TeleGrow

Enhancing the Teleworking Digital Skills for the Middle aged employees

How to TeleGrow Training Modules: The Ultimate Teleworking Training for VET providers

CWEP

Module 6 - Online Safety Basics

Erasmus+

Project funded by: **Call 2020 Round 1 KA2 - Cooperation for innovation and the exchange of good practices/ KA226 - Partnerships for Digital Education Readiness**

Index

1. Introduction to the topic

During these difficult times, people are all trying to adjust to the new era of working from home without the mandatory knowledge of the amount of risks and threats it carries, not only for the people aged 50+, to whom the TeleGrow project is addressed, but to workers of all ages. A 2020 European Commission report states that about 40 percent of EU workers have started working remotely since the COVID-19 pandemic, which is an almost 8x increase compared to the year before it began. This rapid increase in teleworking makes it hard for businesses to implement new and strong security measures, which opens a window for various malicious practices. With the increase of cybercrime activities by over 600% since the start of the pandemic, it is easy to conclude that people aged 50+ who have had little to no experience with teleworking are particularly vulnerable to the dangers it can bring. These dangers involve things such as identity theft, data breaches, malicious software (malware) and viruses, banking frauds, and many more threats that older people might not be well prepared for.

This module is designed to function as a brief introduction to the topic of online security. It will include descriptions of the most common dangers of teleworking and general Internet usage that the TeleGrow project target groups can face. That part of the module will help to understand what spam and phishing are, how to recognize them, and what dangers they may bring. Other common practices, such as hacking, ransomware, or identity theft will also be thoroughly and explained. The module will also explain what measures should be taken to secure private Internet connection and familiarize the learner with the General Data Protection Regulation. Finally, this TeleGrow project module will also include a brief set of exercises for its learners, to test their knowledge acquired throughout this module.

2. Learning objectives

Upon the completion of this module, the learner will:

- be taught about spam and phishing and how to recognize them
- understand what hacking is, how ransomware works and how to protect themselves from identity theft and the consequences they carry
- know what measures to take to secure theirs Internet connection and what is the difference between a weak and a strong password
- acquire knowledge about the General Data Protection Regulation and the ways to protect personal information
- be able to establish a safe work-from-home environment with the use of practical activity at the end of the module

3. Learning contents

Chapter 1 – Spam and Phishing

The word "spam" refers to any unwanted digital messages people receive that were sent to a large group of recipients. This process is most often done by things called "spambots", which are automated programs used to send spam messages to email accounts, social networking sites, or forums. Even though spam may seem like a relatively new problem, its history dates back to 1978, when Gary Thuerk wanted to promote his product by sending unsolicited e-mail to thousands of people, which supposedly generated about $12 million in revenue.

Today's usage of spam messages remains mostly the same, as it is used to generate a profit by promoting something. Generally, the products it advertises are of questionable quality, and the subjects that spam messages advertise most of the time are:

- pharmaceuticals
- adult content
- financial services
- online gambling
- cryptocurrencies

Source: freepik.com

In 2020, around 50% of all e-mails received were spam. The people that create and send spam messages prey on inexperienced Internet users, and opening such e-mails may have very unpleasant consequences, such as sharing private information with unauthorized people or ending up on the mailing lists of various sellers, which will lead to even more unwanted e-mails piling up in someone's mailbox. Even though the numbers might seem overwhelming, people rarely see spam messages in their mailboxes nowadays. This is caused by the rapid development in the area of spam filtering. The statistics revealed by Google in April 2020 showed that they were successfully able to block and filter 99.9% of spam email. This means that today's Internet users, along with 50+ aged people, are much safer from receiving these kinds of messages. This does not mean that the filtering is working flawlessly; there are still spam emails that get through, and to be able to filter them out by themselves, Internet users should know what type of message they should avoid opening. Some of the most common types of spam are:

- Email spoofing

  These kinds of messages try to mimic the sender by forging the same exact e-mail as they have and tricking the receiver into thinking that the email comes from a person or website they can trust. It will often request someone to take some kind of action, which can be either a payment request of an outstanding invoice, validating/unblocking an account, or verification of a purchase, and provide a link that, once clicked, can be used to steal the receiver's personal information. Thankfully, many e-mail providers will warn the user about the risk of being "spoofed" beforehand.

