Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies (FEM)

Bachelor Thesis

Media-literacy for university students: A case study in open-source solutions for identity protection and cyber-security

Murad Nassar

© 2023CZU Prague

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS TOPIC

Author of thesis:	Murad Nassar
Study programme:	Informatics
Thesis supervisor:	John Phillip Sabou, Ph.D.
Supervising department:	Department of Information Technologies
Language of a thesis:	English
Thesis title:	**Media-literacy for university students: A case study in open-source solutions for identity protection and cyber-security**
Objectives of thesis:	The purpose of this study is to sample the awareness of media-literacy among a student population at the Czech University of Life-Sciences, specifically the English speaking international program student body. Therefore, the goal of the project is to explore the level of exposure of students to cyber threats. In particular, the research question for this goal can be summarizes as follows: RQ1: How exposed are English speaking students to cyber-threats in the Czech Republic? RQ2: What are the long-term implications of the career development of international students relative to media-literacy? The study will then conclude with suggestions on the methods and open-source solutions for identity protection.
Methodology:	The thesis is based mixed methods, using both qualitative and quantitative data. Specifically, the project will make use of approximately 100 surveys and several interviews with students at CULS, particularly from the IT departments. Furthermore, this primary-data will be validated with secondary-data using Google forms for a statistical survey of the broader student population. For data collection the study will use Google Forms to create a survey that will be shared with the international student body at CULS, as well as a constructed interview protocol using semi-structured interviewing process to allow contextual exploration of the phenomenon.
The proposed extent of the thesis:	40-50
Keywords:	Identity protection, Cyber-threats, University students, Media literacy, Open-source solutions

Recommended information sources:

1. Cybersecurity Awareness Among Students and Faculty By: Abbas Moallem Date: 21 May 2019
2. Importance of Cyber Security By: Alex Tarter 25 May 2017
3. Intel Identity Protection Technology: the Robust, Convenient, and Cost-Effective Way to Deter Identity Theft By: Xiaoyu Ruan Date: 09 August 2014
4. Personas: Beyond Identity Protection by Information Control A Report to the Privacy Commissioner of Canada By: D.B. Skillicorn and M. Hussain Date: April 2009
5. Understanding Cyber Threats and Vulnerabilities By: Eric Luiijf Date: December 2008

Expected date of thesis defence:	2022/23 SS - FEM

Electronically approved: 14. 7. 2022
doc. Ing. Jiří Vaněk, Ph.D.
Head of department

Electronically approved: 27. 10. 2022
doc. Ing. Tomáš Šubrt, Ph.D.
Dean

Declaration

I declare that I have worked on my bachelor thesis titled " Media-literacy for university students: A case study in open-source solutions for identity protection and cyber-security " 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 15.03.2023

Acknowledgement

I would like to thank John Phillip Sabou, Ph.D., and my family and friends who supported me during my study and thesis writing.

Media-literacy for university students: A case study in open-source solutions for identity protection and cyber-security

Abstract

This thesis focuses on cyber literacy and understanding information security for students by presenting some of the cyber events that have already occurred due to ignorance of information security and lack of adequate resources and information to deal with these events and avoid their occurrence in the future.

The study aims to assess the student's knowledge regarding information security and examine the negative consequences of a lack of awareness in this area.

Moreover, including solutions that can reduce the dangerous consequences of these cyber events, as one of the proposed solutions to this problem, includes integrating information security as a fundamental subject in university curricula.

Clarify some critical concepts in the field of information security and provide open-source and accessible solutions that can be used to reduce cyber events or mitigate their effects and protect identity and information.

Keywords: Identity protection, Cyber-threats, University students, Media literacy, Open-source solutions, Data protection.

Mediální gramotnost pro vysokoškoláky: případová studie open source řešení pro ochranu identity a kybernetickou bezpečnost

Abstrakt

Tato práce se zaměřuje na kybernetickou gramotnost a porozumění informační bezpečnosti pro studenty formou představení některých kybernetických událostí, ke kterým již došlo z důvodu neznalosti informační bezpečnosti a nedostatku adekvátních zdrojů a informací, jak se s těmito událostmi vypořádat a předejít jejich výskytu v budoucnu.

Cílem studia je zhodnotit znalosti studenta v oblasti informační bezpečnosti a prozkoumat negativní důsledky nedostatečné informovanosti v této oblasti.

Navíc součástí řešení, která mohou snížit nebezpečné následky těchto kybernetických událostí, jako jednoho z navrhovaných řešení tohoto problému, je integrace informační bezpečnosti jako základního předmětu do univerzitních osnov.

Objasněte některé zásadní pojmy v oblasti informační bezpečnosti a poskytněte otevřená a přístupná řešení, která lze použít ke snížení kybernetických událostí nebo zmírnění jejich dopadů a ochraně identity a informací.

Klíčová slova: Ochrana identity, Kybernetické hrozby, Vysokoškolští studenti, Mediální gramotnost, Open-source řešení, Ochrana dat.

Table of content

1 Introduction

The Internet has been able to radically change human life through its access to all walks of life, where the Internet has become present in every home due to the features and facilities it provides, as it helped in that rapid technological development as the infrastructure of networks and means of communication developed to the extent that it became possible to download a full gigabyte In one second in some countries and increase in the number of Internet users, companies are competing to innovate phones, tablets, computers, and the Internet of things.

You can browse the latest world news through the Internet from anywhere and anytime while in bed. You can extract hundreds of books, tunes, and information in a few seconds, listen to music and movies, download them, and access gaming platforms and online games. Studying and working became possible remotely via the Internet, communicating with friends and family through video calls or voice calls and messages. You can browse many shopping sites, such as Amazon, and buy what you want, complete banking transactions, pay bills, and enter some sectors that were not expected to exist on the Internet, such as the health, government, and military sectors.

This increase was reinforced by the sudden shift in the Coronavirus crisis, as social distancing was the only solution to the crisis. This led to the increased time spent on screens, whether for work, study, or even to communicate with family and friends. All these reasons combined, and others have increased the number of users, the hours we spend on the Internet, the entry of the Internet into all aspects of life, and the prosperity of life in a beautiful technological way that facilitates all life work. When you hear these words, you can feel that we live in the most days of humanity in terms of technological prosperity.

With this increasing and rapid development day after day, other problems have increased with it, the most important of which is the information security problem, as it has become difficult to obtain an environment completely free of any cyber damage, as these attacks have led to disastrous results around the world. Many companies declared bankruptcy, and their employees became unemployed overnight. Sensitive data was leaked, privacy violations and intellectual and literary thefts, temporary or permanent suspension in vital places such as factories and banks, and Damage to infrastructure such as power plants and water desalination plants, causing Damage to reputation and causing problems in social relations.

All of these reasons highlight the importance of information security and the need for individual and societal efforts to end these attacks, reduce their severity, or even reduce their Damage in the event of their occurrence, and reduce the recovery time after the occurrence of these attacks. In this thesis, we will discuss the most important reasons that lead to cyber events and how to avoid and deal with them, and explain the importance of studying this field for all Internet users and trying to eradicate illiteracy in the field of information security by telling authentic stories of cyber-attacks that led to catastrophic results to take lessons and cues from them, in addition to clarifying Some concepts in the field of information security, which may be considered vague or new to some, and looking differently and positively for some things in the field of information security, such as the importance of passwords, the importance of privacy, and the importance of knowing your rights. Moreover, offer free and open-source solutions that all groups can use to reduce cyber events or reduce their severity if they occur.

2 Objectives and Methodology

2.1 Objectives

The purpose of this study is to sample the awareness of media-literacy among a student population at the Czech University of Life-Sciences, specifically the English speaking international program student body. Therefore, the goal of the project is to explore the level of exposure of students to cyber threats. In particular, the research question for this goal can be summarizes as follows:

RQ1: How exposed are English speaking students to cyber-threats in the Czech Republic?

RQ2: What are the long-term implications of the career development of international students relative to media-literacy?

The study will then conclude with suggestions on the methods and open-source solutions for identity protection.

