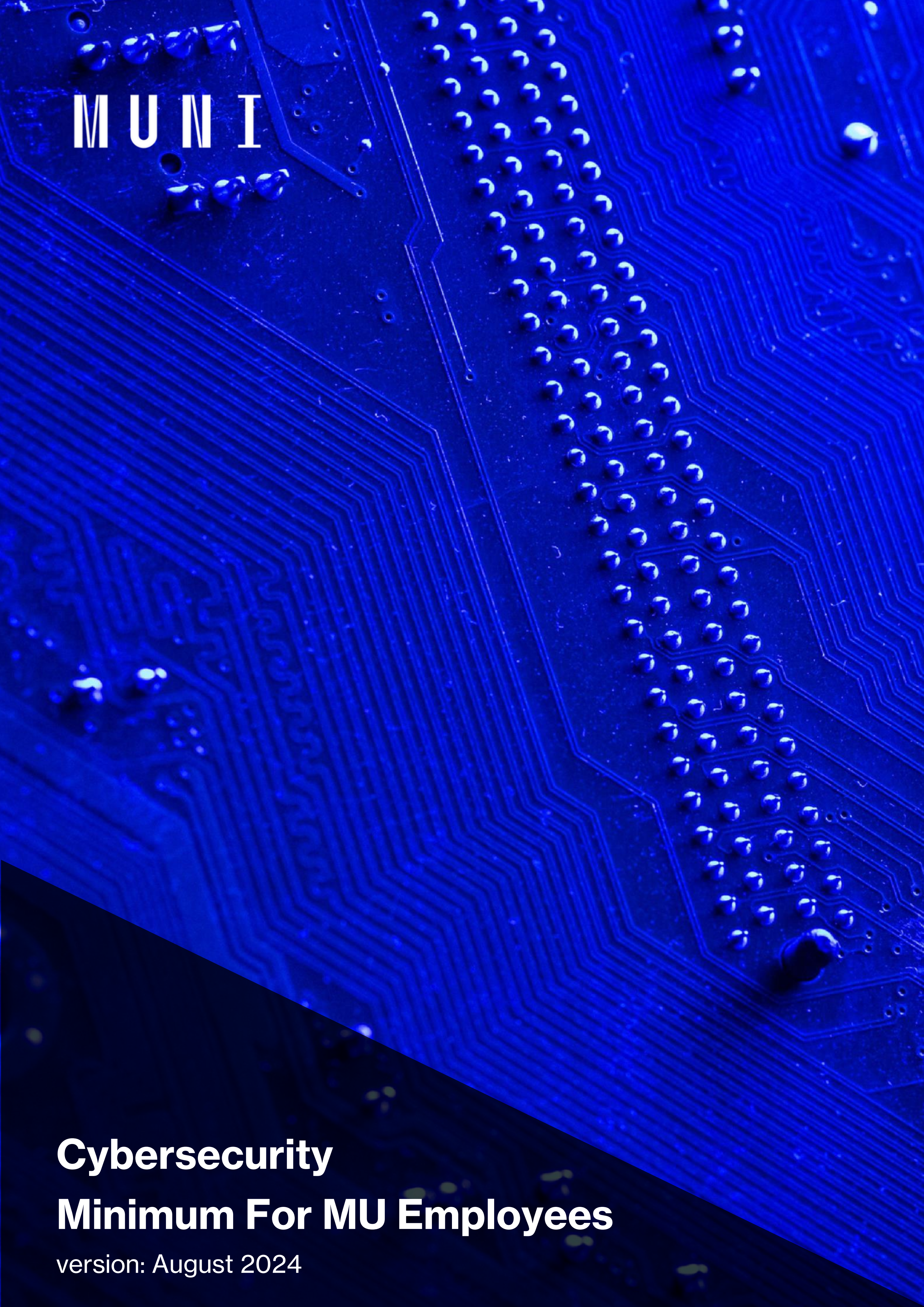

Cybersecurity Minimum For MU Employees

version: August 2024

Institutional training

This document serves as textual support for the **Cybersecurity Minimum for MU Employees**. A course designed to strengthen security habits among employees when navigating the online space. The course represents a compilation of fundamental security recommendations and specific measures for end-users, which need to be implemented not only due to legal obligations but also in consideration of increasing security demands in cyberspace. The training was created in connection with the obligations arising from Act 181/2014 Coll., on Cyber Security and Directive No. 10/2017, the use of information technology. The online training was created as a form of familiarization with these obligations, the content of which was created and guaranteed by the MU Cybersecurity Team[1].

