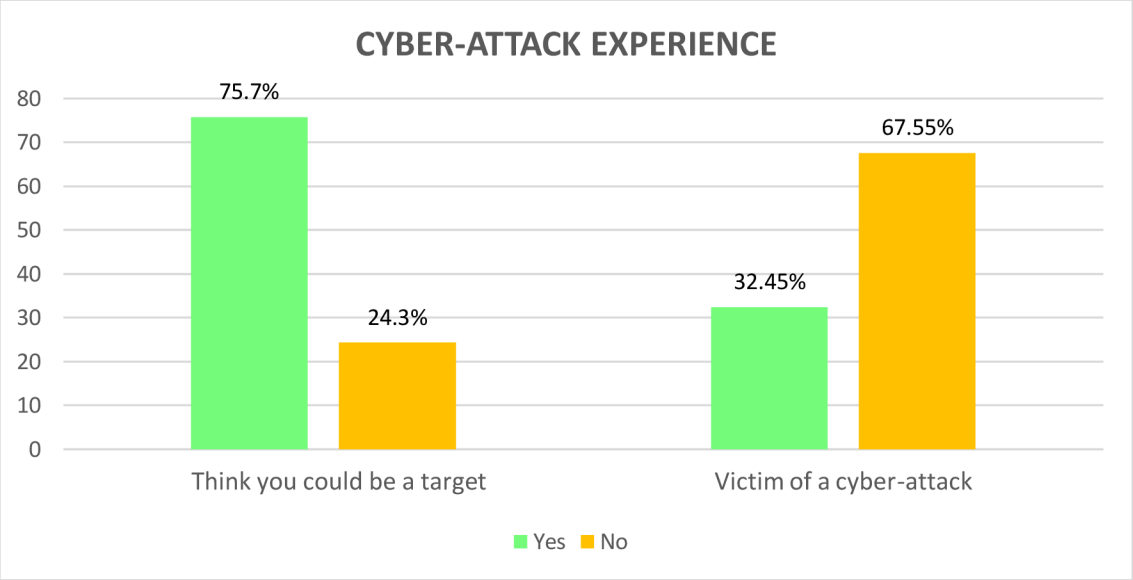
When speaking to the specialists all concur that people approach security as something they set up and no longer need to touch, it is an afterthought.

The survey shows that only 33% of the participants have been the victim of a cyber-attack. When looking deeper into the different answers, it showed that 36 people from the 121 sample were attacked. However, when reviewed, a question that correlated with the original question, "I have been a victim of a cyber-attack in the past?" resulted in inconsistent numbers. The question "If the previous statement applies, did you know how to react and proceed when the cyber-attack occurred?" gave confusing results. As mentioned above, 36 people said they were victims of a cyber-attack, yet 61 people replied to the second question. This either means people replied about their competence of knowing what to do if they ever got attacked, or they lied in the previous question. Considering that 36 people replied they didn't know what to do but figured it out once the problem occurred, and 25 said they knew what to do, it can be assumed that some people answered this question as a hypothetical about their competence rather than lying about being attacked. Another question in the survey supports the previous statement. One of the questions was, "I believe I know how to protect private data or information.". To this, 74% of the participants answered "Yes." Which implies that the surplus in answers was probably thanks to people answering in a hypothetical manner.

Professionals' perspectives

Recalling the information about how age factors into cyber security and that most participants are in their Middle Ages, what was said by the specialist promotes the idea proposed. Individuals in their twenties all the way up to forties are more likely to know how to operate with a computer. Specialist C aids this by reminding everyone that this generation grew up with technology and thus is closer to it than older generations.

Figure 4 - Cyber-attack experiences



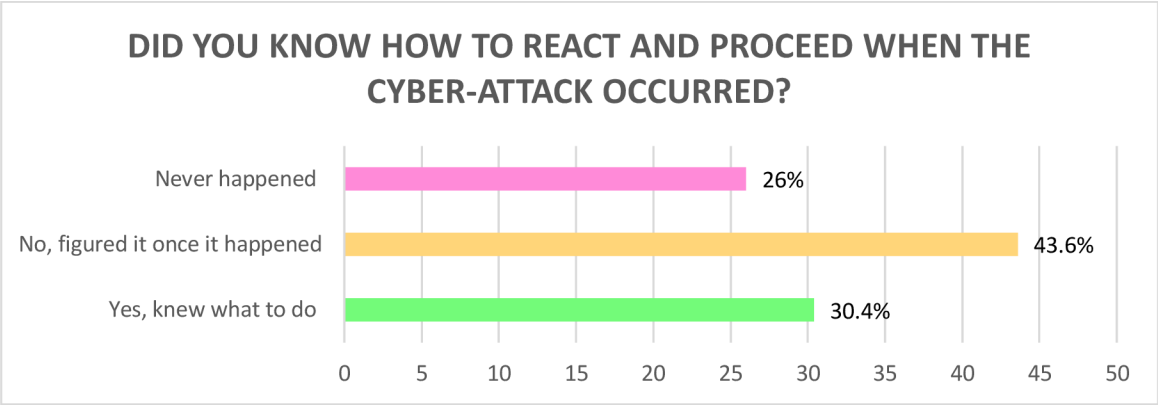
It was also of interest to inquire what they lost thanks to being cyber-attacked and if that changed the way they approach their security. Even though a small number of participants were attacked themselves, many answered the questions about higher vigilance around their computers. Most said that after an attack occurred to someone around them that they started to pay closer attention to what they were clicking on and whom they let have access to their private information or even just use their computer. Others spoke of their experiences, which ranged from something as minuscule as losing 27 followers on Instagram all the way to identify theft.

Professionals' perspectives

This is also something that specialist C mentioned during their interview. They said a person either explains to an individual all the things they could lose, or they lose all their things and then they understand the hard way.

When going through all the replies of the participants, a pattern emerges. Statements such as 'I became more cautious' came up countless times, as well as 'started using double authentication' and 'I made password changes.' After experiencing a cyber-attack or even just a mere scare of one, people seem to recognize how big the problem is. Most then start to seek out the help of different apps and firms to help with the protection of their computers.

Figure 5 - How to React and Proceed



Computer Protection

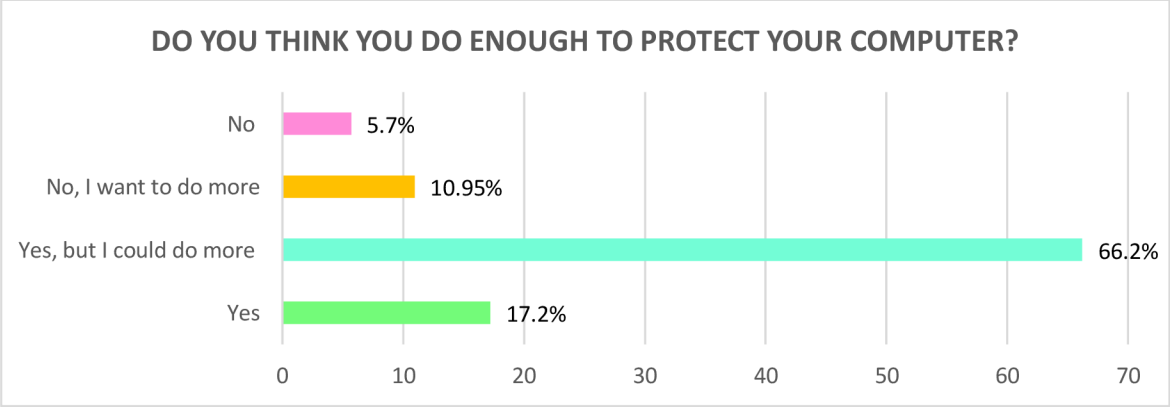
Do they feel they do enough?

The responses say yes. When looking at the results, 66% believe they do enough but could do more, 17% say they do enough, 11% are aware they do not do enough but would like to do more, and 8% believe they do not do enough; nonetheless, they have no intention of changing that in present time. This showcases the approach people must cyber security. Most settle for the bare minimum and trust that they aren't interesting enough for a hacker to actually attack them, or they don't believe they have anything of value to a hacker.

Professionals' perspectives

This is something that frustrated each specialist. They each mentioned how this is something they come in contact every day and they cannot stress enough how much more vigilant people need to be.

Figure 6- Computer Protection



Is ones operating system enough?