2.2 Methodology

The thesis is based mixed methods, using both qualitative and quantitative data. Specifically, the project will make use of approximately **100** surveys and several interviews with students at **CULS**, particularly from the IT departments. Furthermore, this primary-data will be validated with secondary-data using **Google forms** for a statistical survey of the broader student population. For data collection the study will use **Google Forms** to create a survey that will be shared with the international student body at **CULS**, as well as a constructed interview protocol using semi-structured interviewing process to allow contextual exploration of the phenomenon.

3 Literature Review

3.1 Cyber security and cyber incidence

What is the term cyber security, and what are the primary sources for cyber threats and cyberattacks?

Cyber security defends computers, servers, mobile devices, electronic systems, networks, data, hardware, and software, from malicious attacks. It is also known as information technology security or electronic information security.

Common cyber threats include **Malware and Ransomware, Social engineering, Phishing, Unsecured networks, Outdated or un-updated system, and Denial of service (DoS).**

Cyber threats can originate from various sources, from hostile nation-states and terrorist groups to individual hackers, to trusted individuals like employees or contractors who abuse their privileges to perform malicious acts. (Kaspersky, 2023)

3.1.1 Common cyber threats include.

Malware is malicious software that can cause harm in many ways, including taking control of your devices to attack other organizations and obtaining credentials that allow access to your organization's systems or services that you use.

Ransomware is malicious code that prevents you from accessing your computer (or the stored data). The computer itself may become locked, or its data might be stolen, deleted, or encrypted. Moreover, the attacker may demand a ransom. (Kaspersky, 2023)

Social engineering describes hackers' techniques to persuade victims to behave suspiciously. Some questionable actions often involve a breach of security, sending money, or giving up private information. These actions tend to go against our better judgment and defy common sense. However, by manipulating our emotions, good and bad, like anger, fear, and love, scammers can get us to stop reasoning and start acting on impulse without regard to what we are doing. (Malwarebytes, 2023)

Phishing is an attack in which the threat actor poses as a trusted person or organization to trick potential victims into sharing sensitive information or sending them money. Email phishing, smishing, and vishing are some examples of phishing. (Malwarebytes, 2023)

Unsecured networks An unsecured network most often refers to a free Wi-Fi (wireless) network, like at a coffeehouse or retail store. There is no unique login or screening process to get on the network, which means you and anyone else can use it. (Whatismyipaddress, 2019)

Outdated software technology is a concept that encompasses software, hardware, programming languages, services, or practices that are no longer used and Support discontinued.

While **un-updated system** means the hardware and software are not updated because the user did not update them. (Dagher, 2022)

A denial-of-service (DoS) attack is a type of cyberattack when a hacker tries to prevent a computer or other device from being used by its intended users by interfering with its regular operation. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until regular traffic cannot be processed, resulting in a denial of service to additional users. (Trendmicro, 2023)

3.1.2 Real-world cyber incidence

It might be challenging to persuade people to take cybersecurity seriously if they think their information or online identity is optional. To try and persuade them, we can offer a variety of arguments. The possible repercussions of not taking cybersecurity seriously can be illustrated by providing instances and sharing real-life examples of how cyberattacks harm people or organizations. Moreover, underline the individual influence. If people know the potential consequences of a cyber assault on their personal lives, they may be more likely to take cyber security seriously. For instance, if someone's identity is stolen and utilized to do business, or relationships, or face legal troubles, these issues may become quite problematic. Here is a real-life example of how cyber-attacks affected individuals or organizations:

On February 5-2021, a cyber-attack could have caused dozens of deaths and many injuries to the residents of the area covered by a water treatment plant for a city of roughly **15,000** people in the west of Florida; the invader increased the amount of sodium hydroxide, in the water supply by **100 times** more than usual. Sodium hydroxide is used in treatment facilities to reduce water acidity and remove metals from drinking water. Burns, vomiting, excruciating agony, and bleeding can all result from sodium hydroxide poisoning.

However, fortunately, one of the workers noticed this change. The employee noticed his computer screen's mouse was being pushed around, opening various software features that managed the water being treated. After the incident in Florida, the state Department of Environmental Protection issued a warning to public water providers, advising them to be "on heightened alert" for any odd behavior and to keep an eye on system security. Moreover, it provides information security training and focuses more on strengthening cybersecurity. The local government information technology expects the attack was made through phishing mail. This incident is opening many eyes because public health is connected to systems with cybersecurity vulnerabilities. (Bergal, 2021) **The attack was made by phishing mail and Malware.**

The first known death from a cyberattack with ransomware was reported after cybercriminals hit a hospital in Düsseldorf-Germany, in which hackers encrypt data and hold it hostage until the victim pays a ransom. The ransomware invaded **30 servers** at University Hospital Düsseldorf, crashing systems and forcing the hospital to turn away emergency patients. As a result, a woman in a life-threatening condition was sent to a hospital 20 miles away and died from treatment delays. Hospitals cannot afford downtime, so they may be more likely to pay quickly with minimal negotiation to restore their services. So that makes them a prime target. The most aggressive reported attack on healthcare facilities was North Korea's 2017 "WannaCry" ransomware attack, which froze British hospitals and forced doctors to cancel surgeries and turn patients away. (NICOLE WETSMAN, 2020) **The attack was made by phishing mail and Ransomware.**

In 2013, the port of Antwerp, Belgium, fell victim to a cyber-attack by criminals to manipulate the movement of shipping containers containing illegal drugs. The attackers gained access to the port's systems through targeted spear phishing and malware attacks aimed at port authority workers and shipping companies. Once inside the system, they could alter the location and

delivery times of containers carrying drugs, allowing smugglers to collect them undetected. This incident highlights the vulnerability of critical infrastructure to cyber-attacks and the importance of robust cyber security measures to protect against them. (Sam Shead, 2022) **The attack was made by phishing mail and Malware**.

In 2019, Toyota company fell victim to a social engineering attack. The perpetrators utilized various social engineering techniques to deceive the company's employees into wiring **$37 million** to their accounts. The attackers entered the company's email system by acquiring an employee's login credentials through a phishing attack. Subsequently, they leveraged this access to orchestrate the BEC scam. The attackers established email addresses that mimicked those of high-ranking executives within the firm and employed them to send emails to personnel, instructing them to transfer funds to specified bank accounts. The emails contained detailed information on ongoing business transactions and were dispatched from trusted sources, lending credence to their authenticity. The attackers furthered their scheme by developing fake websites and invoices purportedly from legitimate vendors and suppliers, amplifying the illusion of legitimacy. (Andreea Popa, 2021) **The attack was made by phishing mail and Ransomware.**

In December 2019, A ransomware attack left around **300 employees** unemployed. The Heritage Company admitted that the ransomware attack that hit the company caused huge losses. Moreover, they hoped it would be a temporary closure. **After running for 61 years**, the Heritage Company has been the same since then. (Abeerah Hashim, 2022) **The attack was made by denial-of-service (DoS) attack and Ransomware.**

In May 2021, a state of emergency was declared in several US states after hackers caused a vital oil pipeline to shut down. The pipeline company admitted to paying criminals **$4.4m in hard-to-trace Bitcoin** to get computer systems back up and running (Guardian staff , 2021). **The attack was made by Ransomware.**

In July 2010, malicious software, the Stuxnet worm, destroyed Iranian centrifuges. The worm caused the centrifuges to spin faster, destroying them and causing a mysterious explosion at the centrifuge assembly. This incident resulted in significant damage and the destruction of a central centrifuge assembly workshop. Centrifuges are crucial for producing enriched uranium, which can be used as fuel for reactors or in creating nuclear weapons; a double agent

uses a flash drive to infect the computer systems. The systems were not connected to the internet to prevent external attacks. The Stuxnet worm remained dormant until a specific set of conditions was met, and it appeared that everything was functioning normally. Iranian officials attributed the fire to a cyberattack. (NOS News, 2019) **The attack was made by Malware due to Unsecured networks** and **un-updated system.**

23 Feb 2023, **3TB** of sensitive files and important emails of the **Ministry of Defense** were leaked from a server that was used on the government azure cloud that Microsoft made for the Ministry. There is a battle between the Pentagon (the US Department of Defense) and Microsoft because of the incident. Before three years, Microsoft won a **$10 billion** deal from Amazon, Oracle, and Google in 2020 to create this system. No attack or penetration led to the leak of emails and data.