Why another institutional training?

The Cyber Security Act No. 181/2014 Coll. (hereinafter referred to as "ACS") and related regulations impose a series of new obligations on institutions such as Masaryk University. One of these obligations is the necessity to train employees in the field of cyber and information security to strengthen their habits when operating in an online environment. In consideration of this, it is also necessary to periodically train employees, analogous to *Occupational Safety and Health* (OSH) training.

In Masaryk University's environment, users must primarily familiarize themselves with Directive No. 10/2017 on the Use of Information Technologies. This directive defines the basic framework regarding the rights and obligations of users of information technologies at Masaryk University. The directive includes not only definitions of fundamental concepts but also the rights and responsibilities of users when working with IT systems, software, and devices at MU.

To ensure that the obligation is not limited to a formal acquaintance with this directive, the Masaryk University Cybersecurity Team has created the content of this course. The training summarizes basic information and recommendations that should be implemented by the university employees. It includes not only general recommendations and content stipulated by law but also the specifics of Masaryk University in accordance with internal university regulations.

[1] https://csirt.muni.cz/en

Chapters

I. Work with Passwords

A password is one of the fundamental attributes of cyber security. Together with a username, it forms a basic protective mechanism for verifying and identifying a user.

To most university services, we log in using the **MUNI Unified Login**. Its main advantage is that you don‘t need to create and manage user accounts for each service separately – you only need to enter your **UČO** and **primary password**. The **primary password** is used precisely for logging in to services behind the unified login (INET MU, M365, etc.) and to the IS MU. A **secondary password** is also used at MU to log in to less critical services, such as Eduroam, centrally managed computers in classrooms.

Differences between passwords and instructions regarding their change or setup can be found on the IT MU website.

Passphrase

A passphrase consists of several memorable words (e.g., 3@pples&Or@nges#Ban@nas). A passphrase should contain: a minimum of 12 characters, numerals, uppercase letters, and special symbols (e.g., characters, punctuation marks). Its basis can be a part of a poem, a scene you see on the way to work, or perhaps a childhood memory.

It is not recommended to use passwords that contain **easily discoverable information**, such as your child's name or your date of birth. It is also not advisable to place digits or special symbols in predictable positions, such as a digit at the end of the line or replacing the letter O with the digit 0.

What if I use simple passwords?

If you use simple passwords, a **dictionary attack** is a technique where an attacker systematically tries various words and phrases from a pre-compiled dictionary (list) on login forms. The attacker exploits passwords based on common words, names, numbers, or phrases that are easily memorable. To create password combinations, they can use publicly available data, such as information from breached passwords that have appeared in data leaks.

Password Manager

Some studies show that people can remember up to **10 different passwords**. However, the number of accounts requiring a set password is much higher. This can lead to the use of the same or similar passwords for multiple accounts, increasing the risk of compromising other accounts if one password is breached. However, there is a solution to set unique passwords for each account without having to remember them all.

A password manager works as a database where individual passwords and usernames are stored and protected by encryption. The password manager operates on the principle of logging in through a single password, known as the **master password** or main password. This password should be really strong, as it protects all the accounts and login details stored in the password manager. The password manager also allows for generating passwords for newly created or used online accounts. Typically, it offers **browser extensions** that, once logged into the manager, enable automatic filling of login credentials.

> Storing passwords in a browser (such as Google Chrome or Mozilla Firefox) **should not be confused with using** a password manager. Managing passwords is not the primary function of browsers! For this reason, it is more appropriate to choose a tool that specializes in storing and managing passwords, so you can be sure that your passwords are adequately secured. Still unsure which password manager to choose? We recommend you to study our comprehensive website on password managers!

Which password managers do we recommend?

Apple device users can use the Apple Keychain, which is part of the Apples‘ operating systems. Windows and Android OS users or those, who combine devices with different OS, we recommend Bitwarden (ideally the paid Premium version, which costs about as much as $12/year).

What do we strongly not recommend?

Although many browsers actively offer this (e.g. Google Chrome), it is not their main purpose. A better solution is to use a password manager browser add-on (also offered by Bitwarden). **Never share your passwords, never pass on shared passwords in the plaintext!** Don't send passwords via MS Teams either. A more secure option is e.g. encrypted email.

II. Multi-factor Authentication

Multi-factor Authentication[2] („MFA") provides an advanced level of protection by adding an additional factor of identity verification to the obligatory password. The added factor can take many forms, such as a code sent via SMS or email, a one-time code (known as TOTP) generated by a special app, or a physical (in the form of a USB key) or digital (stored in a password manager) security key.