- Advance-fee scams

  Sometimes referred to as the "Nigerian prince scam", one of the ideas behind this is that the sender promises a large sum of money but only if the receiver provides a small loan in advance. This loan is usually said to be required for some sort of legal matter that will unlock the larger sum. The other type of advance fee scam

works in a similar way, but in this case, the sender poses as a close friend or family member of the receiver who needs money due to some sort of emergency.

- Advertisements and malware spam

Advertisement spam is simply an unsolicited message offering some type of product. While these offers may sometimes be true, in many cases, the product either does not exist or will not work. Malware spam is a type of message that contains various kinds of malicious content that is hidden behind links or attachments provided in the message. Once the person downloads and opens the file attached or downloaded through the link, the malicious scripts will run and infect the computer with different types of dangerous malware.

Source: freepik.com

- Phising

Similar to email spoofing but more complex cybercrime is phishing. This malicious practice is used in the context of fraud, espionage, or to set up cyberattacks aimed at various organizations. It involves faking emails or telephone calls and claiming to be from a legitimate source to persuade individuals to reveal their personal or financial information, often with no particular target. Spear phishing messages are also sent from forged e-mails appearing to be trustworthy, but in this case, the cybercriminal collects information about the victim from different sources, such as social media

public posts, sites on which the victim's e-mail is registered, profiles of the victim's friends on social media, or information about employees on the company website.

The hacker can then gather all the information about that person and prepare a personalized message, to which the receiver can fall victim. These emails often contain malicious links but can also be used to form a connection between the criminal and the victim to gain trust and steal sensitive information. Sometimes, spear phishing attacks target any senior executives within a company to trick them into revealing their personal information or valuable company data, which can later be used for malicious purposes. To be less prone to falling for phishing attempts, Internet users should pay special attention to and avoid opening:

- Emails about winning a big prize
- Fake websites closely resembling the original ones
- Threats concerning account deactivation or losing access to it
- Messages about fake malware infection
- COVID-19 themed emails
- Fake relatives asking for money
- Poor grammar and misspelled words in supposedly formal emails

Even though the filters for malicious content delivered by most e-mail providers offer strong protection against spam and phishing, people should keep in mind that it is not flawless and there are certain countermeasures that they can take to even more reduce the chances of having their personal data stolen. To further accomplish this, people should always copy and paste the content of a suspicious message into a search engine (e.g., Google) as there is a chance that it has been reported as a phishing attempt before. Another good practice is to contact the company that supposedly sent the suspicious message without clicking the links or attachments that were inside it. A good idea would also be to install spam filters and anti-phishing toolbars on a computer, as those tools can protect the user from such messages by themselves. In a working environment, employees should try to verbally confirm any requests sent to them via e-mail and change their passwords on a regular basis.

Chapter 2 – Hacking, Ransomware, Identity theft

Due to the recent increase in teleworking and the necessity to stay at home and handle a lot of errands online because of the COVID-19 pandemic, the world is also witnessing an enormous increase in cybercrimes. These can be defined as any illegal activities done by using a computer and are often associated with people called "hackers" or "cybercriminals", who can be divided into many different categories depending on what they want to achieve and how skilled they are.

Source: freepik.com

Hacking is the process of identifying security flaws in a computer system or network in order to gain access to personal or business data. The use of a password deciphering algorithm to gain access to a computer system is an example of computer hacking. Although it is often considered a malicious practice, sometimes it is legal and used with good intentions, mainly to improve online security and secure valuable data inside a certain organization. Such a practice is called "ethical hacking". Usual hacking covers a broad spectrum of malicious practices, starting with slowing down other people's computers, through stealing credit card info, and ending with large-scale intimidation and ransom demands. As mentioned in Chapter 1, hackers can gain access to other people's devices through phishing attempts and malware contained in

suspicious spam messages, but these are not the only methods they use. A common hacking technique to which many people may be prone to is creating a fake Wi-Fi access point in a public place, which once connected to, will redirect the victim to a website which may steal their personal information. To prevent this from happening, people should avoid using public Wi-Fi networks and always be careful when using their devices in places like restaurants, airports, malls, or parks.

Another form of malicious software that may be very dangerous for people aged 50+ who are just starting to telework is **ransomware.** It has proved to be very dangerous as it is not only one of the most concerning Internet security problems today, but it is also very common. This malware encrypts files and documents on anything from a single computer to a whole network, including servers. After the ransomware attack, the victim is left with instructions for paying a ransom to unlock the files; or else, the valuable data will be made public or sold to other cybercriminals, hence the name "ransomware".