How did 3Terra bits leak out? **The admin forgot to create a password on the server! Yes**, he forgot to create a password on the internal mailbox server of the US Department of Defense. The Ministry of Defense and Microsoft blamed each other because of the incident. So here we can see how important the password is and how important information security is for people who work in sensitive places. (Vigliarolo, Brandon, 2023) **It is not an attack, but it shows how important the password is and how important to have knowledge about cybersecurity.**

Facebook's capacity to anticipate the behavior of users enables companies to target potential customers based on decisions they have yet to make. This could allow third-party entities to influence a consumer's anticipated action. Facebook has indicated that it can analyze its entire user base of over **2 billion people** and identify millions of individuals who may be at risk of switching from one brand to a competitor. Such individuals can then be the focus of highly targeted advertising, which may pre-empt and alter their decision-making process entirely, a service that Facebook refers to as "loyalty prediction" that enhances marketing efficiency.

Facebook's approach to advertising using artificial intelligence shares certain similarities with Cambridge Analytica's controversial "psychographic" profiling of voters. Both methods use ordinary consumer demographics, such as interests and location, to predict future actions. However, Facebook can access significantly more extensive user behavior and preferences

databases than Cambridge Analytica and its peers. A report by ProPublica in 2016 revealed that Facebook has approximately **29,000 distinct criteria** for each user.

To make it easy to understand, Meta company that own now (**Facebook, Instagram, Snapchat, WhatsApp**) can create a digital copy of you according to the information and data that we give to all these apps, Either intentionally or unintentionally way, like posts or links or the pages you like and the content you are interested, the danger here is how they can change what we want to what they want With our belief that we chose what we want or expect what we will do by conducting experiments on our digital copy that they create from the information they collect about us, whether legally or illegally ways, and we do not know what is happening behind the scenes either.

Facebook instead offers the ability to target them based on how they will behave, what they will buy, and what they will think. These capabilities are the fruits of a self-improving, artificial intelligence-powered prediction engine, first unveiled by Facebook in 2016 and dubbed "FBLearner Flow."

Some may perceive this as a privacy issue. However, it is crucial to remain cognizant of the data we share on social media and comprehend how ordinary companies we often trust handle our data, let alone cybercriminals who may access it. (Sam Biddle, 2018)**This example shows how essential to take care of your data and identity or what you share on social media and what can happen behind the scenes in your data.**

Hackers gained access to several well-known Twitter accounts in **July 2020**, including those of **Jeff Bezos, Elon Musk, and Barack Obama**, and they used them to spread a bitcoin fraud. The attackers used phishing and social engineering techniques to find Twitter personnel with access to internal systems and tools. They deceived staff members into giving them access codes to the company's systems by disguising themselves as the IT department. After getting into the internal systems, the attackers increased their level of access. They accessed the accounts of well-known people, which they then utilized to spread the word about the bitcoin hoax. This incident generated worries about the security of social media platforms and caused considerable disruption. Twitter put precautions in place after confirming the incident resulted from social engineering and phishing and implemented measures to improve security, such as two-factor authentication and improved employee training on cybersecurity best practices. (Sheera Frenkel, 2021) **The attack was made by phishing mail and social engineering .**

WikiLeaks has made several significant disclosures of confidential material, including secret documents and emails. One significant instance is the internet publication in 2010 of diplomatic cables from the United States, which exposed sensitive information about those connections and resulted in the retirement of several senior officials. Whistleblower website WikiLeaks released **250,000 US diplomatic** cables revealing details of conversations between the secretary of state and US embassies to media outlets worldwide. (NEWS WIRES, 2020)

3.2 Cyber terms and tips

3.2.1 The General Data Protection Regulation (GDPR)

GDPR a piece of European Union legislation, ensures people's protection through the processing of their data and the unrestricted transfer of that data. Following going into effect on May 24, 2016, it became legally binding and directly applicable in all of the **EU's member states on May 25, 2018.**

One of the reasons is that it is probably the most challenging data protection regulation in the world. That means severe consequences for non-compliance, burning a massive hole in lax businesses' pockets. Knowing your rights and protecting your information is essential because you will be subject to legal accountability if your data or information is used illegally. Moreover, if you use other people's data without authorized permission or in an illegal way, you will be subject to legal accountability. Enforcement authorities can issue fines of up to **20 million euros** under the GDPR laws, or **4%** of a business's global annual turnover if that is higher. Over 900 fines have been issued since GDPR was first enforced, the largest of which **was $877 million**. (GDPR.EU, 2020)

Cookies

Cookies are small files of information that a web server generates and sends to a web browser. Web browsers store the cookies they receive for a predetermined period or the length of a user's session on a website. They attach the relevant cookies to any future requests the user makes to the web server. Cookies help inform websites about the user, enabling the websites to personalize the user experience. For example, e-commerce websites use cookies to know what merchandise users have placed in their shopping carts. In addition, some cookies are necessary for security purposes, such as authentication cookies.

Third-party cookies can collect much about your online activity, from your google searches to your shopping habits. Using a privacy-oriented browser that stops third-party trackers from following you around the internet is the first and crucial step in protecting your privacy. (Cloudflare.com, 2022)

Manage browser cookies.

- Third-party cookies blocker from browser extensions .
- Remove cookies from the browser every few months to clear things out.
- Browsers like Brave or safari Stop third-party cookies in their tracks.
- Turn off applications that ask for tracking. (Cloudflare.com, 2022)

3.2.2 Email.

Clicking a link in an email is not always dangerous, but you should know the potential risks and understand how to feature that risks.

Malicious Link.

You could accidentally click a link to download a malicious file such as a virus, trojan, or malware, especially if you do not have protection, such as an antivirus or antimalware, or even if you did not check the link through some link-checking sites such as virus total.

Several things can happen when clicking on a malicious link:

Some links, once clicked, contain a set of codes. It gives the attacker access to your device settings and changes the security settings in your device. Some links are integrated with tracking software to track your online activities. Moreover, it can allow marketers to see what parts of their ads/emails are most effective and use data to target you better for ads. Some links can allow an attacker to use your device to perform server attacks, such as a denial-of-service attack. The link may also contain a malicious program that steals your files, such as your banking information or data and uses them illegally. Moreover, it exposes you to legal accountability.

Also, it may contain ransomware that disables your access to some files or even your device Imagine losing access to however many hundreds or thousands of family photographs or other

critical files you may have saved on your PC. This attack has shut down businesses, governments, and even hospitals. Almost every incident was because someone clicked on a link or opened an attachment without vetting them. You could be taken to a misleading site. Once, that may even resemble a trustworthy website.

Generally, it is best to ask yourself these questions before clicking, do you know the sender? Would they send a message like what you received? Do they usually email you? Were the spelling and grammar how they typically message? Are they claiming to be a Nigerian prince who will give you their inheritance if you do them a favor? Is the address being linked to spelled commonly (**such as paypal.com vs. paypol.com**)?