One of the questions in relation to computer protection was, "Do you rely on your operating system to provide you protection against cyber-attacks?". For this, responses were mixed, and a series of patterns emerged. At the very beginning of the practical part, it was mentioned that this survey was conducted in two languages, and that is where one of the patterns lies. Participants that filled out the English version of the survey were, on average, between twenty-one to thirty years of age. The reason this is mentioned is that 75% of them replied saying they rely on their operating system for protection. This may seem like an unimportant factor, however when compared to the Czech survey the reason this is important is illuminated.

In the Czech version, 52% percent of the participants are of the same age as in the English version, and the rest are almost evenly distributed between thirty-one to sixty years of age. Their percentage was considerably lower; only 46% relayed on their operating system for support. What this shows is that with age, perspective changes, and experience grows. Additionally, to this, the reason why it is pointed out is their replies to why they do or do not rely solely on their operating system for protection. Most younger participants do not seek additional protection because they either A) find it too expensive or B) believe their operating system is all they need. Many do use some sort of ad-block, or they stay vigilant while using their computers. Another reason the difference between the two languages is important is that, based on replies, participants within Czech are more knowledgeable and vigilant when it comes to cyber security. When looking into those that rely only on their operating system, the main reason they do so is that they find additional protection to be difficult or confusing to understand and use. The former proclamation brings about the last pattern. A predominant number of computer users do not understand today's cyber protection services. They find them complex, and with a growth in providers of these services, they find it difficult to know which to choose. In correlation to this, participants do not know which provides trust or what services they should be even looking for to protect their computers.

What protection services are on a user's computer?

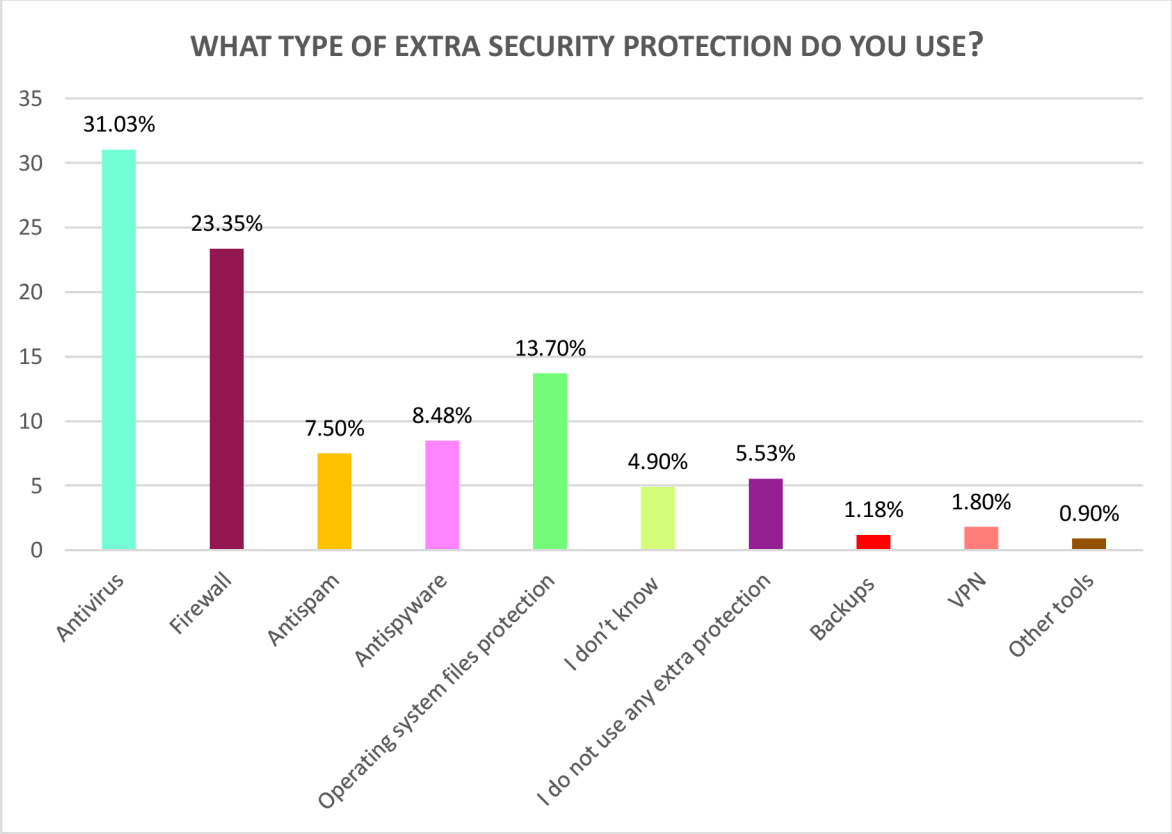
Despite numerous people utilizing only their operating system, it was vital to learn what protection services participants possess for this thesis. To define what the best measures are and if they are being utilized correctly, it was necessary to gain this information. It will help to better understand how everyday computer users operate and how much they

understand. On top of the results list, with 31%, there are antivirus programs, next at 23% firewalls, 13% use their operating system, and the last larger number is antispyware with 8%. The rest of the percentage is divided among antispam, participants not knowing or not using extra protection, backups, VPNs, encryption, ad-block, or a computer cleaning software. Each of the above mentioned are put in numerical order based on the percentage they acquired in the survey, ranking from highest to lowest.

Professionals' perspectives

When asking specialist what they used within their firms they replied by saying they used everything. Later this was elaborated, and the first practices mentioned were antivirus, firewall, VPN, and user education.

Figure 7 - Extra Security Protection



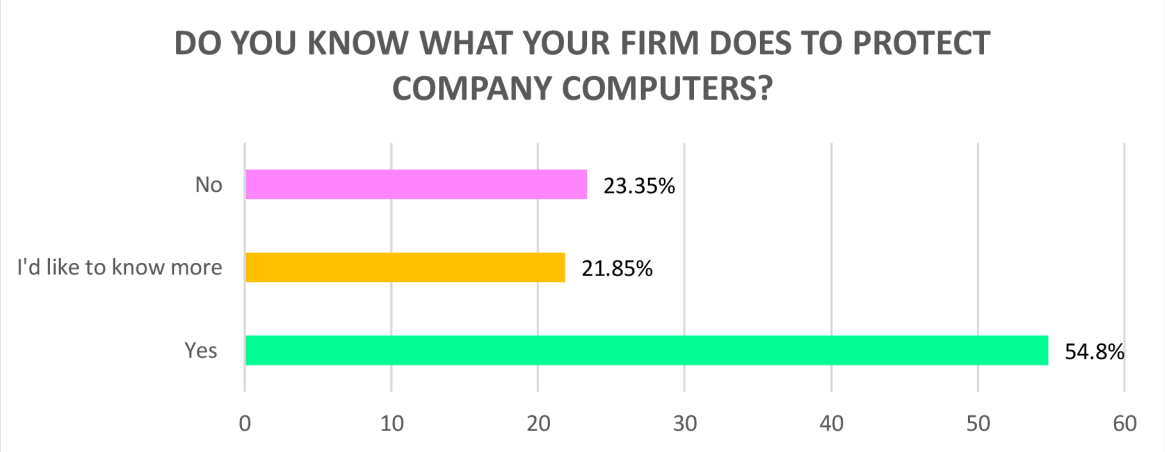
Then, participants who explicitly use company computers were questioned if they were aware of the cyber security measures in place at their workplaces. Out of eighty-eight, 55% knew what their companies employ, and the remaining 22% and 23% either wanted to be further informed on the matter or had no knowledge of what the company made use of.

This demonstrates how much employees know and are taught. Looking at the graph, it visually is impactful however, when focusing on the numbers, they are just slightly above half, which is promising yet not at the levels that would be optimal to prevent as many cyber-attacks as possible.

Professionals' perspectives

The same applies in practice, specialists say that educating their users is never ending, even so there are always several individuals that either doesn't care to know or just don't understand. They also mentioned that there are many firms that don't provide cyber security seminars or overviews for their users, and they advised each firm to start doing so.