This and other malwares, are most commonly spread through attachments in phishing spam messages, which is why it is critical to treat any suspicious emails with extreme caution. Ransomware attacks are highly dangerous because, if successful, they can expose valuable, private information of thousands of employees if aimed at a specific company.

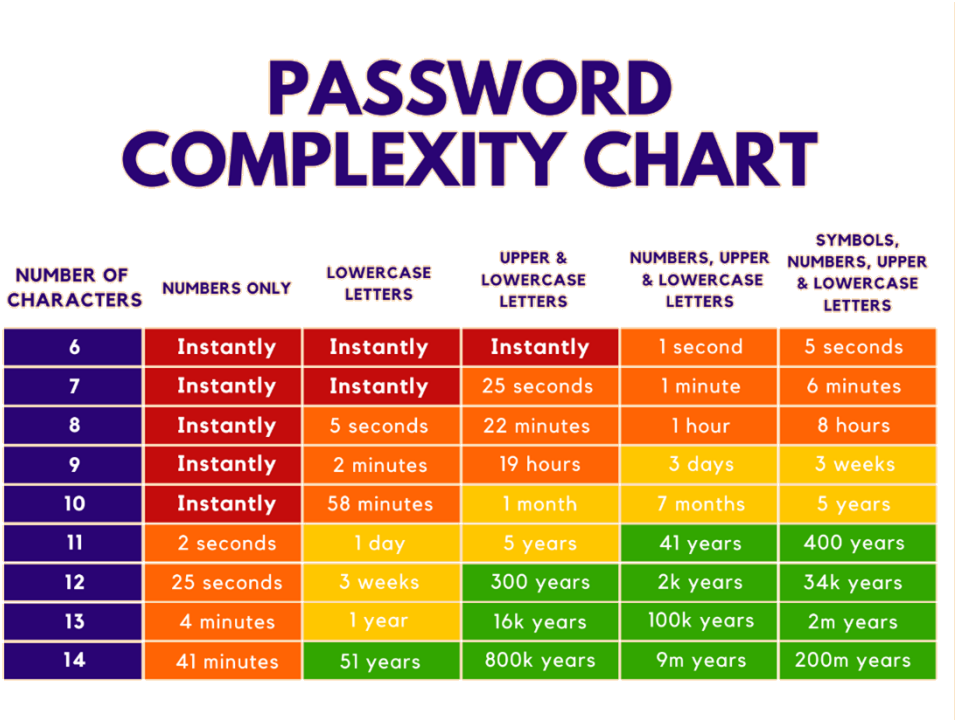
Source: freepik.com

One of the fastest growing forms of cybercrime is identity theft. The criminal steals personal data, such as credentials, bank account details, birthdates, etc. in order to impersonate the victim and use that information to gain monetary profit and cause further harm to people. The methods that hackers use to do that are similar to other cybercrimes. They can acquire this valuable data through phishing attempts or hacking into computers using various malware and fake or badly secured public Wi-Fi access points. Later, they can use the data to obtain loans, buy various things, or even commit crimes on behalf of the victim's name. It is good to regularly check credit reports and look for any inaccuracies or bank transfers that might seem suspicious. The sum of money missing does not necessarily have to be big, because the thief may be stealing from thousands of people at the same time. Identity theft victims should, as soon as possible, report this crime to the authorities, freeze their bank accounts, and open new ones. If it is possible, the victims should contact banks, debt collectors, and other places they know the thief used their personal information. It is also important to contact relatives, employers, and colleagues from the currently employed company, because the thief might be in possession of their information as well.

The techniques used by hackers in order to steal or bring chaos into people's lives are getting more and more sophisticated. Keeping that in mind, people must know how to protect themselves to minimize the chances of being one of the victims of cybercrimes. There is one certain protective countermeasure that, once implemented, reduces the risk of dealing with cybercriminals.

Create a strong password. This is crucial to keeping valuable data secure. A good password is not obvious but is easy to remember. It should not be shorter than 12 characters, because it takes seconds to crack short passwords with today's technology. A strong password should include unique symbols such as numbers and lower-case or upper-case letters, as this will add an extra layer of security to it. It is important to make it strong and hard to forget. A common technique for creating strong passwords is by creating an acronym from a favorite quote or a phrase that is memorable and adding a few special symbols to it. Another good practice is to use

password managers. Those programs generate and store a user's passwords in one safely encrypted account. One more crucial thing is to keep passwords private and never send them to anybody by e-mail or text message. With the data gathered, presented below chart shows how effortles it is for a hacker to break a password that may seem complex for its user.