Clicking links most of the time is safe if you have a good spam blocker blocking most of the bad stuff; Gmail generally has the best spam filter and can help you. Remember to stay diligent and be on alert to this possibility. Bad actors are betting you will not be, so always take a moment to prove them wrong. Never blindly click on links or open attachments. The risk is too significant. (Alex Tarter, 2019)

95% of all attacks on enterprise networks result from successful spear phishing. For mid-size businesses, a phishing attack typically costs **USD 1.6 million**. In **2017, 76%** of companies said they had experienced a phishing attack. Targeted users open **30%** of phishing communications, and **12%** of those users click on any dangerous attachments or links. (Givaudan, 2023)

3.2.3 Passwords

Strong passwords are critical in securing your electronic accounts and devices, as they serve as a barrier against unauthorized access. Creating a long and complex password increases the difficulty of a hacker cracking it, whether through a brute-force attack that systematically tries every combination of letters, numbers, and special characters or an automated machine attack that tries numerous combinations in a short time frame. (Eset, 2022)

Compromised passwords were responsible for **80%** of all data breaches in **2019**, resulting in financial losses for individuals and businesses. While many people worry about forgetting complex passwords, it is crucial to create strong passwords to protect against cyber threats. A strong password can make it exponentially more difficult for cybercriminals to guess,

especially if it is at least **20 characters** long and includes a combination of upper/lowercase letters, numbers, and symbols. Such a password would take a computer approximately three sextillion years to crack. Cybercriminals use various attack methods to target simple passwords, including disinformation campaigns against businesses, data sharing with competitors, and ransom storage. (Amber Steel, 2019)

Creating strong passwords is crucial to ensure the security of electronic accounts and devices and to protect sensitive personal information from cyber threats and hackers. **To create secure passwords, one can follow these tips:**

- Creating solid passwords by incorporating characters, uppercase and lowercase letters, numbers, and uniqueness is recommended as an effective strategy to enhance password security.
- Use a password manager and two-factor authentication for added security.
- Use two-factor authentication (2FA) wherever possible to provide an additional layer of security.
- Incorporate numbers, symbols, and uppercase and lowercase letters to increase the complexity of the password.
- Ensure the password is at least eight characters long to reduce the risk of brute force attacks.
- Change passwords regularly and avoid recycling old passwords.
- By following these guidelines, one can create secure and robust passwords that are more difficult for cybercriminals to crack.. a solid and secure password is critical to reducing the risk of cybercriminals accessing sensitive data. (Eset, 2022)

3.2.4 Safety online.

Privacy

Use your privacy settings to limit who can access your files, and use caution when revealing personal information online. Avoid utilizing location-based services to stop your whereabouts from being tracked. Avoid revealing PINs, bank account details, social security numbers, or credit card numbers online, and use only secure websites with (**https://**). Monitor suspicious activity and be wary of suspicious activity that requires immediate action. It offers something that sounds too good to be true. Requests your personal information. Check Your Online Accounts Regularly Be Wary of Pop-Ups. Keeping social media accounts secret reduces the risk of identity theft.

Keeping your social media accounts confidential is crucial to reducing identity theft risk. Cybercriminals can quickly collect enough personal information about you to impersonate you, causing damage to your money and reputation. (Titanfile.com, 2022)

Software updated.

Keep your operating system apps and software updated to avoid vulnerabilities that hackers can exploit. Software updates provide new and improved capabilities by fixing issues like bugs and crashes. Antivirus developers frequently update their solutions to protect you from new viruses and malware. (Kevin James, 2023)

Network security.

Protect your home or business network with secure Wi-Fi and Internet connections and change passwords frequently. Network security is paramount in protecting workstations from malicious spyware and securing shared data. It uses various measures to prevent **Man-in-the-Middle** (**MiM**) attacks, including splitting information into smaller pieces, encrypting it, and transmitting it through independent channels to deter eavesdropping. Since Bluetooth-capable devices can be compromised, allowing hackers to obtain personal data. When it has not needed, Bluetooth must be turned off. (Maile McCann, 2023)

Virtual Private Network (VPN)

By hiding your identity and **IP** address from other gamers, a Virtual Private Network (**VPN**) stops them from following you and accessing your data, preventing your device from being used in a **DoS attack**. Although it is practical to use public WiFi, doing so exposes users to possible security threats. Unauthorized people can readily see private internet actions, whether conducted at a neighborhood coffee shop perusing the web or in an airport while checking social media. Using a **VPN** offers complete security for your data, including browsing history, passwords, and financial details. (Maile McCann, 2023)

Antivirus and Antimalware.

Antivirus and Antimalware contain specialized tools made by developers that can identify and stop malicious programs. It takes much time for developers to update these vulnerabilities to help us. Stopping the harm of these malicious programs turns a blind eye to what they do, whether through monitoring, stealing files, destroying them, or even changing some settings and

data. It is advised to check external devices for malware before accessing them to limit potential harm. (ncsc.gov.uk, 2019)

Backup.

Creates copies of your platform or personal files on a hard drive or additional storage devices such as an external backup or flash drive. You may rapidly restore your files to their original form without significant data loss or inconvenience if you have a backup. (kaspersky.com, 2022)

Information security awareness.

Think Before You Click! links in texts or emails from people you do not know and be careful about debt consolidation offers and student loan payment. To know the latest hacking techniques and how they can be avoided, the tools that can be used to maintain your safety online, the programs you should avoid, and the techniques used by cybercriminals and avoid falling into them. You can learn some lessons and techniques from sites like YouTube or educational course sites. Alternatively, follow some sites like The Hacker News, The State of Security. (Abbas Moallem, 2019)

Protection application or programs.

Removing adware from your devices will help you receive more relevant adverts because it tracks your internet activities. With programs like AdwCleaner, remove any adware on your computer to protect your privacy. **Examples of programs, tools, and applications to Use:**

-Use Anti-Virus and Anti Malware VPN. Firewalls

-Use an Anti-Phishing Toolbar

-Use a fast search engine to protect your privacy (Duckduckgo). (Andreea Popa, 2021)

-Use secure browsers like Tor browser or Brave browser.

-Intrusion Prevention Systems, Email Security Solutions, DDOS Protection. (Kaspersky, 2022)

4 Practical Part

4.1 The study

The study was meticulously conducted with a deliberate focus on selecting a specific target audience: English-speaking university students. The research was conducted at the Czech University of Life Sciences in Prague (**CULS**), specifically at the University Faculty of Economics and Management (**FEM**). Given this cohort's daily use of computers and the internet, whether for academic or professional purposes, mixed methods using qualitative and quantitative data were employed.

Over **100** students were interviewed in person during official working hours on the university campus. The study comprised **personal interviews** with students, regardless of their language of study (**English or Czech**), as long as they were **proficient in English**. The thorough planning and execution of this research are reflected in using both qualitative and quantitative data analysis techniques. The decision to focus on this category of individuals was based on the following inquiry.

Suppose individuals regularly use technology, and the internet needs acceptable information security awareness. How might those who use these tools to a lesser extent or in different ways fare? The questions were carefully chosen to suit the desired purpose, which is to assess the student's level of information in the field of information security. The questions utilized in the study were carefully selected following **GDPR** and **ISO/IEC 27000** standards and by consulting the Department of Information Technologies (**FEM**) at our university. The questionnaire was administered via Google Forms to facilitate accurate data analysis.

I did the interviews with the students, and the interviews with students were conducted to enhance the study's credibility. Additionally, the questionnaire required the student to input their university email to ensure the authenticity of responses and prevent random submissions or duplicates.

4.1.1 Methodological tools.

Over the years, **Google Forms** has seen several modifications. Menu search, question shuffle for randomized order, limiting responses to one per person, shorter URLs, custom themes, automatically generating answer suggestions when creating forms, and an "Upload file" option are just a few features available. Users can also answer questions that ask them to share content or files from their computer or Google Drive by selecting this option. Because it was essential to collect data from the research population efficiently, I used Google forms. The ease of using Google Forms and displaying the results without needing another program to analyze the data and display it in an easy-to-understand graph, and Results and questions can be displayed in an easy-to-handle format.

4.1.2 Semi-structured interviews.

The interviews were conducted by selecting a student and asking him about the possibility of filling out an application on information security. The **iPad** was used to deal smoothly and efficiently in filling out the questions, as the **iPad contains the questionnaire page**.

In the beginning, I explain the reason for this questionnaire and that it aims to know the level of awareness of students in the field of information security. The interviews were conducted so that I explained the question to a student and ensure that the student understood the purpose of the question so that he could answer correctly and reduce the percentage of error as much as possible in the final results and obtain accurate results.

The purpose of doing the interviews with the questionnaire was for several reasons:

-To avoid filling the request randomly and rapidly by students without understanding or even reading questions.

-Ensure that the student understands the question correctly, given that most of them do not know some terms in the field of information security.

-Some questions depend on each other to form a complete picture of the level of awareness in the field of information security, such as the question about the password.

-Some questions need explanation, such as what to do if you receive an email with a link and attachment.