The basic principle of this verification method is that the added factor is very difficult for an attacker to obtain or duplicate, whether due to limited time or personal distance. Therefore, an attacker cannot proceed further in the login process.

Beware! Using two different passwords consecutively **does not constitute multi-factor authentication**. The effectiveness of multi-factor authentication is also reduced, for example, by allowing message previews on the locked screen of a mobile device. Therefore, we recommend disabling the display of message previews or not using SMS-based verification.

Where possible, we recommend the use of multi-factor authentication, especially for key services and tools where an attacker could cause significant damage if they discover your password. This is particularly important for email accounts, online banking, password managers, and significant university information systems such as IS MU and INET MU. Within Masaryk University, it is desirable to activate MFA for the Microsoft M365 environment as well.

Why set up multi-factor authentication?

Shoulder surfing is a social engineering technique where an attacker observes their victim as they enter sensitive information (passwords, PIN codes, credit card numbers) on a device with a display. The essence of the attack lies in the attacker strategically getting close to the victim, allowing them to have a direct view of the display and carefully monitor key or character presses. The attacker uses crowded places, such as public transport, for this attack, where it's easier to be in close proximity to the target.

How to set up multi-factor authentication?

In accordance with the information and instructions on the IT MU website, we recommend using a **security key** (WebAuthn) as the primary option and a **verification code** (TOTP) as the secondary option to increase the security of your account and identity. Setting up the

[2] MFA = Multi-Factor Authentication. Alternatively, you may also encounter the term two-factor authentication (2FA = Two-Factor Authentication). In the context of this training, the terms 2FA and MFA can therefore be considered interchangeable.

activation of multi-factor authentication for individual services can be done through the User Profile for managing selected services.

a) **Security Key (WebAuthn)**

It is a physical or virtual device used to verify identity based on a secret key. A computer or smartphone can serve as a security key (e.g., Windows Hello for Windows or Touch ID for macOS) or a special USB key (e.g., YubiKey). If you are unsure whether your device has this feature, we recommend testing it using the following link.

How does it work? When logging in, the server sends a challenge that the security key "signs." The server then verifies whether this response was signed with the private key corresponding to the stored public key.

b) **Verification Code (TOTP)**

This involves one-time codes with limited time validity generated by a special (TOTP) app (e.g., Aegis Authenticator for Android and Raivo OTP for iOS). To properly set up multi-factor authentication, it is necessary to add a token for verification codes and interconnect everything in the multi-factor authentication of Masaryk University's Unified Login. Afterwards, simply copy and paste or transcribe the code displayed in the app when logging in. The code updates every 30 seconds.

Recommendation: If possible, prefer a security key over a one-time code. A security key is more convenient to use and resistant to phishing.

III. Device Security

Securing our digital devices, such as computers, tablets, and smartphones, is crucial for protecting privacy in today's digital world. Insufficiently secured devices are very attractive targets for attackers. They can, for example, install malicious software, which can have fatal consequences for your privacy in the form of theft of sensitive data or money from bank accounts.

How to secure your device?

The first step in securing your digital devices is to **ensure their physical safety**. Therefore, do not leave your devices unlocked when you leave them. After all, your devices store many valuables worth protecting.

We also recommend that **each device be locked** ideally using a fingerprint, facial recognition, or a PIN. What we do not recommend is using gesture unlocking on mobile devices, which is very easy for an attacker to breach. Another tip for you is: **Do not lend devices** that you use exclusively (whether for work or private purposes) to other people! Be cautious. This reduces the risk of someone stealing, for example, your login details to your bank account or other valuables.

If you ever **find a USB drive, SD card**, or other **storage medium**, definitely do not connect it to your own device. You never know what might be on it. Although you may be tempted to find out what you have found, there is a risk that the device contains malicious software that could damage your computer. Therefore, we recommend overcoming your curiosity and **handing over the medium to the IT department** for inspection.

Watch out for lures!

Baiting is a social engineering method where an attacker leaves an infected device (e.g., USB drive or other storage medium) in a place where the victim can easily find it (e.g., an elevator, parking lot, building entrance). They then exploit the curiosity of the victim, who inserts this medium into their device. This installs malicious code that allows the attacker to gain access to the victim's device or the entire network where the device is located.