PASSWORD COMPLEXITY CHART

NUMBER OF CHARACTERS	NUMBERS ONLY	LOWERCASE LETTERS	UPPER & LOWERCASE LETTERS	NUMBERS, UPPER & LOWERCASE LETTERS	SYMBOLS, NUMBERS, UPPER & LOWERCASE LETTERS
6	Instantly	Instantly	Instantly	1 second	5 seconds
7	Instantly	Instantly	25 seconds	1 minute	6 minutes
8	Instantly	5 seconds	22 minutes	1 hour	8 hours
9	Instantly	2 minutes	19 hours	3 days	3 weeks
10	Instantly	58 minutes	1 month	7 months	5 years
11	2 seconds	1 day	5 years	41 years	400 years
12	25 seconds	3 weeks	300 years	2k years	34k years
13	4 minutes	1 year	16k years	100k years	2m years
14	41 minutes	51 years	800k years	9m years	200m years

Data gathered at: https://www.security.org/how-secure-is-my-password/

From the data gathered, it is easy to confirm what has been stated earlier. 12 characters long password should be a minimum for optimal security and it does not even have to be really complex. To make it unbreakable for at least 300 years, all it takes is a password with lower and uppercase letters. It should be noted, that **it is strictly unadvised to put own name as a password** as it can be easily cracked, no matter the length.

Chapter 3 – Secure Internet Connection

It is well known that the internet is a reliable but dangerous source of information and entertainment. Because of the amount of malware, spies, and hackers just waiting for a good opportunity to attack, it is crucial to know how to defend against it, because sometimes, a good password is not enough. There are plenty of ways which can bolster the security of an internet connection, and a lot of them do not require advanced technological knowledge.

For a start, it would be advised to implement **two-factor authentication** (2FA) whenever it is possible. This alone can deter most hackers from breaking into someone's account. It works as second layer of verification when logging into an account, while one is usually a password, the latter is often a unique key sent to the user's cellphone number which must be entered after logging with a password. It is considered a really strong method of protecting users from the danger of their passwords being stolen as the uniquity of the key makes is much harder for a hacker to break into an account.

Another good practice is to use a **Virtual Private Network (VPN)**. Every time someone connects to a network, a stream of data is being exchanged between the user and servers. VPN creates a secure connection between these two parties by encrypting the data before it is sent or received by users. A VPN hides the user's IP address and location so the cybercriminals can no longer discover their potential victims' locations because, thanks to the VPN, it would track them to the location of the VPN server making it a lot harder to get a look into their data. It is a great tool to secure the connection while using public Wi-Fi networks in places like airports or restaurants which are easily hackable.

Source: freepik.com

To set up this kind of connection it is necessary to find a reliable VPN service provider and subscribe to it. There are a few providers on the market who offer their services for free but it is advised to acquire a paid subscription as it offers more features for a safer connection. Once a preferred VPN provider is found, the user will be prompted to download the necessary software. It must be always downloaded directly from the provider's website as downloading from a different source may result in downloading files that contain malware. Most VPN apps are available on a vast variety of devices and their set-up process is accessible for everyone. Once an app is downloaded, and the account is created all that is left to do is to activate it and become less concerned about someone hacking into our device.

Changing the default router name and password might also help to safeguard the network. Every router comes with a generic name and password, which are needed to set them up for the first time. Right after that, a good practice is to change its name and password to something unique, keeping in mind the guidelines for creating a strong password. It is so, because router names (SSID – service set identifier) most often contain the brand and the model in their names, which makes it easier for hackers to find routers they know are vulnerable to breaches. It is also possible to

completely hide the SSID of a router, so that the chances of a hacker finding out about the connection are close to zero.