4.1.3 Limitations of the study

The language used in this questionnaire is **English only**, and the target group is only English speakers because **I needed to understand the English** language to answer the questionnaire. The target group was university students only and the Czech University of Life Sciences in Prague (**CULS**) only. Some students were concerned about filling out the university's email, as I explained that the purpose of putting the **university's mail** is that the target group for the questionnaire is university students. The presence of the university's mail is evidence of the validity of the results. Some people were also worried about filling in questions about the password because they thought hacking could compromise this information.

5 Results and Discussion

5.1 Information security in the educational process

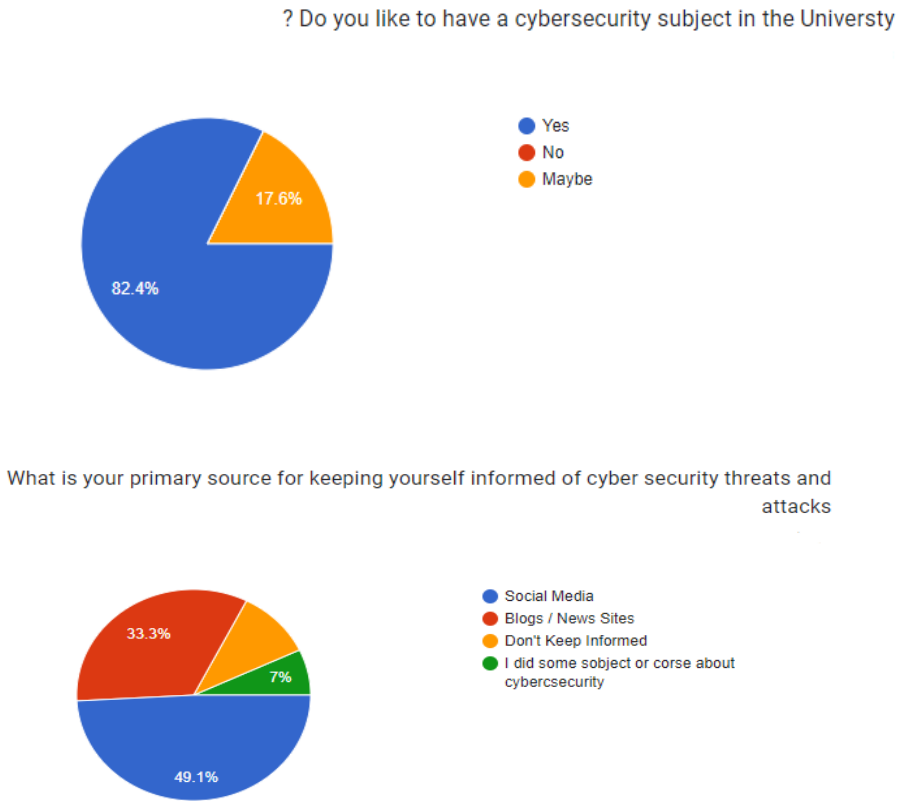
Integrating the information security course into the educational process can positively eradicate cyber illiteracy and reduce cyber incidents or mitigate their consequences. People trust information from education, whether universities or schools, more than other education sources. Some need to improve in seeking knowledge and learning new things, and education can motivate people to learn information security. This will motivate the student because it will be part of the study plan. Some people need more reliable sources to obtain information, which can be found during information security. Also, education is considered the most widespread sector in all walks of life.

The topic of information security often brings to mind the concept of First Aid and the significance of first aid in all walks of life, including government institutions, corporations, and educational institutions, among others. First aid equips individuals with fundamental knowledge that can be utilized to preserve human life. Although possessing a first aid certificate does not necessarily qualify an individual as a doctor, it empowers them to act promptly and potentially save lives in certain situations.

Following consultation with the **Department of Information Technologies** at our university, it has been determined that including information security as a subject in the **bachelor's degree** program at our faculty (**FEM**) is essential. We propose a request to make the subject available to university students, or at least to Faculty of Economics and Management (**FEM**) students, where feasible, considering the significance of this field and the lack of awareness among college students.

From the study, **82%** of students want a cybersecurity subject that can give information security fundamentals to help them be aware of cyber threats and attacks, whereas **7%** only had a cybersecurity subject or training. The proposed subject would cover the fundamentals of information security. Considering the increasing prevalence of cybersecurity threats.

Figure 1. Question 1- Results



Source: Own Illustration

The absence of an equivalent program to first aid or safety training for information security is worth considering. A program focused on protecting individuals from cybersecurity risks by imparting knowledge on information security would be valuable. as valuable as first aid. Including cybersecurity education in the education system would be beneficial, as it would help individuals understand how to stay safe online and protect against cyber threats. Cybersecurity education should be considered a critical life skill like first aid training. Educating people about cybersecurity can create a safer and more secure online environment. Taking cybersecurity seriously is necessary to prevent the escalation of cyber-attacks and the resulting losses, even at the level of human lives, such as the Florida incident.

5.1.1 The open sours solutions

This thesis will examine open-source solutions for identity protection and cyber-security, including their effectiveness and limitations. A comprehensive review will analyze existing

research on the topic. A case study approach will be used to investigate the implementation and impact of open-source solutions in the real world. The outcomes of this research will yield significant insights into utilizing open-source solutions to enhance identity protection and fortify cyber-security.

Open-source solutions have become increasingly popular as an alternative to proprietary software in identity protection and cyber-security. These solutions are freely available to the public and can be modified and distributed by anyone, which makes them cost-effective, transparent, and auditable. Open-source solutions are often more cost-effective than proprietary software, as they do not require licensing fees.

However, it is worth mentioning that open-source solutions may not be as user-friendly as proprietary software, making them more difficult for non-technical users to understand and implement. Additionally, open-source solutions may have a different level of technical support or documentation than proprietary software, making it more difficult for users to address any issues that may arise.

Furthermore, it is essential to remember that the security of an open-source solution depends on the community of developers who maintain and improve it. Community support can result in a lack of updates and security fixes, making the solution vulnerable to attacks. It is pertinent to acknowledge that while open-source solutions can bolster cyber-security, they should be supplemented with additional security measures, such as robust passwords and timely security software updates. It is important to note that no single tool can provide complete protection, so combining different tools is recommended to improve your overall cybersecurity.

It is also crucial to have a comprehensive security strategy that includes training, awareness, and monitoring to help minimize cyber-attack risks. A wide range of open-source solutions is available for identity protection and cyber-security:

Tor is a network that facilitates anonymous communication by routing traffic through several layers of encryption, thus ensuring high privacy and security, to protect your privacy. (https://www.torproject.org/)

ClamAV is an open-source antivirus solution, designed to provide protection against viruses and various forms of malware. It offers a reliable defense mechanism for detecting and eliminating malicious software that may pose a threat to computer systems. (https://www.clamav.net/)

OpenVPN is solution that provides a robust defense against cyber threats. It accomplishes this through encryption of internet traffic and the establishment of a secure connection between devices. (https://openvpn.net/)

KeePass is an open-source password manager, designed to enhance identity protection by securely storing and generating strong, unique passwords. It provides a reliable solution for users to safeguard their credentials and mitigate the risk of cyber threats. (https://keepass.info/)

Let's Encrypt Let's Encrypt is an open-source certificate authority that provides free **SSL/TLS** certificates to help secure websites. (https://letsencrypt.org/)

OSSEC is an open-source host-based intrusion detection system that can help protect against unauthorized access to systems and data. It can monitor system logs and alert administrators when it detects suspicious activity. (https://www.ossec.net/)

Snort is an intrusion detection system that operates on an open-source framework designed to identify and thwart cyber-attacks. (https://www.snort.org/)

KeePass is an open-source password manager that can help generate and store strong and unique passwords. (https://keepass.info/)

Wireshark This free network protocol analyzer can monitor network traffic and detect any suspicious activity. (https://www.wireshark.org/)

Spybot Search and Destroy This is a free anti-spyware tool that can detect and remove spyware and other malicious software. (https://www.safer-networking.org/)