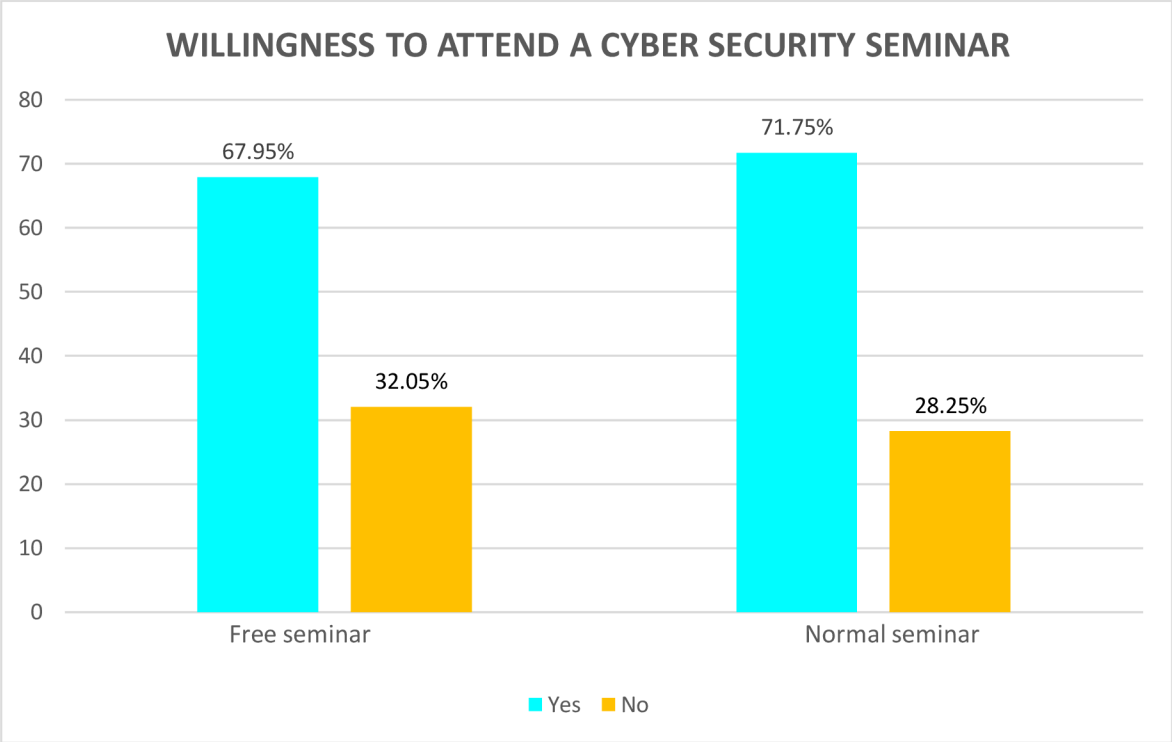
Figure 8 - Company Computer Protection



Cyber Security Education

Company and personal computer users were inquired about if they had ever been educated on cyber security, and 70% answered yes. When asked if they would take a cyber security class or seminar to learn more on the subject, 72% said yes that they would be interested in doing so. Then when asked if they would take one if offered for free, an increase in numbers was expected; however, the opposite happened. The numbers went down 4%, leaving the total number of participants willing to go to a free cyber security seminar at 68%. After giving this phenomenon, some thought thanks to the similarity in sentence build, some people may have just skipped over the question thinking it was a duplicate. Nonetheless, this is still a good amount of people interested in learning more about the ways they can protect themselves digitally.

Figure 9 - Cyber Security Seminar

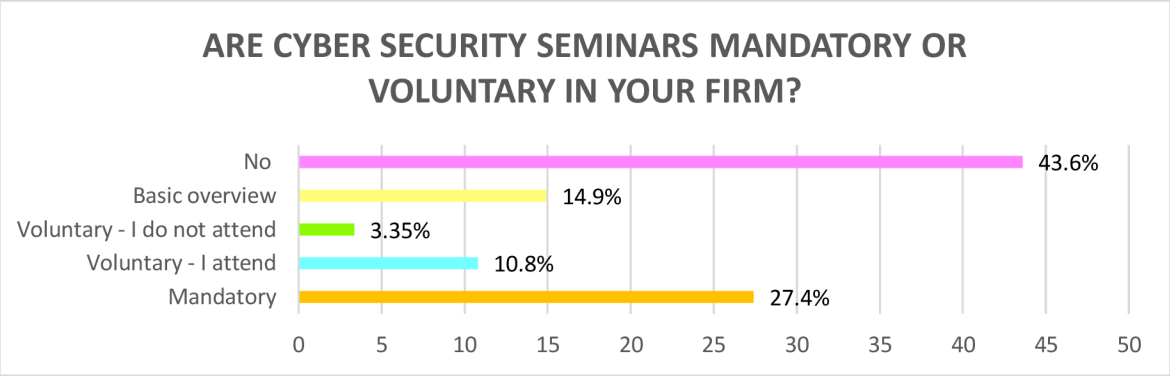


Focusing on company computers, it was further surveyed how well-educated participants are. Firstly, they were queried if their companies provided cyber security seminars. Out of seventy-four company users, only 45% said their companies provide a class. Secondly, they were asked if those that were provided this option had it as a mandatory part of their job or if it was voluntary. Only 27% had mandatory seminars. A basic overview of cyber security was provided to 15%, and 11% had voluntary seminars and chose to go. The remaining percent either didn't have the option or chose not to attend these seminars. This, in a sense, showcases the importance firms put on cyber security.

Professionals' perspectives

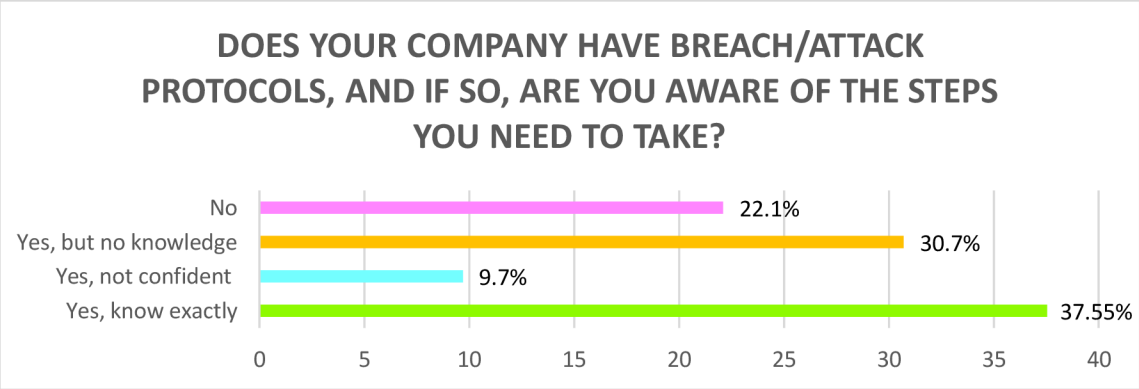
If the firm itself doesn't put emphasis on its security, why would its employees feel it to be important? As mentioned before by the specialists it is of highest importance to inform users what the dangers are. Users need to know what to look out for and firms need to be more proactive.

Figure 10 - Cyber Security Seminars Attendance



Additionally, participants were questioned, "Does your company have breach/attack protocols, and if so, are you aware of the steps you need to take?". Eighty-three participants responded to this, 38% know exactly what to do, 31% know of the existence of protocols but do not know them, 22% claim their firm has no such thing, and 9% answered that their company has them, but they are not confident in using them. Overall, 78% know what to do; however, when taken apart, the amount of people that know what to do is concerningly low.

Figure 11 - Breach/Attack Protocols



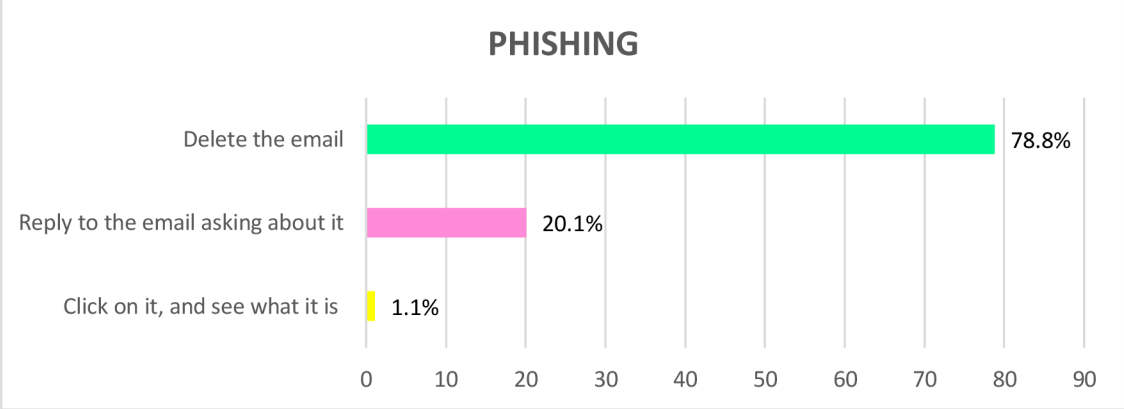
Knowledge

At the end of the survey, each participant was asked to answer a set of four reaction-based questions. This was to see if people knew how to identify basic, non-complex cyber-attack attempts. The reason basic attacks were chosen as reaction questions is simply that a more complex and sophisticated hacking attempt would be specifically crafted to an individual, firm, or clientele. The results of these, as expected, were very positive.