Source: freepik.com

Keep everything updated. Updating usually seems like an unnecessary hassle, and sometimes can even make a device function worse than before, by adding new features that are not needed or by removing ones that were useful. It is important to pay attention to any update notifications that may appear. Any software is not without flaws. Most of them contain hidden vulnerabilities that even the developers were not aware of at the beginning. Once found, these can be exploited by hackers. Which is the reason why every piece of software needs its newer versions that have fixes in the vulnerable places. This is very important from the online security point of view, as keeping everything updated also reduces the chances of a successful hacker attack. Users that keep an eye on updating their software regularly decrease the chances of a cyberattack aimed at their devices, as it is possible that the older vulnerabilities that could be used by hackers are already fixed. There is a chance that updating might break certain functions of the software, or even make it unusable on some devices, which is why, once after updating, it is good practice to check whether the update did not break anything. Besides that, software that is not updated can miss the newer functions that are very convenient. On the other hand, the older versions of the software can just stop working on newer devices or those that are kept up to date. Even though updating things can seem a little time-consuming, it is very important,

not only for security reasons but also for the sake of having all the latest functions of a certain device or software. A good practice would be to do a weekly check of the software used in terms of updating it. This is a really fast and simple way to keep the data more secure and bolster the performance of the software used.

Antivirus software is a must, and it should be installed on every device. It is not hard to fall victim to a phishing attack, and nowadays, with the growing popularity of working remotely, infecting a computer with a virus can cause a compulsory break from work for days or even weeks. An antivirus is a kind of software that checks every file or piece of data that is currently installed or is being installed on a computer. It is made to determine whether any of the files on a computer could be a potential threat or cause any damage to the users and their devices. The antivirus works in two different ways. One of which is a **signature-based** method that works as a list of known files containing malware that are published by antivirus companies. Once a match is found between the file on the list and on the user's device, it's blocked. This is a common method which works well, as there are thousands of malware discovered every day, so the list is really data-rich. The only downside to this method is that once the user's device is infected with a virus that is not on the list, then it might not be protected from it. The other way in which the antiviruses protect the devices is **behavior-based**. This one is more complex and it is not as commonly used as the other methods, and only the most advanced antiviruses use it. As the name suggests, this method studies the behavior of a certain file and makes a judgement on whether this file may be dangerous to the device. It checks for any attempts to modify or encrypt the data on the device and then blocks it because it flags it as a virus.

Source: freepik.com

Antiviruses protect users not only by blocking the files that are on their devices, but most of them also block users from entering unauthorized sites that can cause possible threats to their devices. Some of these programs can also clean so-called "junk files" to free some space on the device. This procedure can sometimes also boost the processing speed of a computer or smartphone. Antivirus is a crucial component of every device that is prone to getting infected with malicious data, and it offers a wide array of advantages that act as a closed door that does not let any viruses inside and turns any existing ones out.

With all of these suggestions in place, it is extremely rare that someone will become a victim of a cyberattack, and even if someone attempts to steal the data from someone’s computer, it is extremely improbable that they'll succeed.

Chapter 4 – GDPR and Personal information Safety

The General Data Protection Regulation (GDPR), which came into force on May 25th, 2018, had its origins back in the 1950s. It was then that the Convention on Human Rights was created, laying the first foundations for the protection of personal data. Three decades later, with the rise of computers, the Data Protection Convention was created, declaring that privacy was, in fact, a human right. On October 24th, 1995, the Data Protection Directive came into being to regulate the data protection laws and the transfer of personal data outside of the Union. 17 years later, an update to these regulations was proposed and, after 4 years from that proposal, the General Data Protection Regulation was adopted by the European Parliament to become fully enforceable throughout the European Union just two years later, in May of 2018.

Source: freepik.com

The core of the GDPR is to give the EU citizens more control over their personal data. It is a massive set of 99 articles regulating the data protection rules and the way the data can be accessed. It has replaced the previous Data Protection Directive from 1995 because of the fact that the technological environment looked significantly different than it does now. Nowadays, almost every European citizen owns at least one smartphone, and businesses offering goods or services online have become as popular as their traditional equivalents. With the GDPR, it is easier to control what personal

information can be stored, shared, or collected by various parties. This information may vary from IP addresses, through monthly income information, to a person's eating habits.

Within the GDPR, there are 7 core principles that should be used as a guide on how user's data should be managed. These rules can be perceived as a framework designed to show the main purpose of the regulation. Amongst these 7 rules are:

- Lawfulness, fairness and transparency.

Meaning that the data must be stored and processed in a legal manner. It should not mislead other users as to how it is stored and how it is used.

- Purpose limitation.

Suggests that the personal data shall be collected and stored for clear, unambiguous, and legal purposes and not further processed in a way that is contradictory to those purposes.

- Accuracy.