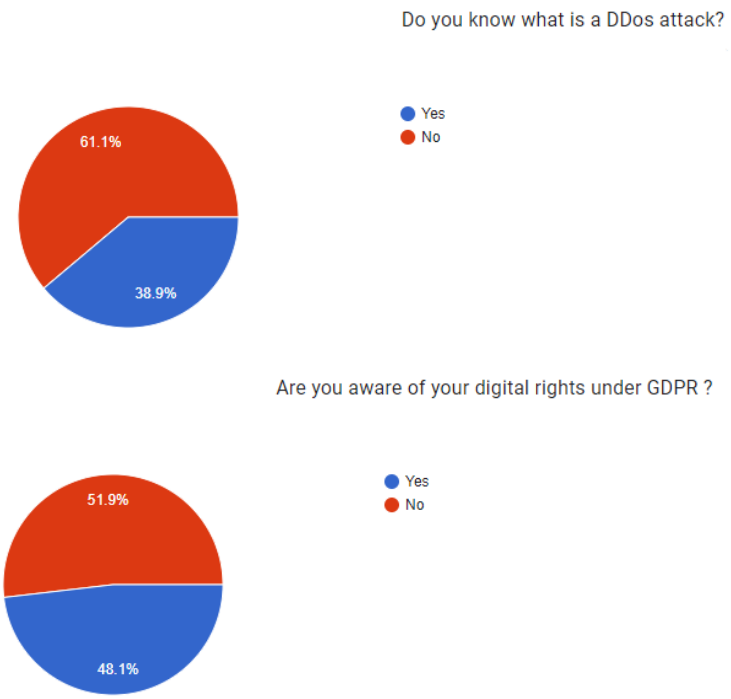
Avast Free Antivirus This is free antivirus software that can protect your computer from viruses, spyware, and other forms of malware. (https://www.avast.com/free-antivirus-download#pc)

CCleaner This free tool can help optimize your computer's performance and remove unnecessary files and registry entries. (ccleaner.com)

Malwarebytes This free anti-malware software can detect and remove malware, trojans, and other malicious software. (https://www.malwarebytes.com/)

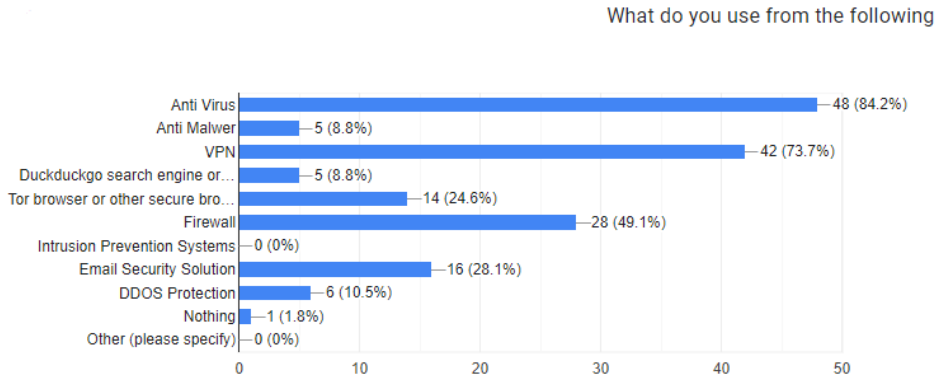
How exposed are university students to cyber threats in the Czech Republic?

Figure 2. Question 2 - Results

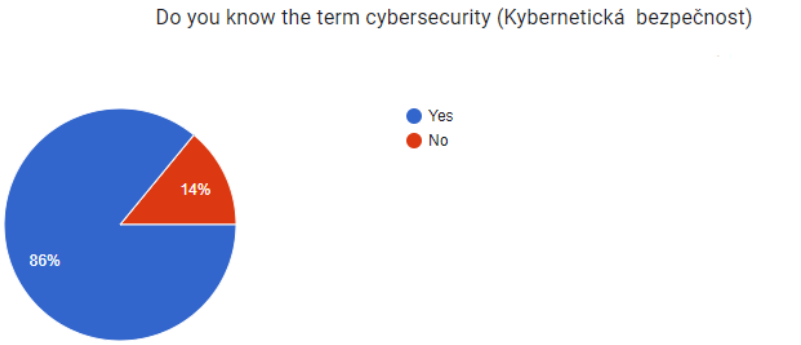


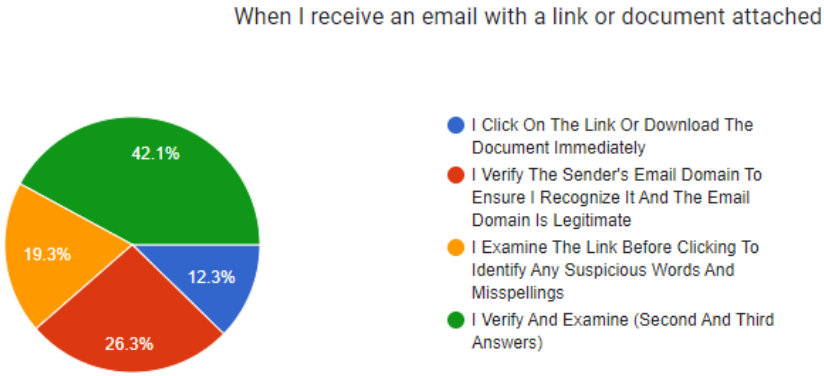
Source: Own Illustration

Figure 3. Question - Results



Source: Own Illustration





Source: Own Illustration

It is easier to answer such questions by clearly studying the mentioned sample. Therefore, we conducted a study to understand the extent of students' information in information security. Moreover, the extent of their awareness of the dangers resulting from these threats. During the questionnaire, the focus was on understanding the questions for the students, and the work of the questionnaire in the form of personal interviews was one of the reasons for obtaining the

best results. The questions were carefully chosen by the assistant of the Information Technology Department, as mentioned in the practical section. by selecting real questions through which we can analyze their answers, we can reach an answer to several questions, including determining the level of awareness of students in the field of information security. by analyzing the answers, we got from the questionnaire, some of which I will mention here. through the results of some basic questions in the field of information security, we concluded to answer this question.

Do you know the term cybersecurity?

Despite the question's simplicity and ensuring that the student understands the question, **14%** were unfamiliar.

Do you know what a DDoS attack is? One of the most critical and successful cyber-attacks is the DDoS attack.

This attack and how to protect against it have been explained in the theoretical part.

A relatively large percentage, **61%** were unfamiliar.

Are you aware of your digital rights under GDPR? The General Data Protection Regulation (**GDPR**), which was explained in the theoretical part as well, due to its importance .**51%** Unfamiliar with their rights in the field of information security.

What do you use from the following applications?

What is your action when you receive an email with a link or document attached?

These are some of the questions whose answers are somewhat worrisome. As I mentioned in the theoretical section, I explained the importance of answering these questions and the seriousness of ignoring them

According to the result, our university students are highly exposed to cyber threats.

However, like all individuals who use technology, students may be at risk of cyber-attacks. Factors include a need for awareness about cyber-security and access to resources or technology that can enhance security. Additionally, cybercriminals may target students who are aware that they may have a large amount of personal and financial information stored on their devices, making them an attractive target for lack of information about cyber threats and experience on how to deal with these events.

5.2 What are the long-term implications of the career development of students relative to media literacy?

The long-term implications of media literacy on the career development of students can be significant. In the long term, media literacy can help students be more competitive in the job market, as employers will look for candidates with knowledge and experience. It can also help students to be more resilient and adaptable in the face of an ever-changing digital landscape. It will also significantly reduce future cyber events' effects and consequences and reduce or even prevent recovery time and budget for cyberattacks. It is, moreover, creating a generation more aware of information security and preserving information and identity.

It is a crucial skill in today's digital age. Knowing the proper means and places to get information is very important. This skill set empowers individuals to identify and steer clear of misinformation and propaganda, enabling them to make well-informed decisions regarding the use of technology in both their personal and professional lives. Cybersecurity helps to ensure the privacy and security of individuals and organizations by safeguarding against cyber-attacks and other online threats. Accelerate recovery time from attacks and control them if they happen. Essential for protecting critical infrastructure from cyber-attacks that could have severe consequences for society. Cybersecurity plays a crucial role in preserving the confidentiality and security of data, ensuring its accessibility when needed, and mitigating a wide range of cyber threats.

