ME/PSO

HANDBOOK

Cybersecurity Handbook

Awareness, threat recognition and protection in the digital world

Companion material for the training course:
"Raising Cyber Security Awareness"

Document No. MEPSO-PRI-SAJ-003 · Classification: Internal Use
Information and Cyber Security Department · MEPSO AD Skopje

Contents

1. Introduction

We live in a world where almost everything is connected — work, communication, finances. This connectivity brings enormous benefits, but also new risks that all of us need to understand.

Cybersecurity is not just a task for technical experts. Each of us, through our everyday digital habits, contributes to the security or the vulnerability of the organization. This handbook will give you a basic understanding of the threats and practical habits for protection.

You do not need to be a technical expert to be secure. You only need to develop awareness, healthy skepticism and a few good habits. That is enough to avoid the vast majority of threats.

> **Why it matters.** Cyber attacks do not discriminate — they can hit anyone. But an informed and attentive user is a much harder target. Knowledge is your best defense.

2. What is cybersecurity

Cybersecurity is the practice of protecting systems, networks, devices and data from digital attacks. The goal is to ensure the confidentiality, integrity and availability of information.

2.1 Why it matters to everyone

- It protects your personal and work data;
- It prevents financial losses and identity theft;
- It ensures the uninterrupted operation of the organization;
- It protects the critical infrastructure on which society depends.

2.2 The human factor

A large share of successful attacks exploit human nature — curiosity, trust, fear, the desire to help. Technology can protect a lot, but the final decision is often yours.

> **Fact.** The majority of security incidents involve human error. That is exactly why your awareness and attention are key.

3. The landscape of modern threats

Threats are diverse and constantly evolving. Here are the most common ones:

Threat	Description
Malicious software	Viruses, worms, trojans that damage systems
Ransomware	Locks data and demands a ransom
Phishing	Fraud via fake messages
Social engineering	Manipulating people into disclosing information
Identity theft	Misuse of personal data
Password attacks	Attempts to guess or steal passwords

4. Malicious software

Malicious software (malware) is any program created to cause damage, steal data or gain unauthorized access to a system.

4.1 Types

Type	Behavior
Virus	Attaches itself to files and spreads
Worm	Spreads on its own across networks
Trojan	Disguises itself as a legitimate program
Spyware	Secretly collects information
Adware	Displays unwanted advertisements

4.2 How it spreads

- ✓ Infected email attachments
- ✓ Malicious links and websites
- ✓ Infected USB devices
- ✓ Pirated or unapproved software
- ✓ Unpatched systems with security vulnerabilities

4.3 Protection

- ✓ Keep an active and updated antivirus
- ✓ Regularly update the operating system
- ✓ Do not install unapproved software
- ✓ Be careful with attachments and links
- ✓ Do not plug in unknown USB devices

5. Ransomware — locking data for ransom

Ransomware is a particularly dangerous type of malware that encrypts your data and demands a ransom to unlock it. It can paralyze the entire operation.

5.1 How it works

After infection, ransomware locks the files and displays a message demanding payment, most often in cryptocurrency, in exchange for the unlocking key.

> **Important.** Paying the ransom does not guarantee the return of your data and encourages crime. The best protection is prevention and regular backups.

5.2 Protection

- ✓ Make regular backups of important data
- ✓ Do not open suspicious attachments or links
- ✓ Keep your systems updated
- ✓ Report immediately if you notice unusual encryption of files

6. Social engineering

Social engineering is the manipulation of people into disclosing confidential information or taking actions that endanger security. Instead of attacking technology, attackers attack human nature.

6.1 Common techniques

Technique	Description
Impersonation	Pretending to be a trusted person or institution
Urgency	Creating pressure for a quick, unconsidered reaction
Authority	Posing as a superior or an authority
Helpfulness	Exploiting the desire to help
Curiosity	Baits that provoke curiosity

> **Defense.** Healthy skepticism is key. If something seems urgent, unusual or too good to be true — stop and verify through an independent channel.

7. Password and account security

Passwords are the keys to your digital life. Protecting them is the foundation of cybersecurity.

- ✓ Use long passwords (at least 12 characters)

- ✓ Combine letters, numbers and symbols
- ✓ A unique password for every account
- ✓ Use a password manager
- ✓ Enable two-factor authentication wherever available
- ✓ Never share passwords

> **Tip.** Two-factor authentication is one of the most effective protections. Even if a password is compromised, the second factor prevents an unauthorized login.

8. Safe internet browsing

- ✓ Check that the address starts with "https" for sensitive pages
- ✓ Be careful with suspicious or unknown websites
- ✓ Do not download files from untrusted sources
- ✓ Watch out for fake ads and pop-up windows
- ✓ Keep your browser updated

9. Mobile devices and security

Smartphones and tablets hold a great deal of sensitive information and are a frequent target.