Finally, we recommend that you **keep your operating system and antivirus software** (whether on your computer or mobile) **up to date**. This means not postponing the offered updates! Every program has bugs that attackers can exploit to their advantage. Updates prevent this. The ideal solution is to **enable automatic updates**.

Two antivirus programs = stronger security?

The presence of two or more antivirus programs on a device causes conflicts when checking files. Common antivirus applications monitor files in **real-time** – for example, when a web browser is launched, the antivirus will check the firefox.exe file, which is part of the browser. If multiple antiviruses are running on the device, each of them will try to check this file simultaneously. As a result, the **file will not be properly** checked because at any given moment, only one application may have access to it.

However, there is an exception in the case of **Microsoft Defender**, which is part of the Windows operating system. If a user installs another antivirus program, Windows Defender automatically disables itself to prevent conflicts and duplicate scanning.

Our final piece of advice on keeping your devices secure is: **Only download files from official and verified sources**. This reduces the risk of downloading a harmful virus into your computer or mobile that could block your device. However, even in official stores like the App Store or Google Play, dangerous apps can appear. Therefore, always **carefully read** what permissions the downloaded app requests. Only allow those that are necessary for the app's functionality. Guard your privacy and do not grant apps access to areas they don't need to access. Be particularly cautious when it comes to requests for access to the camera, microphone, contacts, or messages! It is also advisable to check the app's ratings, which can indicate whether the app is harmful.

IV. Data and everything around them

The term **data** can refer to all information recorded in digital form that an employee **receives, processes, or creates in the course** of their work. Every employee should ensure the appropriate storage and protection of data to prevent loss, damage, or misuse.

Data storage and backup

Data storage and backup are processes that ensure the protection and preservation of important data and information. Their goal is to minimize the risk of data loss due to hardware device failures, computer viruses, or accidental deletion. The university offers a wide range of options for **data storage and backup**, with each storage solution providing different levels of security.

Before deciding where to store your data – whether on a USB disk, network storage, or in the cloud - it is advisable to consider which storage options are suitable for the types of data you have. If you are unsure about the type of data you are dealing with, do not hesitate to consult with experts from the ICS.

Why Store and Backup?

Ransomware is **malicious software** that aims to encrypt data or block user access to a device. Typically, the attacker demands a ransom payment in digital currencies such as Bitcoin for decrypting the data. Ransomware can be **inadvertently downloaded**, for example, from an email attachment, during visits to compromised websites, or through other infected devices on the network. Once the user runs the attachment, data encryption occurs, and a ransom demand pops up. Without the decryption key, it is impossible to access the encrypted files.

How to store and back up data in the MU environment?

Users can utilize Microsoft 365 for data storage and backup, specifically through the cloud services OneDrive and SharePoint. It is essential to emphasize that work-related information and data should only be stored in officially recommended and used organization tools.

a) **OneDrive** is a 'personal' storage that allows users to store, share, and sync their files and documents online. This storage is suitable for storing your files that you don't need to share. You can connect your OneDrive folder to your devices following the instructions provided by IT MU.

b) **SharePoint** is primarily designed for sharing documents and facilitating collaboration with them within departments, teams, or across the organization.

Backup ensures the protection and preservation of essential data and information in case of accidental deletion, hardware malfunction, or ransomware.

You can combine multiple storage options according to their purpose, for example:

- Backup work data on the **work** Google Drive (log in using UČO@mail.muni.cz) or OneDrive (log in using UČO@muni.cz)
- Private photos and videos on **personal** Google Drive (log in using your personal account)

Recommendation: Implement the "3-2-1 backup rule"! Three copies, two media, with one stored in a different location (home/work). This might sound excessive, but for truly important data, whose loss would affect you financially or emotionally (e.g., research data, an article in progress, family photos), this rule will give you peace of mind.

It is not permitted to use private storage solutions (e.g., Dropbox, **personal** Google Drive) for storing work-related information and data.

Access Permissions

When using storage solutions like SharePoint and OneDrive, it is important to monitor access permissions to shared documents to minimize the risk of unauthorized access and sharing. On the IT MU website, you can find guides and procedures on how to check the settings of individual permissions or how to properly share documents to prevent unwanted information leaks outside the defined user circle.

Recommendation: Set sharing conservatively, only for authorized persons. Share files only with those who need access and remember to revoke sharing once the reasons no longer apply. Instructions on how to set up sharing can be found at it.muni.cz. **Do not share work data publicly.** Unless there is a specific reason, never share work data "with everyone on the internet." Exceptions might include freely available presentations and PR materials.