5.3 Discussion

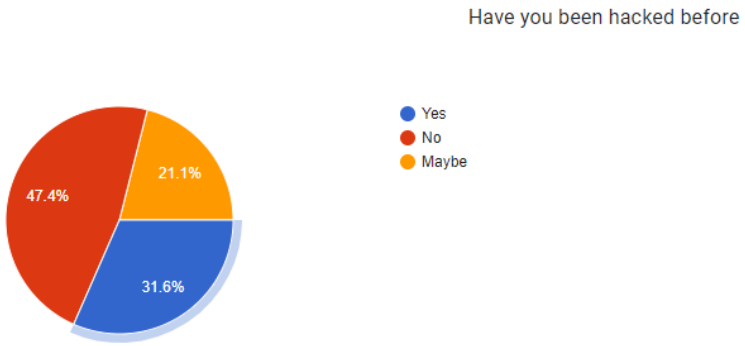
I noticed, through interviews with students, that there are several worrisome issues in the field of information security. A large percentage do not know where to get the information from Interestingly, it seems they need to be more motivated to learn. A large percentage relies on information from social media, which is not considered a reliable source. Moreover, it is among the most significant cyber attacks and deception sources.

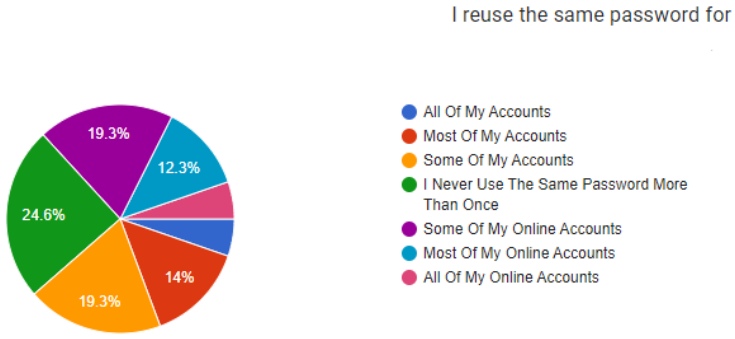
Examples:

One of the students replied that it had not been **hacked in the past and would not be hacked in the Future**. Upon reaching the e-mail question, he said he would click the **link without checking.**

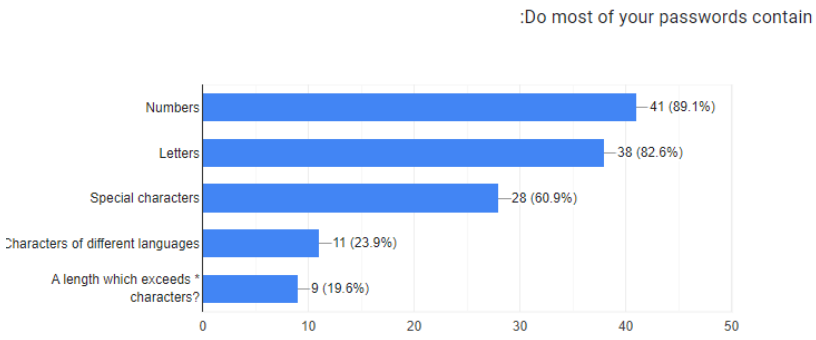
He also replied that he needed to learn what two-factor authentication was. Moreover, when I ask how you can be sure, he says that is what I think! Just because you have not discovered a hack does not necessarily mean you are not. This indicates ignorance in the field of information security. Another example is the question of passwords. One of the students uses the password in all his accounts and his personal information in the password. In the theoretical section, I explained the seriousness of such situations.

Another student was hacked before and is still using the same old methods without looking to develop himself and raise his level of information security.

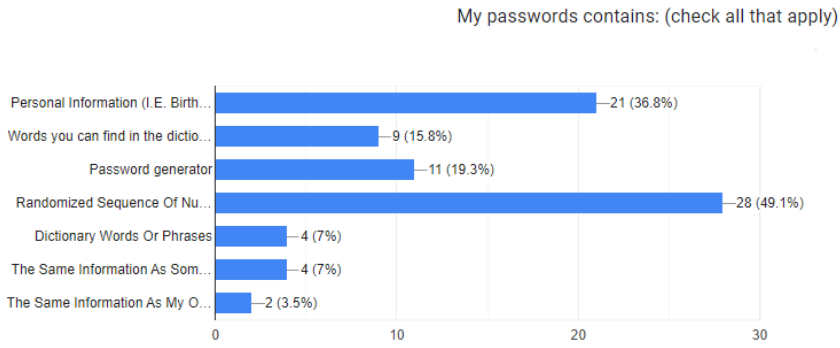


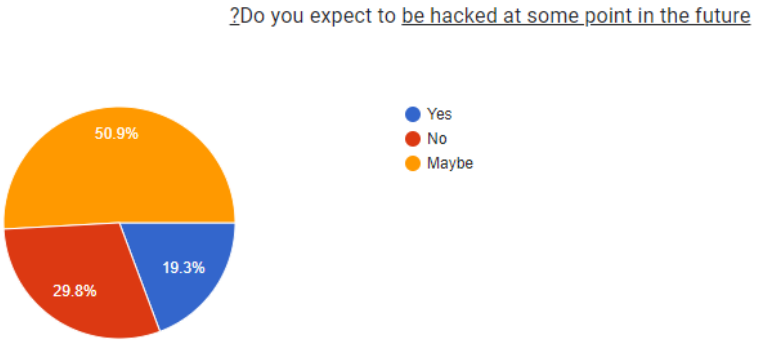


Source: Own Illustration



Source: Own Illustration





Source: Own Illustration

5.3 Conclusion

The thesis discusses several key concepts in cybersecurity and guides how individuals and organizations can protect themselves against cyber threats. It also highlights the availability of free tools and websites that can be used to increase security and protection, as well as the importance of obtaining information from reliable and accurate sources. Furthermore, the article explores the impact of media and communication on information security, emphasizing the need to stay informed about best practices and emerging threats, so individuals and organizations can better safeguard their valuable information and maintain the integrity of their digital assets.

Despite students' extensive use of technology for entertainment, work, or study, research shows a need for more experience and knowledge in information security. Addressing this knowledge gap requires providing a curriculum for information security education, increasing education and awareness on this subject, and guiding an individual on obtaining information and support from correct sources.

Safeguarding personal and confidential data from unauthorized access, theft, or manipulation by cybercriminals is paramount. Cybersecurity measures are necessary to prevent identity theft, financial fraud, and other malicious activities. Individuals store a significant volume of personal information such as banking details, credit card information, social security numbers, and passwords on their devices, making it crucial to implement adequate measures to protect this information.

Cybersecurity measures also prevent cyber-attacks from compromising individuals' devices, leading to data loss, privacy invasion, and potential harm to their reputation. To ensure adequate protection, individuals should exercise caution when providing personal information online, use strong passwords, and employ security tools such as firewalls, anti-virus software, and two-factor authentication. Awareness of the risks associated with phishing emails, suspicious phone calls, and unusual activities or transactions is also crucial, and incidents should be reported immediately to relevant agencies. Cybersecurity is Essential for protecting critical infrastructure from cyber-attacks that could severely affect society. Cybersecurity plays a crucial role in preserving the confidentiality and security of data, ensuring its accessibility when needed, and mitigating a wide range of cyber threats. Moreover, combine more than one protection method to get the best results.

Further research could explore the impact of cyber risks through artificial intelligence and machine learning and the psychological and physical effects of electronic attacks. Prioritizing cybersecurity and implementing adequate security measures is crucial for safeguarding personal information and maintaining its integrity and reliability. Our study has revealed a concerning lack of experience and knowledge in information security among students who interact with technology daily, whether for entertainment, work, or study. This knowledge gap highlights the need to provide a curriculum for information security education, focusing on increasing education and awareness on this subject.