The first question was, "You get an email from your friend out of the blue, and the subject line is 'YOU GOTTA SEE THIS.' When you open the email, it contains a link or file with no message in the body. What would you do?".

To this, 79% answered that they would delete the email, 20% would reply to the email asking about it, and 1% would click on the link. Although the number of people who answered that they would delete the email was dominant in this sample size, that is still approximately 24 at risk of being attacked or becoming the cause of a security breach. In this scenario, the primarily chosen incorrect answer is not all that bad, considering replying to the email won't cause an attack itself; however, the probability that the hacker will reply instead of the friend is high.

Figure 12 - Phishing



The second question asked was, "While at work, someone or a colleague walks up to you and hands you a USB saying that a 'known associate' or 'higher up' is sending you this USB. They say it contains information you need to review. How do you react?".

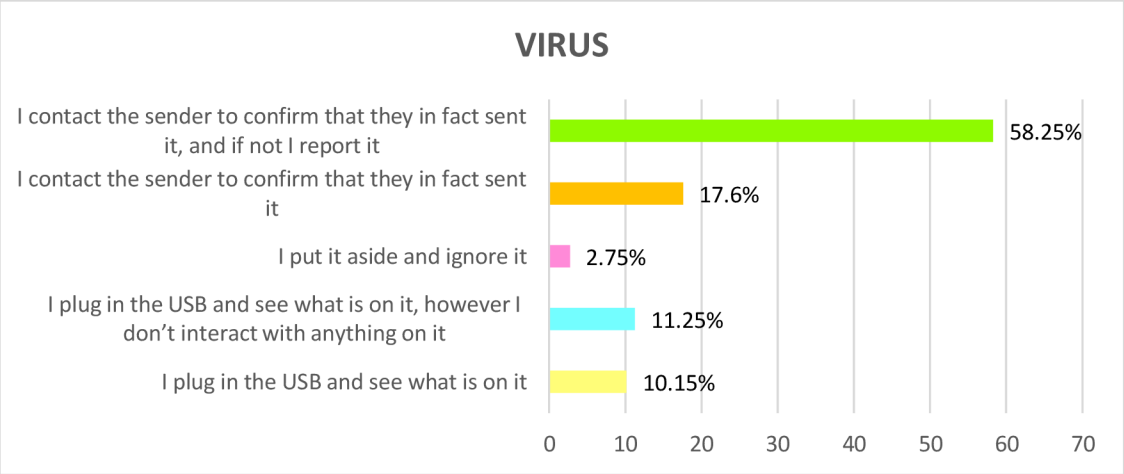
Here 58% replied, "I contact the sender to confirm that they, in fact, sent it, and if not, I report it," 18% just confirm with our sender, 11% answered, "I plug in the USB and see what is on it; however, I don't interact with anything on it," 10% plug-in said USB and interact with it; lastly 3% puts it aside and just ignores it. When putting together this question, it was vital to give similar answers but ultimately only have one correct answer. It may seem confusing or misleading; however, that, in a sense, is how cyber security works. There are many things one could do, and they aren't necessarily always good or bad; sometimes, just one little difference changes everything. When it comes to the USB, reporting it was vital and not reporting opens the doors to it potentially happening again to another victim.

Ignoring the situation is wrong whether it would truly be from an employer or not. As for plugging it in, the moment one does so, they let whatever is on the USB into their computer.

Professionals' perspectives

When breaching this subject with specialists they say one small detail makes a big change.

Figure 13 - Virus



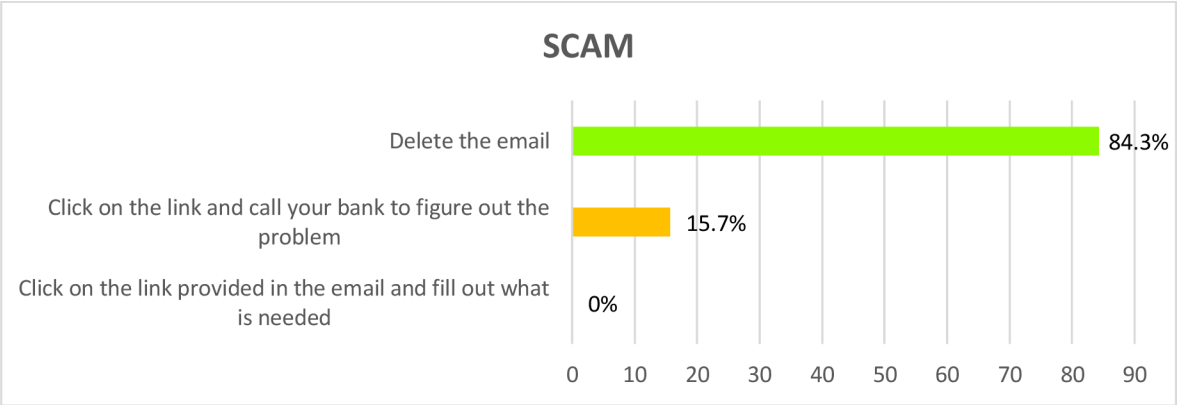
Thirdly inquired, "You get an email from your bank provider informing you that your account is suspended pending confirmation of your personal information. The logo for your bank is in the body of the email, and the email is addressed "Dear Customer." The sender of the email is service@'nameofyourbank'customerserviceteam.com. What do you do?".

The most frequent answer was that they would delete the email, with 84% choosing this. However, 16% chose to click on the link and then call their bank to try and resolve the issues. Here most people are more aware of what to do and are much more vigilant, thus the high numbers in correctness. This is a more common attack, and many people know exactly what to do because they learned what to look out for.

Professionals' perspectives

Specialists A, C, D refer their own firms and how they run regular in firm fake email tests to keep their employees vigilant to these types of attacks.

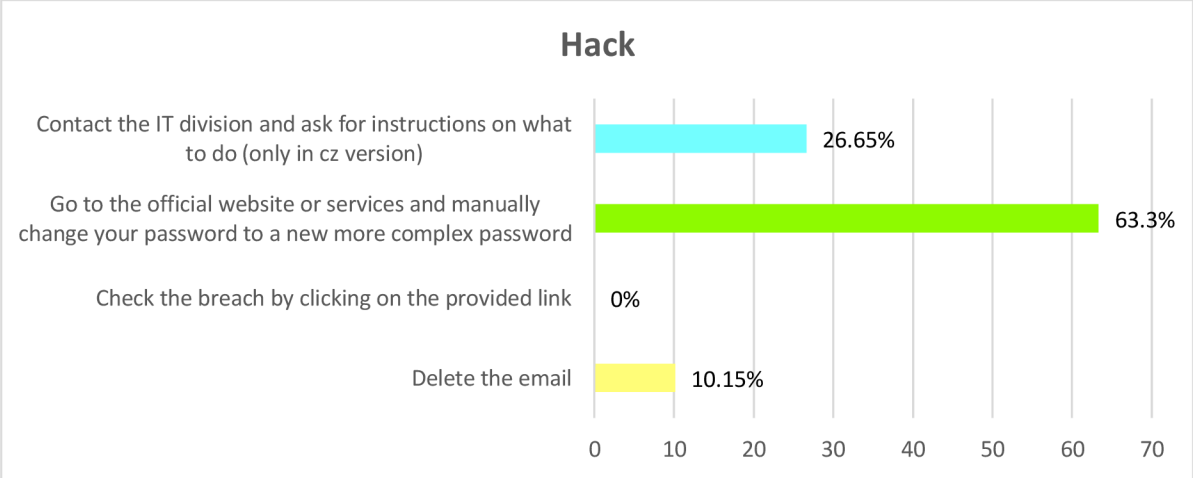
Figure 14 - Scam



The fourth and final question was, "You get an official email from your administrator informing you that one of your passwords has been compromised. What do you do?".