It means that all reasonable measures must be taken to ensure that any personal data that is inaccurate, is immediately erased or corrected. Personal data should be accurate and, when required, kept up-to-date.

- Data minimization.

Organizations should not collect more data than they need from their users. It should be adequate and limited to what is necessary regarding the purposes for which it is processed.

- Storage limitation.

Means, that the data should not be stored for longer than necessary.

- Integrity and confidentiality.

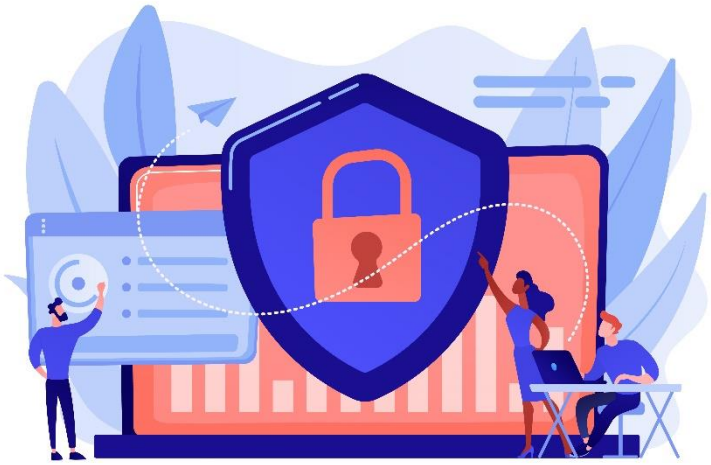
In other words, it is the security of the stored data. It should be processed with adequate technical or organizational measures to ensure the best security of the personal data, including protection against unauthorized or unlawful processing and against unintentional loss, destruction, or damage.

- Accountability.

This means that the companies should provide evidence that they follow the rules listed above and ensure that they take measures to handle the personal data in an ethical manner.

The GDPR was designed to protect the users and their data. Keeping that in mind, they provided **eight rights** for individuals. The most significant being:

- The right to information on the gathering and use of their personal data.
- The right to access, review and receive a copy of their personal data that is being gathered and processed by certain parties.
- The right to have their personal data erased.



Source: freepik.com

The other five rights of individuals are: the right to rectification, the right to restrict processing, the right to data portability, the right to object, and the right to not be subject to automated decision making.

Due to the growing awareness of the value of personal information, people have started to pay more attention to how much data they give to companies, and prefer to choose those parties that are transparent about the data collection. Due to the GDPR, companies need to be more aware about what data they collect and how they secure it due to the high fines associated with noncompliance with the GDPR regulations.

Knowledge about the GDPR along with the other practices mentioned in this guide can not only ensure the high level of security of the user's personal information, but also make it harder for cybercriminals to breach their way into companies' databases. Strong passwords and knowledge about various malicious practices such as phishing and viruses, if applied and understood correctly, can make people working remotely feel much safer during these times in which teleworking has become a worldwide common practice.

Chapter 5 – Practical Activity

Practice 1. Creating a password that's strong and memorable.

A strong password is long, complicated, and contains a lot of symbols, but it is also easy to remember. With that in mind, let's create one using these few simple steps:

1. Think about a sentence or a quote that you often think about. For example, a famous Wayne Gretzky quote:
   You miss 100 percent of the shots you don't take.
2. Now, make an acronym from that quote:
   Y(ou) **m**(iss) **100 p**(ercent) **o**(f) **t**(he) **s**(hots) **y**(ou) **d**('ont) **t**(ake) = Ym100potsynt
3. Now, add special characters to it. For example, let's swap "1" with "!", "p" with "%", add an underscore and change the letter case, so the final effect will look like this:
   Ym!00%ots_Ydt

The password looks complicated but if we analyze it, we can see it is quite simple and easy to remember. A good practice is to train writing it for some time, so our muscle memory will remember the order of the buttons pressed.

Source: freepik.com

Practice 2. Check your mailbox for SPAM and possible phishing attempts.

We have learned about the various malicious e-mails that can be sent to us and how to recognize them.

Open your mailbox and check if there are any advertisements for products you've never heard of or notifications about winning some kind of prize. Also check for suspicious e-mails about unpaid invoices or account suspensions. Analyze them, but under any circumstances **DO NOT** open any links or attachments provided in the messages. Then, erase those messages and think about how many suspicious e-mails there were.

