Safe Online: The Basics of Cyber Self-Defense for the Modern World

Study text

Mehmet Ali Dursun
Kutahya Dumlupinar University
Jana Mikušová
Mendel University in Brno
Hussein Mkiyes
Bratislava University of Economics and Business
Estera Szakadatova
EconoMind

Enhancing Digital and Soft Skills for Ageing Workforce
EDSAW
Project number: 2023-1-SK01-KA220-ADU-000159273

ISBN 978-80-69196-08-7

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Authors:
Mehmet Ali Dursun, Kutahya Dumlupinar University, Chapters 1 and 7
Hussein Mkiyes, Bratislava University of Economics and Business, Chapters 2 and 5
Jana Mikušová, Mendel University in Brno, Chapters 3 and 6
Estera Szakadatova, EconoMind, o.z., Chapters 4 and 8

Reviewers:
Sergio Miranda; University of Salerno, Italy
Ulaş Yabanova; Çanakkale Onsekiz Mart University, Türkiye

This outcome was prepared in the framework of the project Enhancing Digital and Soft Skills for Ageing Workforce. Project number: 2023-1-SK01-KA220-ADU-000159273. Erasmus+ Key Action 2: Cooperation for Innovation and Exchange of Good Practices KA220-ADU - Cooperation partnerships in adult education.

Contents

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Chapter 1
Introduction To Cybersecurity

1.1. Introduction

In today's digital world, it has become more critical than ever to ensure security at the personal, corporate and government level. Cyber security is a field of techniques, policies and practices developed to protect the data of individuals and organizations from malicious attacks.

During this lesson we will learn the following:

- The basic principles of cybersecurity and why it is critical
- Methods for Creating and Managing Strong Passwords
- Effective Strategies for Protecting Personal Data
- Methods for Preventing Online Fraud and Identity Theft
- Safe Internet Usage and Browser Settings
- Antivirus Software and Firewalls
- Strategies for Preventing Social Engineering Attacks and Cybercrimes
- Social Media and Mobile Device Security

With the rapid advancement of the digital age, the internet and computer systems have become an inseparable part of our lives. Today, our personal information, financial data, company secrets, and sensitive government-level information are stored and shared in online environments. However, this digitalization has brought along risks such as cyber threats, data breaches, identity theft, and ransomware.

At this point, cybersecurity emerges as the process of protecting information assets against such threats. Cybersecurity is an indispensable element not only for individuals but also for companies, governments, and the entire digital ecosystem.

In this course, the basic principles of cybersecurity, types of threats, protection methods, and cyber defense strategies will be discussed. Having knowledge about cybersecurity will strengthen individuals and organizations against attacks and help them minimize security vulnerabilities.

1.1.1. Definition and Importance of Cybersecurity

Cybersecurity is the process of protecting computer systems, networks, devices, programs, and data from malicious attacks.

The fundamental goals of cybersecurity include:

- **Confidentiality**: Preventing unauthorized individuals from accessing sensitive data.
- **Integrity**: Ensuring that data is protected from unauthorized alterations.
- **Availability**: Ensuring that authorized individuals or systems can always access data securely.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

These three fundamental principles (CIA Triad - Confidentiality, Integrity, Availability) form the foundation of modern cybersecurity practices. The security of a system or data depends on the ability to maintain these three principles.

Cybersecurity is of vital importance for both individuals and organizations. Ranging from the protection of personal data to national security, cybersecurity plays a critical role in preventing sensitive information from falling into the hands of malicious actors.

1.1.2. The Importance of Personal Cybersecurity

Individuals share their personal information while using internet banking, social media, email, mobile applications, and shopping platforms in their daily lives. However, threats such as phishing attacks, malware, and ransomware can lead to the theft or misuse of this data.

Examples of Cyber Threats for Individuals:

- **Identity Theft:** The theft of personal information to create fake identities.
- **Social Engineering Attacks:** Manipulating human psychology to gain access to confidential information.
- **Ransomware:** Malicious software that encrypts data on computers and demands a ransom to decrypt it.

Cybersecurity Strategies for Individuals:

- **Use strong and unique passwords:** Passwords should be at least 12 characters long and contain uppercase and lowercase letters, numbers, and special characters.
- **Use two-factor authentication (2FA):** Add an extra layer of security when logging into email, banking, and social media accounts.
- **Keep antivirus and security software up to date:** Use updated software to protect systems from new threats.
- **Avoid clicking on suspicious links:** Be cautious of emails and links from unknown sources.

1.1.3. Corporate Cybersecurity Importance

Companies and organizations manage systems that contain large amounts of customer data, financial records, and trade secrets. The theft or damage of this information can lead to both financial losses and reputation damage.

Key Cyber Threats Faced by Companies:

- **Data Breaches:** Unauthorized access to sensitive information.
- **Insider Threats:** Employees consciously or unconsciously creating security vulnerabilities.
- **Denial of Service Attacks (DDoS - Distributed Denial of Service):** Overloading servers with excessive requests or access attempts, causing systems to crash.