7 References

Abbas Moallem. 2019. *Cybersecurity Awareness Among Students and Faculty.* 2019.
Abeerah Hashim. 2022. 6 times when hackers forced companies to go bankrupt and shut down. [Online] 2022. https://privacysavvy.com/security/business/6-times-hackers-forced-companies-to-go-bankrupt-shut-down/.
Alex Tarter. 2019. *Importance of Cyber Security.* 2019.
Amber Steel. 2019 . Passwords Are Still a Problem According to the 2019 Verizon Data Breach Investigations Report. [Online] 2019 . https://blog.lastpass.com/2019/05/passwords-still-problem-according-2019-verizon-data-breach-investigations-report/#:~:text=80%25%20of%20hacking%2Drelated%20breaches%20still%20tied%20to%20passwords&text=The%202019%20DBIR%20confirmed%20that,the%20use%20of%.
Andreea Popa. 2021. Social engineering attacks: 12 famous cases you probably forgot. [Online] 2021. https://attacksimulator.com/blog/social-engineering-attacks-famous-cases/.
Bergal, Jenni. 2021. Florida Hack Exposes Danger to Water Systems. [Online] 2021. https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems.
ccleaner.com. [Online] ccleaner.com.
—. [Online]
Christopher Hadnagy. 2018. *Social Engineering: The Science of Human Hacking.* 2018.
Cloudflare.com. 2022. What are cookies? | Cookies definition. [Online] 2022. https://www.cloudflare.com/learning/privacy/what-are-cookies/.
Dagher, Kate. 2022. Signs and Risks of Using Outdated Systems. [Online] 2022. https://fellow.app/blog/engineering/signs-and-risks-of-using-outdated-systems/#:~:text=using%20outdated%20systems-,What%20is%20an%20outdated%20system%3F,to%20get%20the%20job%20done..
Eset. 2022. 8 Reasons to Keep Your Social Media Set to Private. [Online] 2022. https://www.eset.com/uk/about/newsroom/blog/8-reasons-to-keep-your-social-media-set-to-private/#:~:text=Avoid%20identity%20theft,%20share%20too%20much%20information%20online..
GDPR.EU. 2020. Complete guide to GDPR compliance. [Online] 2020. https://gdpr.eu/.
Givaudan. 2023. Tip 5: Don’t click on links or open attachments in messages where the source doesn’t seem trustful. [Online] 2023. https://www.givaudan.com/specials/infosec/tip-05.
Guardian staff . 2021. US invokes emergency powers after cyber-attack on fuel pipeline. [Online] 2021. https://www.theguardian.com/us-news/2021/may/10/us-invokes-emergency-powers-after-cyberattack-shuts-crucial-fuel-pipeline.
https://keepass.info/. [Online] https://keepass.info/ .
—. [Online] https://keepass.info/.
—. [Online]
—. [Online]
https://letsencrypt.org/. [Online] https://letsencrypt.org/ .
—. [Online]
https://openvpn.net/. [Online] https://openvpn.net/ .
—. [Online]
https://www.avast.com/free-antivirus-download#pc. [Online] https://www.avast.com/free-antivirus-download#pc.
—. [Online]
https://www.clamav.net/. [Online] https://www.clamav.net/.
—. [Online]

https://www.malwarebytes.com/. [Online] https://www.malwarebytes.com/.
—. [Online]
https://www.openssl.org/source/. [Online] https://www.openssl.org/source/.
https://www.ossec.net/. [Online] https://www.ossec.net/.
—. [Online]
https://www.safer-networking.org/. [Online] https://www.safer-networking.org/.
—. [Online]
https://www.snort.org/. [Online] https://www.snort.org/.
—. [Online] https://www.snort.org/.
https://www.torproject.org/. [Online] https://www.torproject.org/ .
—. [Online] https://www.torproject.org/.
https://www.veracrypt.fr/code/VeraCrypt/. [Online]
https://www.veracrypt.fr/code/VeraCrypt/.
—. [Online]
—. [Online]
https://www.wireshark.org/. [Online] https://www.wireshark.org/ .
—. [Online]
Kaspersky. 2022. Top 10 Internet Safety Rules & What Not to Do Online. [Online] 2022. https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online.
—. 2023. What is Cyber Security? [Online] 2023. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.
kaspersky.com. 2022. Why You Need Backup Files. [Online] 2022. https://www.kaspersky.com/resource-center/preemptive-safety/backup-files.
Kevin James. 2023. Cybersecurity Education: Importance In The Education Sector For 2023. [Online] 2023. https://cybersecurityforme.com/importance-of-cybersecurity-in-education/#:~:text=Cybersecurity%20awareness%20training%20is%20important,ransomware%2C%20and%20other%20computer%20threats.
Maile McCann. 2023. What Is A VPN Used For? 9 VPN Uses In 2023. [Online] 2023. https://www.forbes.com/advisor/business/software/why-use-a-vpn/#:~:text=Having%20a%20VPN%20protects%20your,for%20one%20reason%20or%20another..
Malwarebytes. 2023. Social engineering. [Online] 2023. https://www.malwarebytes.com/social-engineering.
—. 2023. What is phishing? [Online] 2023. https://www.malwarebytes.com/phishing.
ncsc.gov.uk. 2019. What is an antivirus product? Do I need one? [Online] 2019. https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product#:~:text=Once%20it's%20on%20your%20computer,protect%20your%20data%20and%20devices..
NEWS WIRES. 2020. WikiLeaks releases 250,000 US diplomatic cables. [Online] 2020. https://www.france24.com/en/20101128-wikileaks-documents-leaked-usa-european-media-cables-embassies-diplomacy-washington.
NICOLE WETSMAN. 2020. Woman dies during a ransomware attack on a German hospital / It could be the first death directly linked to a cybersecurity attack. [Online] 2020. https://www.theverge.com/2020/9/17/21443851/death-ransomware-attack-hospital-germany-cybersecurity.
NOS News. 2019. 'The Netherlands helped with hack attack on Iranian nuclear program'. [Online] 2019. https://nos.nl/artikel/2300067-nederland-hielp-bij-hackaanval-op-iraans-atoomprogramma.

Sam Biddle. 2018. FACEBOOK USES ARTIFICIAL INTELLIGENCE TO PREDICT YOUR FUTURE ACTIONS FOR ADVERTISERS, SAYS CONFIDENTIAL DOCUMENT. [Online] 2018. https://theintercept.com/2018/04/13/facebook-advertising-data-artificial-intelligence-ai/.
Sam Shead. 2022. Hackers can bring ships and planes to a grinding halt. And it could become much more common. [Online] 2022. https://www.cnbc.com/2022/06/27/hackers-can-now-bring-cargo-ships-and-planes-to-a-grinding-halt.html.
Sheera Frenkel. 2021. A Brazen Online Attack Targets V.I.P. Twitter Users in a Bitcoin Scam. [Online] 2021. https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html.
Titanfile.com. 2022. Top Cybersecurity Tips in 2022. [Online] 2022. https://www.titanfile.com/blog/cyber-security-tips-best-practices/.
Trendmicro. 2023. Denial of Service (DOS). [Online] 2023.
Vigliarolo, Brandon. 2023. Sensitive DoD emails exposed by unsecured Azure server. [Online] 2023. https://www.theregister.com/2023/02/23/azure_dod_emails_exposed/?fbclid=IwAR16RrFBlF0s8EwTpTqzy8AwCwDiXbW2oz9oYzmE-TS2DvS4Kcr3ZgfvEKg.
Whatismyipaddress. 2019. What Makes a Network Unsecure? [Online] 2019. https://whatismyipaddress.com/unsecured-network-2.

8 List of pictures, tables, graphs, and abbreviations

8.1 List of abbreviations

- CULS - Czech University of Life Sciences in Prague.
- DDoS - Denial of service.
- TB - Terabyte
- GDPR - The General Data Protection Regulation.
- 2FA- two-factor authentication.
- HTTP - Hypertext Transfer Protocol Secure
- MiM - Man-in-the-Middle.
- VPN - virtual private network.
- FEM - Faculty of Economics and Management.
- US - United States.
- FBI - Federal Bureau of Investigation.
- SSL - Secure Sockets Layer.
- TLS-Transport Layer Security.