Useful links:

How secure is your password:
https://www.security.org/how-secure-is-my-password/

How to install a VPN connection:
https://www.businessnewsdaily.com/15710-how-to-install-a-vpn-connection.html

4. References

Anderson, S. (2022). *What Is Phishing? Guide with Examples for 2022*. SafetyDetectives. Retrieved May 10, 2022, from https://www.safetydetectives.com/blog/what-is-phishing-and-how-to-protect-against-...

Awati, R., & Teravainen, T. (2021). *What is email spam and how to fight it?* SearchSecurity. Retrieved May 9, 2022, from https://www.techtarget.com/searchsecurity/definition/spam?msclkid=9aeb4557cf8211ec82e6cfc07708ec54

Barracuda. (2020). *Spear Phishing: Top Threats and Trends* (Vol. 5). Barracuda. Retrieved May 10, 2022, from https://lp.barracuda.com/rs/326-BKC-432/images/BEU-AMER-Spear-Phishing-Vol5...

Castagna, R., & Lavery, T. (2021). *General Data Protection Regulation (GDPR)*. WhatIs.Com. Retrieved June 24, 2022, from https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR

Cheema, A. N., & Aamir, R. (2021). Trends of cyber crimes. *Proc. 18th International Conference on Statistical Sciences*, *35*, 261–269. https://www.researchgate.net/profile/Muhammad-Suhail-6/publication/353070981_Comparison_of_Ridge...

Chng, S., Han Yu, L., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*. https://doi.org/10.1016/s2451-9588(22)00018-5

Digital Marketing Experts – Editorial Review Board. (2021). *The Importance of Updating*. THAT! Company. Retrieved June 24, 2022, from https://www.thatcompany.com/the-importance-of-updating...

D'Mello, Y. (2018). *How did we get here? A brief history of the GDPR*. AiThority. Retrieved June 24, 2022, from https://aithority.com/technology/analytics/how-did-we-get-here-a-brief-history-of-the-gdpr/

Edwards, R. (2022). *How Can I Secure My Internet Connection?* SafeWise. Retrieved June 24, 2022, from https://www.safewise.com/online-security-faq/secure-internet-connection/

Elvin, A. E., Sundström, F., & von Heland, W. (2021). *Understanding the Effects of Cyber Security Risks and Threats on Forced Teleworking Organizations* (Master's dissertation). Department of Informatics, Lund School of Economics and Management, Lund University. Retrieved June 24, 2022, from https://lup.lub.lu.se/student-papers/search/publication/9052971

FIT Information Technology. (2022). *What is antivirus and why is it important?* Retrieved June 24, 2022, from https://it.fitnyc.edu/what-is-antivirus-and-why-is-it-important/

Fogg, S. (2022). *What is GDPR? The Basics of the EU's General Data Protection Regulation*. Termly. Retrieved June 24, 2022, from https://termly.io/resources/articles/what-is-gdpr/

Fruhlinger, J. (2020). *Ransomware explained: How it works and how to remove it*. CSO Online. Retrieved May 11, 2022, from https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it...

Gajić, A. (2022). *Spam Statistics*. 99firms. Retrieved May 9, 2022, from https://99firms.com/blog/spam-statistics/?msclkid=18264839cf8b11ec8144c5ced7add618

General Data Protection Regulation (GDPR) – Official Legal Text. (2019). General Data Protection Regulation (GDPR). Retrieved June 24, 2022, from https://gdpr-info.eu/

Gibson, K. (2022). *6 Famous Identity Theft Cases in Recent Years*. Home Security Heroes. Retrieved May 12, 2022, from https://www.homesecurityheroes.com/famous-identity-theft-cases/

Gupta, M. (2021). Identity Theft in Cyberspace in India. *International Journal of Research Publication and Reviews*, *2*(7), 1700–1701. https://www.ijrpr.com/uploads/V2ISSUE7/IJRPR791.pdf

Hiley, C. (2021). *Brief history of cybersecurity and hacking*. CyberNews. Retrieved May 11, 2022, from https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/?msclkid=ebaaa52cd10911ecbb48b6bc018d0384

Jančis, M. (2022). *How to create a good and strong password*. CyberNews. Retrieved June 16, 2022, from https://cybernews.com/best-password-managers/how-to-create-a-strong-password/

Janssen, D. (2022). *VPN Explained: How Does It Work? Why Would You Use It?* VPNoverview.Com. Retrieved June 1, 2022, from https://vpnoverview.com/vpn-information/what-is-a-vpn/

Johansen, A. G. (2018). *What to Do If Your Identity Is Stolen: 14 Steps*. LifeLock. Retrieved May 12, 2022, from https://www.lifelock.com/learn/identity-theft-resources/do-these-things-immediately-if-your-identity-has-been-stolen

Lopez, A. (2021). *Top 10 Reasons Why an Antivirus Is Important*. Business 2 Community. Retrieved June 24, 2022, from https://www.business2community.com/cybersecurity/top-10-reasons-why-an-antivirus-is-important...