- ✓ Lock the device with a PIN, password or biometrics
- ✓ Install apps only from official stores
- ✓ Pay attention to the permissions apps request
- ✓ Keep the operating system updated
- ✓ Do not leave the device unattended
- ✓ Enable remote wipe in case of loss

10. Security on public networks

Public Wi-Fi (cafés, airports, hotels) is convenient, but carries risks. Attackers can eavesdrop on traffic on unprotected networks.

- ✓ Use a VPN on public networks
- ✓ Avoid sensitive transactions on public Wi-Fi
- ✓ Turn off automatic connection to open networks
- ✓ Check the network name — attackers create fake ones

> **Rule.** Do not access sensitive systems or enter passwords over public Wi-Fi without a VPN. Always use a VPN for a secure connection.

11. Protecting your privacy

- ✓ Be careful what you share on social media
- ✓ Review your privacy settings
- ✓ Do not post sensitive personal or work information
- ✓ Be aware — the information you publish can be used against you

12. Backups and recovery

Backups are your safety net. If data is lost due to an attack, a failure or an error, a copy makes recovery possible.

- ✓ Make regular backups of important data
- ✓ Keep copies in a safe, separate location
- ✓ Verify that the copies actually work
- ✓ Follow the IT Department's recommendation on how to archive

13. Practical scenarios

Scenario 1: An urgent call from "technical support"

Someone calls claiming to be from technical support, saying your computer is infected. They ask you to install a remote access program so they can "fix" it.

Correct reaction: You install nothing and grant no access. Legitimate support does not call you unexpectedly like this. You hang up and report it to the real IT Department.

Scenario 2: A free prize

You receive a notification that you have won a prize and need to enter personal details to claim it.

Correct reaction: You ignore it. If something is too good to be true, it is most likely a scam. You do not enter any data.

Scenario 3: A suspicious application

You find an app that promises a useful feature, but requests access to your contacts, messages and location even though its purpose does not require it.

Correct reaction: You do not install it. Excessive permissions are a sign of a suspicious app. You install only from official sources.

14. Frequently asked questions

Does antivirus protect me completely?

No. Antivirus is an important layer, but not sufficient on its own. Your attentiveness, updated systems and good habits are equally important.

What matters most for cybersecurity?

Awareness. Most attacks require your participation (a click, entering data). An attentive user avoids the vast majority of threats.

How often should I change my password?

Whenever compromise is suspected, and periodically for critical accounts. More important than frequent changes is that the password be strong, unique and protected with 2FA.

Is it safe to use public computers?

With great caution. Do not enter passwords for sensitive accounts, always log out, and do not leave personal data behind. If possible, avoid them for important tasks.

What if I think I am infected?

Disconnect from the internet, do not enter any passwords, and report to the IT Department immediately. A quick reaction limits the damage.

15. Glossary and checklist

Term	Meaning
Malware	Malicious software — a general term for harmful programs
Ransomware	Software that locks data and demands a ransom
Trojan	A malicious program disguised as a legitimate one
Social engineering	Manipulating people into disclosing information
VPN	Virtual private network for a secure connection
Two-factor authentication	A second layer of protection at login
Backup	A copy of data used for recovery in case of loss

Basic cyber hygiene

- ✓ Strong, unique passwords + 2FA
- ✓ Updated systems and antivirus
- ✓ Care with email, links and attachments
- ✓ VPN on public networks

- ✓ Regular backups
- ✓ Reporting every suspicion

Cybersecurity beyond work

Good cybersecurity habits do not end when you leave the workplace. Protecting your digital life at home is equally important — and the same principles often protect you both at work and privately.

Your home network

- ✓ Change the default password on your home router
- ✓ Use a strong password for your home Wi-Fi
- ✓ Update the router when upgrades are available
- ✓ Set up a separate guest network for visitors

Protecting your family

- ✓ Talk to your family about cyber risks
- ✓ Help them recognize scams
- ✓ Pay attention to children's safety online
- ✓ Keep home devices updated and protected

> **A shared culture.** Cybersecurity is a way of thinking, not a set of rules just for work. When it becomes a habit in every aspect of life, you and your loved ones are much safer.

Continuous learning

Technology and threats are constantly changing. Stay informed, follow the recommendations, and do not hesitate to ask when in doubt. Learning about cybersecurity is a lifelong journey.

16. Conclusion

Cybersecurity is a continuous process, not a one-off activity. The threats will change, but the basic principles remain: be careful, be skeptical of the unexpected, and maintain good digital habits.

> **Key message.** You are the most important line of defense. Every informed decision you make increases your security and that of the entire organization.

MEPSO AD Skopje — Electricity Transmission System Operator of North Macedonia
Document No. MEPSO-PRI-SAJ-003 · Classification: Internal Use