Disk encryption

Disk encryption ensures that even if someone gains physical access to your disk, the data on it will be unreadable. If your device is stolen, encryption prevents the attacker from accessing your sensitive information.

- On Windows, encryption is provided by a system component called **BitLocker**.
- On macOS, you activate encryption using the **FileVault** tool.
- Modern **mobile devices** are auto encrypted, but it is essential to use a screen lock.

Recommendation: Enable disk encryption on your computers! Anyone can activate disk encryption; it only takes a few clicks and significantly enhances the security of your data.

V. SECURE COMMUNICATION

Users at MU have access to university mailboxes with addresses in the format **uco@muni.cz** and **uco@mail.muni.cz**. Employees can also request the creation of a faculty mailbox through local IT support. Email communication can be accessed through web interfaces or email clients (such as Microsoft Outlook, Mozilla Thunderbird, or iCloud).

Within the organization, the primary means of communication is the M365 email system with a license for MS Outlook. Additional email settings can be configured in IS MU. An alternative option is to use the @mail.muni.cz email with forwarding to MU Gmail.

Instructions regarding the configuration of email mailboxes can be found on the IT MU website.

Recommended platforms for video conferencing include MS Teams and Google Workspace. Alternatively, you can also use the Zoom application. It is emphasized that strict adherence to logging in through the university license is necessary when working with these applications.

Keep in mind that work-related topics often contain sensitive information

Therefore, it is not appropriate to forward work email to personal email accounts. The reason is that third-party servers are used for receiving and sending messages, and this does not guarantee the protection of sensitive data and security!
Communicate your work matters exclusively through official work channels. Do not share information of this kind via personal communication platforms (e.g., Messenger, WhatsApp, etc.) or social networks (Facebook, Instagram, etc.).

COMMUNICATION PLATFORMS AT MU

MS Teams is a collaborative tool that allows for individual and group work chats, audio and video calls, and videoconferences. It is part of the university's Microsoft M365 license. Additionally, employees have access to Zoom and Google Meet. However, it is necessary to log in using your university account. The advantage of these tools is that communication is always encrypted.

End-to-end encryption is the foundation of secure electronic communication. It works by having the sender encrypt the data before sending, and decryption occurs only on the recipient's side. This ensures that the message content is not readable by anyone other than the recipient during its transmission over the network.

How to secure your email?

Encryption is the foundation of properly secured electronic communication. It works by encrypting messages that are sent using the recipient's public key, which is then decrypted by the recipient using their private key. This ensures that the message cannot be read by anyone else during its journey through cyberspace – a feature provided by tools with end-to-end encryption (meaning only the communicating parties can decrypt the message).

If you need to electronically sign documents or secure email communication, you can use personal certificates. With the help of a personal certificate issued by a trusted certification authority through the Trusted Certificate Service (TCS), you can prove your identity in email communication. In addition, it is possible to obtain a personal qualified certificate at Masaryk University, which is recognized by government authorities as well.

Certificates can be used in several scenarios, including identity verification of a person or object, privacy protection to ensure that information is only accessible to designated individuals. Encryption keep information unreadable to unauthorized parties, and digital signatures to ensure the non-repudiation and integrity of a message.

Connection

When browsing websites, a web browser sends information necessary for displaying the page correctly, such as screen resolution and selected language. However, this information can be used to reduce the user's anonymity (e.g., to determine the source website a user is coming from, gather geolocation data, etc.).

To find out what information your browser reveals about you, you can visit the website https://amiunique.org.

Wi-Fi (Wireless Fidelity) is a technology that enables wireless internet connectivity using radio waves. Wi-Fi is commonly used to connect computers, smartphones, tablets, and other devices to the internet in homes, offices, and public places like cafes or airports. To connect to a Wi-Fi network, you need a device that supports wireless connectivity (such as a smartphone or computer) and access to a Wi-Fi router or another device that provides internet access.

VPN (Virtual Private Network) is a network that allows you to connect to the internet through a secure and encrypted connection, protecting your privacy. When you use a VPN, your actual IP address (the numerical identification of your specific device, such as a computer) on the internet is hidden, and instead, the IP address of the VPN server is displayed. When working outside the university network (beyond a wired connection or Eduroam), it's always recommended to use a VPN for security purposes. Masaryk University provides **free** VPN access to its employees and students. Instructions for installation can be found on the IT Services MU website.

VI. phishing

In the online environment, we communicate constantly – sending and receiving a large number of emails and messages from various sources. However, communication in cyberspace comes with many risks. So, how do we ensure level of security?