Malwarebytes. (n.d.). *What is spam?* Retrieved May 11, 2022, from https://www.malwarebytes.com/spam...

Martens, B. (2021). *The Ultimate Internet Safety Guide for Seniors (2022)*. SafetyDetectives. Retrieved June 24, 2022, from https://www.safetydetectives.com/blog/the-ultimate-internet-safety-guide-for-seniors/?msclkid=9e7ed272cf5f11ecbe3d195abee11879

Milasi, S., González-Vázquez, I., & Fernández-Macías, E. (2020). *Telework in the EU before and after the COVID-19: Where we were, where we head to*. Joint Research Centre. Retrieved June 24, 2022, from https://joint-research-centre.ec.europa.eu/system/files/2021-06/...

Minahan, B. (2020). *How to Create a Strong Password in 6 Easy Steps*. aNetworks. Retrieved June 1, 2022, from https://www.anetworks.com/how-to-create-a-strong-password-2021/

Mitra, A. (2017). *What is a spambot and how to stop spambots?* TheSecurityBuddy. Retrieved May 11, 2022, from https://www.thesecuritybuddy.com/anti-spam/what-is-spambot-and-how-to-stop-spambots...

Molinaro, D. (2022). *How Does Two-Factor Authentication (2FA) Work?* Avast. Retrieved June 1, 2022, from https://www.avast.com/c-how-does-two-factor-authentication-work...

Movassagh, N. (2021). *Awareness and perception of phishing variants from Policing, Computing and Criminology students in Canterbury Christ Church University.* (Master's dissertation). Canterbury Christ Church University School of Law. https://repository.canterbury.ac.uk/item/8yq89/awareness-and-perception-of-phishing-variants-from-policing-computing-and-criminology-students...

Peterson, S. (2019). *The Ultimate Guide for Online Security and Privacy in 2020*. The Hack Post. Retrieved June 1, 2022, from https://thehackpost.com/the-ultimate-guide-for-online-security-and-privacy-in-2020.html

Proofpoint. (n.d.). *What is Email Spoofing? Definition & Examples*. Retrieved June 24, 2022, from https://www.proofpoint.com/us/threat-reference/email-spoofing?msclkid=df4910a2d03511ecb958bcffa531b6ab

Spoofing and Phishing. (2022). Federal Bureau of Investigation. Retrieved May 10, 2022, from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing?msclkid=8cb3cf19d04d11ecb7c47a9f8893c5e8

Tanwar, R., Choudhury, T., Zamani, M., Gupta, S., & Tajpour, A. (2021). Information Security and Optimization. In *Information Security and Optimization* (pp. 25–26). CRC Press. Retrieved May 10, 2022, from https://books.google.nl/books?id=...

TechFunnel Contributors. (2020). *Most Common Hacking Techniques for Beginners*. Techfunnel. Retrieved May 11, 2022, from https://www.techfunnel.com/information-technology/hacking-techniques/?msclkid=94348692d12111eca373f0ead6ff7fe9

Tschabitscher, H. (2021). *What Is an Example of Spam Email?* Lifewire. Retrieved May 9, 2022, from https://www.lifewire.com/what-and-why-spam-email-1173993#toc-what-are-some-examples-of-spam

Tsonchev, A. (2020). *Six of the biggest security threats facing the remote workforce*. TechRadar. Retrieved June 24, 2022, from https://www.techradar.com/news/six-of-the-biggest-security-threats-facing-the-remote-workforce?msclkid=9e80a80ccf5f11ec92c0ce7275373494

Williams, L. (2022). *What is Hacking? Types of Hackers | Introduction to Cybercrime*. Guru99. Retrieved June 24, 2022, from https://www.guru99.com/what-is-hacking-an-introduction...

Title page picture source: freepik.com