For this question, there was a small edit in the Czech survey. The Czech version had an extra option to reply available. This being “Contact the IT division and ask for instructions on what to do (only in the Czech version)," 53% of the Czech participants chose this option, 34% chose "Go to the official website or services and manually change your password to a new more complex password.” The last option presented was also chosen by most of the English participants. When combined, a total of 63% chose the option where they change their password. Lastly, the remaining option of deleting the email was chosen by 10% of participants from a combination of both surveys. The added answer in the Czech survey didn't change anything in the end; both answers that had the higher score were correct. When it comes to passwords, people also have learned to be more vigilant, and it is reflected in the answers.

Figure 15 - Hack



5.2 Interviews

Each interview question was thought through and taken into consideration based on the survey presented to the public. It was vital that the interview questions and survey correlated. Even though both the survey and interview had to in some way be intertwined, the interviews were more in-depth than the survey. Each interview had a set of the same questions that differentiated in follow-up questions based on the interviewees' answers. The discussions lasted an hour each and were recorded with the interviewee's knowledge. These recorders were later transcribed.

For a better understanding and protection of my sources, each interviewee obtained a letter under which they will be referred, and when addressed as a whole, the term specialist will be used. Altogether, there were 5 participants, so letters range from A to E. Each of these people work in the IT sector and are in one way or another connected to cyber security. That may be directly or indirectly. By indirectly, it is meant that they are in day-to-day contact with cyber security but may not be directly in their firm's cyber security team itself. Every interviewee has been with their firm for at least one year and has been in some way connected to cyber security from a younger age or worked in a different IT firm before the one they are currently a part of now. The companies they are a part of are on larger scales and, based on their clearance, were able to give me information. Nonetheless, each interviewee answered all the questions asked one way or another. Job positions range from CEO to IT support. This was done because each department and position approaches cyber security slightly differently. Each agrees on its importance, but each meets it differently, providing us with different viewpoints. Different viewpoints should help figure out what society or, rather, the public can do to better their cyber security. For a better overview, the main questions that brought the most insight will be highlighted and discussed. Each question will have its own section, and the answers of the interviewees will be evaluated.

Before going over what each interviewee said, the thought process behind the chosen questions will be presented. Before getting into some of the more complex questions, it was thought it would be best to define what it is we are trying to stop; to fight something, one must know what to fight.

What Is Hacking?

When asked this question, four out of five responded in a similar sense. It is the act of entering a space one is not supposed to be in. What is meant by this is that a person uses a certain skill set to walk through the holes of a system. A good way to interpret this is to imagine you have a set of keys specific to the doors in your firm. A hacker comes with a giant set of almost random keys and keeps trying different keys until he finds the correct one and then proceeds to open every door they need to get to their goal. Specialists A, B, C, and D support this statement, someone getting information or into places they are not supposed to be. However, specialist E brings a different point of view. They say it is having a unique talent to find shortcuts. Hacking itself isn't bad; someone just knows something so well that they can see ways to make things easier for themselves. If what E says applies, then it is all in the hands of motivation.

What Is The Cause Of Cyber-Attacks?

Three specialists, C, D, and E, all mentioned specifically money or some financial gain. While the other two also spoke of money, they also spoke of incentives. Specialist B used an example from a video game environment where they spoke of people, mainly younger kids, hacking the game itself to become a top player in a specific game. An example of an incentive that isn't financially motivated. Something both C and A mentioned is that hackers are curious; they like figuring things out like a puzzle.

When talking to A, they elaborated more on the curiosity aspect and the motivation itself. They mention that a proper hacker on his or her own is harmless, so to say. Their drive is to learn and see what all they can do; they don't actually aim to gain something. They just want to keep pushing their limits. The motivation problem occurs when a hacker intercepts a more social human or someone with a sinister motive. At that point in time, a hacker becomes a weapon. It's when they are working for a commission with a set goal that they no longer have any breaks and start to cause harm.

After discussing the causes and what makes a hacker hack, it is only natural to talk about what weapons they utilize. Which attacks are the most dangerous to users? Big attacks that put companies out of service for days or is it rather your standard scammer that is truly the evil mastermind.

What Is The Biggest Threat In Cyber Security?

Here everyone had a different answer. Starting off from the top, A said the human factor is dangerous because it is unpredictable. There is always negligence, whether that be to the actual security protocols or just disregarding the need for better security within a firm. They also said that the most dangerous are specific attacks. Ones that are aimed and fueled with motivation. Moving on to B, they think that DDOS attacks are the most dangerous.

C said identity theft and encryption because using these, a hacker could and most likely will blackmail you or, in the former case, become you and take everything you have. Money-wise, that is. Specialist D had a similar answer; they spoke of private information being stolen. They mentioned how it is something that can happen on a personal level as well as in a firm. This can then be turned into profit for the hacker who obtained this data. Finally, E, E is saying one's ignorance of the operating system or configuring it is what causes problems. To elaborate on that, it is attacks where these are used to benefit a hacker that the true danger arises.

The next question that was asked seems unavoidable. During these talks, each specialist is speaking of what they have encountered and how they view the cyber world. Since they are the ones living in it daily, they would seem to have more knowledge on the subjects than everyday people. They see how it all goes down and what causes these attacks to happen.

What Causes The Most Breaches In Cyber Security?

Everyone's answers differentiated, but each had the mention of some sort of human factor. Either gaining access to a user's login, users themselves, or just someone falling victim to a phishing attempt. Specialist C adds to this by saying that most times, it can also be accompanied by a lax security system which makes gaining access to everything much simpler. Specialist A contributes to this, they tell us that yes, the human factor is a big cause of breaches however a hacker will achieve their goal no matter what if they want it enough. The user is an easy access route. This is supported by D and C, who mention users clicking on suspicious links or files that are ultimately phishing attacks.

It has been established that users are a big part of cyber security. They play a big role when it comes to technology since they are the ones using it every day. Technology itself,

software's, programs, and defenses run on their own. Code tells them what to do, and they do it. That's where humans factor in, they don't follow a code.

How Do Humans' Factor Into Cyber Security?

A statement from E commences this discussion best. They said, "It directly contributes. It is because of the human factor that IT attacks happen.". Specialist D goes on to say that humans influence cyber security daily in both positive and negative ways. Positively they are working through VPNs, proceeding to use all the right protocols; however, cyber security is not foolproof. An individual can connect to an unprotected public network or happen to fall for a scam and all security goes down the drain. When talking to B, they mention that one must use their head while on a computer, that the systems themselves could be working, but if an individual doesn't think while working, they can be the cause of a leak. A agrees with this, stating, "it is always easier to use technology than using people during any changes in systems," and C says that they have a rule within their company "if you have even the slightest suspicion contact us, and we will evaluate it.". Humans change the way security is approached.

Since all our specialists work with larger amounts of people, the thought that maybe age plays a role in cyber security came about. What a younger person finds logical, an older may not, and vice versa.

Does Age Play A Role In Cyber Security?

Upon hearing this question, A instantaneously starts to ponder and says, "Age is a very philosophical question.". Similarly, so B, C, D, and E react by stopping to think for a few beats. Then each proceeded to reply. E states that the older generation tends to avoid learning about the safeties of the internet and gives a few reasons why. One of the reasons was the fear of it being too complex to understand, or it could be as simple as just deeming it unnecessary. The others go on to say that at certain stages in our lives, we view things differently. The younger and older we are, the more naïve or trusting we can be, says B and C. Specialist C goes on to even say that it isn't age itself but rather the character of the person that changes their approach to cyber security. The more a person trusts, the more likely they are to fall victim to an attack. As for D, he explains how the generation between ages fifteen to forty are more likely to be vigilant thanks to being around technology much more than the

older and younger generation. Age reflects how we see the world, which includes the cyber world and its security.

Humans themselves play a role, as well as their age, which brings about the next question.

How Can Cyber Security Be Improved?

A says, "People should educate themselves more.". B says, "Talk about it more, hold trainings, and spread this information further and further and further.". C says, "Start teaching people in school so they know the basics from the moment they touch a computer.". D says, "An increase in general knowledge around cyber security.". E says, "Attractive quizzes and courses for different generations. Education and awareness of issues.".

In the previous case, the specialist spoke for themselves, and nothing needed to be added. Human error can't be avoided, but it can be minimized, and the risks are lowered by using different security measures.