Phishing is a fraudulent technique in which an attacker typically impersonates a trustworthy person or institution and **manipulates** the victim, often using urgency or time pressure, to perform an action for them – such as:

- sharing information,
- installing malicious software,
- clicking on a link in an email that leads to a fake website. On this website, fraudulent forms are usually placed to **input login credentials, credit card numbers, and other sensitive information**.

Phishing emails are extremely dangerous. They can easily masquerade as regular work emails, increasing the risk that users will click on forged links or provide sensitive information without realizing that it's a scam.

Email Headers

The sender of an email may appear similar to the name and email address of a legitimate organization (such as a bank), but in reality, it may differ slightly in the name or domain (the part after the "@" symbol), such as @mail.munI.cz instead of the official @mail.muni.cz.

What to do?

It is necessary to verify the sender's address and check
for any minor changes in the domain name (such as using "v" instead of "u", etc.).

What does an incorrect URL look like?

https://www.muni.cz

https://www.mvni.cz (with "v" instead of the letter "u")

Email Body

It is important to check the **content of a phishing email**, which may contain URL links leading to unknown websites and requests for sensitive information such as login credentials and credit card numbers. Attackers may create fake urgent situations in emails (such as threats of data loss) to pressure users into quick action without proper consideration.

What to do?

Even though these emails may seem trustworthy at first glance, it is crucial to realize that a legitimate authority (such as a bank or university) will never request sensitive information like passwords via email. Critically evaluate the email's content and the websites it links to. Watch out for unusual text with grammatical errors, convoluted phrases, and nonsensical greetings. Additionally, ensure that the links lead to legitimate websites and that the URL address is indeed the one you intend to visit.

Email Footers

Logos placed in the footers of emails are often exploited to create a sense of an official email. When a user sees the logo of an institution they know and trust, they may become less cautious and more susceptible to providing sensitive information without realizing it is an attack.

What to do?

When receiving emails from unknown senders, it is essential to be cautious and not be swayed by seemingly credible elements. If you have doubts about their authenticity, do not click on the links. Instead, contact the institution or sender directly to verify the email's authenticity.

Email Attachments

Suspicious email attachments may, at first glance, appear to be legitimate files or documents (PDF, DOC, MP3). A significant feature is that the name of the forged attachment has a different extension - instead of "DOC" or "DOCX," different letters are used that do not match the icon. Compressed attachments (RAR, ZIP) can also be suspicious.

What to do?

It is essential to have a **funcional and up-to-date antivirus** program, not open the attachment and if necessary, use a tool to check suspicious files.

Attackers can be inventive!

Vishing (voice-phishing) and **Smishing** (SMS phishing) are new forms of attacks that exploit the element of surprise and the user's lack of knowledge.

a) **Vishing** works on the principle of making fraudulent calls to a user's personal or work number. The caller pretends to be a bank employee or technical support and urges the user to react quickly in connection with alleged issues on their accounts. Typically, the user is bombarded with information like "your account has been compromised" or "the bank has detected an unauthorized payment," and the caller insists on immediate action.

b) **Smishing** uses a similar method of attack but through fraudulent text messages. Attackers disguise messages as legitimate communication from trusted entities (banks or mobile operators) while attempting to obtain sensitive information such as login credentials (usernames, passwords, mobile codes, etc.) or credit card details.

Our final advice is: critically evaluate the demands placed on you! **Trustworthy entities such** as banks or other institutions will never request sensitive information and data, such as passwords, through email, phone calls, or SMS messages.

VII. incident reporting

The Cybersecurity Team of Masaryk University (referred to as "CSIRT-MU"), which is part of the Institute of Computer Science, takes care of the secure online environment at the university. Its activities include coordinating and addressing security incidents related to MU's infrastructure.

If you have become a victim of an attack or suspect that you have received a fraudulent email, do not hesitate to contact members of CSIRT-MU by sending an email to csirt@muni.cz or by filling out the contact form.

Při nahlašování incidentů je třeba:

- **Provide the source** of the report, which includes your **first name**, **last name**, and **UČO**.
- **Define the issue**, describing in your own words as precisely as possible what complication you are experiencing. Every detail will assist the relevant staff member in resolving the issue, as they will have a better understanding of the situation.
- **Submit evidence**. For example, if you received a fraudulent email, forward it in its entirety, including attachments, links, and email headers. In the case of other issues, it is advisable to provide additional evidence, such as a screenshot of the screen.