Which Practices Are Best In Cyber Security?

One would assume a list would be presented, but be that as it may, nothing is ever black and white. When it comes to computers, nothing is as simple as installing and letting the program do its thing. Once the app is installed, one needs to know how to navigate it. Each specialist agrees that it starts with one's operating system. The very first interviewee, A, showcases this by giving an in-depth rundown of what all goes into protecting oneself online, "First, you need a personal firewall (where you input what you allow to happen to your computer) just because you are in front of your computer and using the keyboard does not mean that someone else isn't connected to your computer. Antivirus and Antispam. Antivirus alone isn't enough it depends on what the firm offers and a vaccine (how often are virus samples updated). The same applies to antispam; it should be used on your side as well as your email provider's side. Most people don't even know that their providers are using antispam, which brings us to the problem that there is not enough correspondence between the providers and their clients. There should also be a type of antivirus that will be capable of uncovering malware, spyware, etc.". This is then repeated by each specialist, just in fewer words. Specialists C and D one should have a mixture of all of them in some way. Specialist E reminds everyone that regular updates and password changes are exceptionally important

as well. Most importantly, however, a person needs to know what they are putting and or have on their computer.

That cyber security can be complex, and understanding the ins and outs may be confusing. To really put things in perspective and try to find the root of the problem, one last question was asked.

What Is One Thing You Wish Everyone Using An Electronic Device Would Know Or Abide To?

The answers received were what one would expect by the end of these interviews. Yet no one failed to surprise with their clever ways of wording things. Specialists B and D said they wish people would learn more about the topic and be cautious with what they are doing. Specialist E told us not to be afraid of our devices and to continuously educate oneself. Specialist C answered with a saying, "Don't trust but verify," to which they added you never know who the person on the other side of the computer is; they could be a dog. Lastly, specialist A stated that cyber security should be a little bit like AIDs. Everyone has a general overview of the disease and knows what to do to avoid it as best they can; the same should go for cyber security.

The interviews, as mentioned before, all lasted much longer, and many more things were covered, but it was felt these were the main questions and points that should be illuminated from the rest. Each specialist had a slightly different take on things as well as some things that overlapped or were identical. Every conversation was eye-opening and defiantly gave a deeper view into the systematics and practices behind cyber security.

5.3 Discussion

One of the first big comparisons that can be made between the survey and interviews is the usage of operating systems. Specialist A notes that they are frequently asked whether one's operating system is enough to protect them. In the survey, it is found that multiple people do rely only on their operating systems for protection. The specialists agree that it starts with one's operating system, but one must add to it and grow their protection base. On the contrary, two of the specialists also mentioned that if an individual is using MS Windows, that operating system has a built-in program named defender that works almost just as well as any downloaded cyber security program. However, it has a drawback. One must know how to set it up so that an individual's computer is properly protected. In the literature review it is noted that when an attacker wants to they find a hole in the program and use it against the user (Mitnick, Simon 2002). Meaning that if the end user is aware of how to set up their operating systems built in defense properly an attacker can swiftly penetrate the set up security measures and exploit them. However many users lack awareness creating our drawback (Zhang-Kennedy, Chiasson 2022).

Throughout this thesis, many different security measures were discussed. In the literature review the most common measures were analyzed and a brief overview was provided. It was said that two factor authentication is growing in popularity and antiviruses are a part of a basic computer cyber security set up. Another note presented in the literature review was that firewalls are a basic protection staple as well and are usually set up on a user’s computer. Participants of the survey were asked which practices they used that they thought to be the most effective. During the interviews, the specialists were asked the same. When it came to the public, most answered the standard. The top three employed security defenses were ones OS as discussed above, antiviruses, and a firewall. When looking over the numbers themselves, the number of people that didn't use any protection or were not aware if they had any was slightly concerning. Yes, the majority used some sort of protection but when compared the numbers are jarring. Ten percent have no awareness or don't use any security for their computer; thirty use an antivirus, twenty have a firewall, and thirteen percent use their OS. These numbers are not high. When asked in the survey why they might not utilize some form of protection, a number of people answered, saying they don't understand the systems. Even individuals who had some type of protection set up wrote of their confusion with the programs.

As stated in the research, cyber security has always been a specialized area and for the most part only people within the community understand how everything works. This is than further supported by the literature review where it is said that many firms employ companies to run security for them. Each and every user is aware of threats that exist yet when it comes to the daily lives of users who are non-experts they get easily lost in all the complex measures for the defense of their devices (Zhang-Kennedy, Chiasson 2022). Naturally, this question was then brought to the specialists. When asking the specialists what they found to be the best measure, the majority said to have a mix of everything. That would be a lot of programs, and most of the survey takers are already lost in what they have now. One solution mentioned by specialist C was to go online and look at verified bundles one can download and not have to think about too much. They went on to mention some security firms that are found to be the best, for example, ESET. Another thing they found curtail was having knowledge on the subject. That is one thing that was lacking among the participants.

Everyone from the IT sector kept mentioning the importance of knowledge and awareness, even throughout the research itself, it was mentioned many times in books and scholarly articles. Erickson spoke about it in his books where he elaborated by sharing countless situations where knowledge was power. When looking into hackers such as Mitnick he himself said that it was always about knowing more than the target. Yet no one is explaining the importance or putting urgency to learning how to protect oneself. When observing the graphs once more, one can see that several companies don't provide any type of cyber security, and when they do, it is not a mandatory thing one must attend. The researcher isn't part of a big corporation, so it is considered that many do not see the importance in certain sectors for this type of security. Nonetheless, the specialists disagree. Not because it is important for their job but because they see the impact an attack can make.

Taking online forums as an example, in today's age, it is exceptionally common to get a message from a friend or family member saying they found a super shocking video of the recipient and they should check it out. The public is surrounded by cyber-attacks, and instead of bringing awareness to the importance of how to protect oneself, it has been normalized. As was hinted at or directly discussed in each interview, the danger is growing at lightning rates, and the number of attacks is doubling. Most of the attacks mentioned are thanks to lack of knowledge and awareness. If we circle back to our review of cyber security awareness

one of the papers reviewed and cited discussed how in today's age there is a knowledge gap in cybersecurity among non-expert end-users, and improving their knowledge and awareness is crucial for effective cybersecurity (Khando et al. 2021).

How does the public or society rather bridge this gap? The survey portrays that the situation is not as dire as was expected. The specialists gave real-time situations and examples of scenarios proving that the situation is damaging. The participants showed that they are willing and want to learn. The specialists want people to be educated. A solution arises for future evaluation, find a way to make this knowledge easy and fun to learn. Specialist E says this as a way to help bridge the gap and with the knowledge collected through this study the potential exists. It was simple to see where individuals were lacking and they themselves expressed what they found difficult to comprehend. If we take that information and merge it with starting to raise awareness on this subject in grade school, future attacks can be avoided in potentially large numbers. As was previously mentioned one author already touched this subject and they spoke of the impact multimedia platforms had when educating users about cyber security awareness. The author broke down the phenomenon into three key aspects. Adaptability, Usability and Learning. The knowledge has to be adaptable since it is an ever changing field. Next it needs to be easy to use and reusable. Lastly it needs to be an active learning process where tools and people collaborate to help eliminate as many threats as possible (Zwilling et al. 2022).

6 Conclusion

In conclusion, this thesis has embarked on a comprehensive exploration of the level of awareness users have and various cybersecurity measures, seeking to determine their effectiveness in safeguarding computers, data, and systems against threats. The research has shed light on the strategy that holds the greatest promise for protecting individuals and organizations from cyber threats.

The literature review entailed an exhaustive examination of numerous scientific research papers, articles, and books authored by cybersecurity specialists and former hackers. The resulting clear and comprehensive research question provided a solid foundation for understanding the complexities of cybersecurity awareness in everyday users. Posing questions through semi-structured interviews in the practical portion of the research

has deepened the understanding of user behavior and the ways in which security measures and awareness can be refined to enhance protection. It has uncovered valuable insights into the cyber hygiene practices of individuals, revealing both strengths and areas for improvement. By understanding what measures users actively employ to protect their desktops and laptops, as well as the extent of their awarness, future researchers are better equipped to evaluate the efficacy of these approaches. This thesis has concluded that the metophhorical key to increasing cybersecurity awareness and online safety is allowing users to more freely access the knowledge necessary to improve their digital literacy. Users have been found to be severely underinformed when it comes to issues of their online privacy and security, meanwhile, the steps to take in order to avoid such mistakes are quite simple, and most safety risks are easily avoidable for experienced users. The base of knowledge necessary in order to allow for informed online decision-making is not as extensive as many may believe, making this issue one that can be drastically minimized through minor systematic changes to education.

Moreover, this research has not been limited to the perspective of end-users alone. Investigated also were the practices and strategies employed by experts in the cybersecurity field. Their insights have offered a unique perspective, potentially unveiling undisclosed algorithms or techniques that may not be readily accessible to the general public. These expert perspectives may hold the key to more robust cybersecurity practices that can benefit individuals and organizations alike.

In summary, the research findings have provided a detailed understanding of the state of cyber security awareness within the sampled population, offering valuable insights into their knowledge and behavioral patterns. Furthermore, the research has successfully identified the cybersecurity measures most frequently adopted by everyday computer users, while underscoring the critical need for a mixed approach to cybersecurity which combines technological advancements with user education and expert insights. This research contributes significantly to the existing body of knowledge on cybersecurity, emphasizing the importance of addressing the divide between theoretical knowledge and practical implementation in this domain. Such insights are essential for equipping individuals and organizations with the necessary tools to navigate an increasingly digital world while safeguarding their digital assets and information.

References

ALDAWOOD, Hussain and SKINNER, Geoffrey, 2019. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet*. Vol. 11, no. 3, p. 73. DOI 10.3390/fi11030073.

ALGHAMDIE, Mohammed.I., 2021. A novel study of preventing the cyber security threats. *Materials Today: Proceedings*. p. S2214785321029345. DOI 10.1016/j.matpr.2021.04.078.

ALHAYANI, Bilal et al., 2021. Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. *Materials Today: Proceedings*. p. S2214785321016722. DOI 10.1016/j.matpr.2021.02.531.

ALKATHEIRI, Mohammed Saeed, CHAUHDARY, Sajjad Hussain and ALQARNI, Mohammed A., 2021. Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications. *Sustainable Energy Technologies and Assessments*. Vol. 45, p. 101219. DOI 10.1016/j.seta.2021.101219.

AL-SHARIF, S. et al., 2016. White-Hat Hacking Framework for Promoting Security Awareness. In : *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–6. Larnaca, Cyprus : IEEE. November 2016. ISBN 978-1-5090-2914-3. DOI 10.1109/NTMS.2016.7792489.

AMAN, Muhammad Naveed, BASHEER, Mohamed Haroon and SIKDAR, Biplab, 2019. Two-Factor Authentication for IoT With Location Information. *IEEE Internet of Things Journal*. Vol. 6, no. 2, pp. 3335–3351. DOI 10.1109/JIOT.2018.2882610.

ANWAR, Raja Waseem, ABDULLAH, Tariq and PASTORE, Flavio, 2021. Firewall Best Practices for Securing Smart Healthcare Environment: A Review. *Applied Sciences*. Vol. 11, no. 19, p. 9183. DOI 10.3390/app11199183.

CHOW, Sherman S.M. et al., 2005. A generic anti-spyware solution by access control list at kernel level. *Journal of Systems and Software*. Vol. 75, no. 1–2, pp. 227–234. DOI 10.1016/j.jss.2004.05.027.

DHILLON, Gurpreet et al. (eds.), 2019. *ICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings*. Cham : Springer International Publishing. IFIP Advances in Information and Communication Technology. ISBN 978-3-030-22311-3.

ERICKSON, Jon, 2008. Hacking: The Art of Exploitation, 2nd Edition. *No Starch Press*. Vol. 2, p. 492.

EVANS, Mark, HE, Ying, MAGLARAS, Leandros, YEVSEYEVA, Iryna, et al., 2019. Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. *International Journal of Medical Informatics*. Vol. 127, pp. 109–119. DOI 10.1016/j.ijmedinf.2019.04.019.

EVANS, Mark, HE, Ying, MAGLARAS, Leandros and JANICKE, Helge, 2019. HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security*. Vol. 80, pp. 74–89. DOI 10.1016/j.cose.2018.09.002.

G. A., Marin, 2005. Network security basics. *IEEE Security & Privacy*. Vol. 3, no. 6, pp. 68–72. DOI 10.1109/MSP.2005.153.

GENÇ, Ziya Alper, LENZINI, Gabriele and SGANDURRA, Daniele, 2021. Cut-and-Mouse and Ghost Control: Exploiting Antivirus Software with Synthesized Inputs. *Digital Threats: Research and Practice*. Vol. 2, no. 1, pp. 1–23. DOI 10.1145/3431286.

GIRI, Shailendra and SHAKYA, Subarna, 2019. E-government Use in Nepal: Issues of Database Management and Data Security. *Journal of the Institute of Engineering*. Vol. 15, no. 2, pp. 218–224. DOI 10.3126/jie.v15i2.27669.

GRIMES, Roger A., 2017. *Hacking the Hacker: Learn from the Experts Who Take Down Hackers*. Indianapolis, Indiana : John Wiley & Sons, Inc. ISBN 978-1-119-39626-0.

GUNKEL, David J., 2001. *HACKING CYBERSPACE*. Northern Illinois University : Westview Press. ISBN 0-8133-3669-4.

ISO, 2019. *ISO in brief* [online]. International Organization for Standardization. Retrieved from : https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100007.pdf

ISO, 2022. *Standards and innovation What does the research say ?* [online]. International Organization for Standardization. Retrieved from : https://www.iso.org/publication/PUB100466.html

ISO, 2023. *ISO Strategy 2030* [online]. International Organization for Standardization. Retrieved from : https://www.iso.org/publication/PUB100364.html

JEYARAJ, Anand and ZADEH, Amir H., 2022. Exploration and Exploitation in Organizational Cybersecurity. *Journal of Computer Information Systems*. Vol. 62, no. 4, pp. 680–693. DOI 10.1080/08874417.2021.1902424.

KASHYAP, Ramgopal, 2019. Chapter 2 - Big Data Analytics Challenges and Solutions. In : *Big Data Analytics for Intelligent Healthcare Management*, pp. 19–41 [online]. Elsevier. ISBN 978-0-12-818146-1. Retrieved from : https://doi.org/10.1016/C2018-0-01336-5

KATSANTONIS, Menelaos N., MAVRIDIS, Ioannis and GRITZALIS, Dimitris, 2021. Design and Evaluation of COFELET-based Approaches for Cyber Security Learning and Training. *Computers & Security*. Vol. 105, p. 102263. DOI 10.1016/j.cose.2021.102263.

KÄVRESTAD, Joakim et al., 2020. Constructing secure and memorable passwords. *Information & Computer Security*. Vol. 28, no. 5, pp. 701–717. DOI 10.1108/ICS-07-2019-0077.

KHANDO, Khando et al., 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*. Vol. 106, p. 102267. DOI 10.1016/j.cose.2021.102267.

KRISHNASAMY, Vidhyanandhini and VENKATACHALAM, Saravanarajan, 2021. An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryption algorithm. *Materials Today: Proceedings*. p. S2214785321032235. DOI 10.1016/j.matpr.2021.04.303.

KUMAR, Dr Sunil and AGARWAL, Dilip, 2018. Hacking Attacks, Methods, Techniques And Their Protection Measures. . Vol. 4, no. 4, p. 6.

LEE, Younghwa and KOZAR, Kenneth A., 2008. An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management*. Vol. 45, no. 2, pp. 109–119. DOI 10.1016/j.im.2008.01.002.

LI, Yuchong and LIU, Qinghui, 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. Vol. 7, pp. 8176–8186. DOI 10.1016/j.egyr.2021.08.126.

MA, Chen, 2021. Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports*. Vol. 7, pp. 7999–8012. DOI 10.1016/j.egyr.2021.08.124.

MARE, Shrirang et al., 2014. ZEBRA: Zero-Effort Bilateral Recurring Authentication. In : *2014 IEEE Symposium on Security and Privacy*, pp. 705–720. San Jose, CA : IEEE. May 2014. ISBN 978-1-4799-4686-0. DOI 10.1109/SP.2014.51.

MITNICK, Kevin D. and SIMON, William L., 2002. *The art of deception: controlling the human element of security*. Indianapolis, Ind : Wiley. ISBN 978-0-471-23712-9.

OGBANUFE, Obi, 2021. Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity. *Computers & Security*. Vol. 108, p. 102340. DOI 10.1016/j.cose.2021.102340.

PÉREZ-SÁNCHEZ, Antonio and PALACIOS, Rafael, 2022. Evaluation of Local Security Event Management System vs. Standard Antivirus Software. *Applied Sciences*. Vol. 12, no. 3, p. 1076. DOI 10.3390/app12031076.

REESE, Ken et al., 2019. A Usability Study of Five Two-Factor Authentication Methods. .

SALAHDINE, Fatima and KAABOUCH, Naima, 2019. Social Engineering Attacks: A Survey. *Future Internet*. Vol. 11, no. 4, p. 17.

SMITH, David T. and ALI, Azad I., 2019. YOU'VE BEEN HACKED: A TECHNIQUE FOR RAISING CYBER SECURITY AWARENESS. *Issues In Information Systems*. Vol. 20, no. 1, pp. 186–194. DOI 10.48009/1_iis_2019_186-194.

WRIGHT, Rebecca N., 2003. BASIC Programming Language. In : KURTZ, Thomas E. (ed.), *Encyclopedia of Physical Science and Technology*, pp. 61–77. third. Elsevier. Computer Software. ISBN 978-0-12-227410-7. DOI 10.1016/B0-12-227410-5/00838-3.

ZHANG-KENNEDY, Leah and CHIASSON, Sonia, 2022. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys*. Vol. 54, no. 1, pp. 1–39. DOI 10.1145/3427920.

ZWILLING, Moti et al., 2022. Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*. Vol. 62, no. 1, pp. 82–97. DOI 10.1080/08874417.2020.1712269.

Appendix A - Survey questions

1. **What is your age?**

   12-16

   17-20

   21-30

   31-40

   41-50

   51-60

   61-79

   80+

2. **Which job sector do you work in?**

   Corporate

   Freelancer

   Entrepreneur

   Public services

   Unemployed

   Health care

   Education

   Computer and IT

   Engineering

   Science

   Agriculture

   Entertainment

   Arts

3. **What is your highest received education?**

   Middle school

   High school

   Bachelor

   Masters

   Higher title

4. **What type of computer do you use?**

   Laptop

   Desktop computer

   both

5. **What operating system do you have in your computer?**

   MacOS

   Windows

   Linux

   Other

6. **Do you use a company computer (one provided by your company) or personal computer (one you bought on your own for private use)?**

   Company computer

   Personal computer

   Both

7. **Have you ever been educated on cyber security?**

   Yes No

8. **Would you take a seminar on cyber security if you had the option?**

   Yes, I would like to know more

   No, I am not interested in this topic

9. **Would you take a free seminar on cyber security?**

   Yes No

10. **Do you keep up to date with the latest security news or trends?**

    Yes, all the time

    Sometimes

    Only when it appears on media

    No

11. Do you think you could be the target of a cyber-attack or hacker?

Yes No

12. In your opinion, what are 3 main reasons you would get hacked or cyber attacked?

13. Have you ever been attacked or hacked and what did it cost you (loss of data, money,…)?

14. If you were attacked or hacked did your behavior towards cyber security change in anyway, if so how?

15. What are you most scared of?

Theft of login information (passwords)

theft of contacts

Money theft

theft of credit card information

loss of data

viruses

spyware

spam

other

16. What do you think is the most dangerous among cyber-attacks?

Virus

Spyware

Spam

Phishing

Scams

Hacking

Theft

17. I can identify when I (mark all that apply) :

am being hacked

am receiving spam

am getting scammed

am getting phished

have a virus

18. Do you let other people use your computer while being signed in as yourself?

Yes

Only if its an emergency

Only friends and family

Only family

Only if I forget to log out

No, never

QUESTIONS DIRECTED AT USERS WHO CHOSE PERSONAL COMPUTER

19. Do you actively seek and use protection against cyber-attacks for your computer?

Yes No

20. Do you rely on your operating system to provide you protection against cyber-attacks?

Yes No

21. In correlation to the previous questions, what is your reasoning behind your answers?

22. If you use extra protection what type of protection do you use?

Antivirus

Firewall

Antispam

Antispyware

Operating system files protection

I don't know

I do not use any extra protection

23. I believe I know how to protect private data or information.

Yes No

24. I have been victim to a cyber-attack in the past.

Yes No

25. If the previous statement applies, did you know how to react and proceed when the cyber-attack occurred?

Yes, I knew exactly what to do

No, I had to figure it out once it occurred

QUESTIONS FOR USERS WITH COMPANY COMPUTERS

26. Do you think your company does enough to protect your computer/s from cyber-attacks?

Yes No

27. Do you know what your firm does to protect company computers?

Yes

I'd like to know more about it

No

28. I have been educated on how to protect sensitive data?

Yes

Maybe

A little

No

29. Does your company provide cyber security classes/seminars?

Yes No

30. Are cyber security classes/seminars mandatory or voluntary/optional in your firm?

Mandatory

Voluntary, I choose to attend

Voluntary, I do not attend

We have a basic rundown when hired

My company does not provide this

31. Are you satisfied with the level of cyber security your company provides?

Yes

They could do more

No

They are too cautious

32. Has your company ever been breached/attacked, if so, how? (e.g. information leaked, virus, Dan from accounting opened an attached file from a sketchy email, Accounts stolen…)

33. Does your company have breach/attack protocols and if so are you aware of the steps you need to take?

Yes, I know exactly what to do

Yes, but I am not confident in using them

Yes, but I don't know them

No, they do not

34. Do you think you do enough to protect your computer?

Yes

Yes, but I could do more

No, I want to keep it safer

No

QUESTIONS FOR EVERY PARTICIPENT

35. **You get an email from your friend, out of the blue, and the subject line is "YOU GOTTA SEE THIS". When you open the email all that it contains is a link or file, with no message in the body. What would you do?**

    Click on it, and see what it is

    Reply to the email asking about it

    Delete the email

36. **While at work someone or a colleague walks up to you and hands you a USB saying that a "known associate" or "higher up" is sending you this USB. They say it contains information you need to review. How do you react?**

    I plug in the USB and see what is on it

    I plug in the USB and see what is on it, however I don't interact with anything on it

    I put it aside and ignore it

    I contact the sender to confirm that they in fact sent it

    I contact the sender to confirm that they in fact sent it, and if not I report it

37. **You get an email from your bank provider informing you that your account is suspended pending confirmation of your personal information. The logo for your bank is in the body of the email and the email is addressed "Dear Customer". The sender of the email is service@'*nameofyourbank*'customerserviceteam.com. What do you do?**

    Click on the link provided in the email and fill out what is needed

    Click on the link and call your bank to figure out the problem

    Delete the email

38. **You get an official email from your administrator informing you that one of your passwords has been compromised. What do you do?**

    Delete the email

    Check the breach by clicking on the provided link

    Go to the official website or services and manually change your password to a new more complex password

Appendix B - Interview questions

1. What is your name?
2. What is your age?
3. What is your job position?
4. What is your job description?
5. How long have you been in the industry?

6. What do you envision under the term hacking?
7. Are you familiar with white hat hacking, if so could you please explain this term using your own words?
8. What is your opinion on white hat hacking?
9. Do you think there is a difference between a Black and Gray hat hacker, if so what are they?

10. Do you keep up to date with the newest practices and trends of the cyber security world?
11. Do you personally take all the steps needed to fully protect yourself digitally?
12. Do you think age plays a factor in protecting yourself digitally?
13. If so, what steps do you think we as a society can take to bridge this gap/adapt the system?

14. How did you learn about cyber security?
15. Have you ever come in contact with a cyber-attack?
16. What do you think is the cause of cyber-attacks?
17. What do you think is the biggest threat in cyber security?
18. In your opinion what causes the most breaches in cyber security?
19. How do humans factor into cyber security?

20. Which practices do you personally think are best in cyber security?
21. Which of these practices do you use?
22. Which would you recommend for individuals?
23. Which would you recommend for firms?

24. How do you think we can improve cyber security?
25. How do you think we can improve cyber security when it comes to human error?
26. How has the evolution of the internet changed the way you approach cyber security?
27. Has the transition to faster internet changed your approach to cyber security?
28. How has the transition to faster internet progressed things within your firm?
29. How has the transition to faster internet helped in cyber security?
30. Have security practices evolved since the transition to faster internet?
31. How have practices in the CR evolved in comparison the rest of the world?
32. What is one thing you wish everyone using an electronic device would know or abide to?