Cybersecurity Strategies for Companies:

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

- Provide regular cybersecurity awareness training to employees.
- Implement firewalls and network security policies.
- Regularly back up critical data.
- Conduct penetration testing to identify security vulnerabilities.

1.1.4. The Importance of Cybersecurity for Governments

Governments develop cybersecurity policies and regulations to protect critical infrastructures and national security. Government systems contain highly sensitive data, such as military information, healthcare data, and election security.

Cyber Threats at the Government Level:

- **Cyber Warfare:** Digital attacks between nations.
- **Infrastructure Attacks:** Cyber attacks targeting electricity grids, transportation systems, and healthcare services.
- **Election Security Attacks:** Attacks aimed at manipulating democratic elections.

Cybersecurity Strategies for Governments:

- Create cybersecurity laws and regulations.
- Develop robust cyber defense systems to protect critical infrastructures.
- Collaborate internationally to combat cyber threats together.

1.1.5. Reasons for the Increase in Cybersecurity Threats

Cyber attacks are becoming more sophisticated and widespread every day. So, what are the main reasons for the increase in these threats?

Main Reasons for the Increase in Threats:

- **Acceleration of Digitalization:** As more data is stored in digital environments, the attack surface expands.
- **Increase in Internet-Connected Devices (IoT):** Smart devices increase security vulnerabilities.
- **Cybercrime Becoming Profitable:** Ransomware and data breaches are major sources of income for cybercriminals.
- **AI-powered attacks:** Artificial intelligence makes attacks faster and more effective.

The Role of Cybersecurity in Our Lives - Cybersecurity is a topic everyone must be aware of in the modern world.

1.2. Overview of Common Cyber Threats and Attack Types

1.2.1. The Importance of Cyber Threats and Attacks in Today's World

With the integration of technology into our lives, information security has become one of the most critical issues today. While the internet, smart devices, and digital platforms enable fast access to data, this also expands the target area for cybercriminals.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Cyber threats pose a significant risk to everyone, from individuals to government institutions. The direct consequences of cyber attacks include personal information theft, financial losses, corporate data breaches, and even national security threats.

Key Statistics:

- According to IBM's 2023 Data Breach Report, the average cost of a data breach is estimated to be $4.45 million.
- In 2021, there were 623 million ransomware attacks worldwide.
- The damage caused by cybercrime to the global economy could exceed $10 trillion by 2025.

Why Are Cyber Attacks So Dangerous?

- **Wide scope:** They can target individuals, companies, and governments.
- **Stealth**: Many cyber attacks can continue for a long time without being detected.
- **Financial losses:** Companies and individuals may face significant financial damage.
- **Loss of trust:** It leads to reputational damage for brands and governments.

Why Have Cyber Threats Become Such a Major Issue?

- Increase in digitalization: Many sectors, including banking, healthcare, education, and trade, have fully transitioned to the digital space.
- Growth of connected devices (IoT - Internet of Things): Smartphones, cameras, and home automation systems have become vulnerable to cyber attacks.
- Profitability of cybercrime: Ransomware, data breaches, and identity theft provide substantial financial gain for attackers.
- Lack of security awareness: Many users remain unaware of cyber security measures, leaving them vulnerable to attacks.

In this section, we will examine the most common types of cyber threats and attack techniques.

1.2.2. Understanding Cyber Threats

Cyber threats have become one of the most critical issues in today's digital era. With the increasing dependence on technology, businesses, governments, and individuals are at constant risk of cyberattacks. These threats range from simple phishing scams targeting individuals to complex state-sponsored cyber warfare. Understanding these threats is the first step in developing effective defense mechanisms.

What Are Cyber Threats?

Cyber threats refer to any malicious activity that aims to disrupt, damage, or gain unauthorized access to digital systems, networks, or data. These threats can come in various forms, including malware infections, phishing attempts, distributed denial-of-service (DDoS) attacks, and more.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Cybercriminals use these techniques to steal sensitive information, cause financial losses, disrupt business operations, and even compromise national security.

Why Are Cyber Threats Increasing?

Several factors contribute to the increasing number of cyber threats:

- **Digital Transformation:** More businesses and individuals store and transmit data online, increasing their vulnerability to cyberattacks.
- **Internet of Things (IoT):** The rise of smart devices has introduced additional attack vectors for cybercriminals.
- **Ransomware-as-a-Service (RaaS):** The commercialization of cybercrime, where attackers sell ransomware kits to less skilled hackers, has made attacks more frequent.
- **Lack of Cybersecurity Awareness:** Many users and organizations still fail to follow best cybersecurity practices, leaving them vulnerable to attacks.

1.2.3. Types of Cyber Threats

Cyber threats can be classified into different categories based on their attack methods and objectives. Below, we explore the most common cyber threats and attack types in detail.

Malware (Malicious Software)

Malware is a broad category of malicious software designed to harm, exploit, or otherwise compromise digital systems. Malware can infiltrate systems through email attachments, software vulnerabilities, malicious downloads, or infected websites.

Common Types of Malware

- **Viruses**: Malicious code that attaches to legitimate files and spreads upon execution.
- **Worms**: Self-replicating malware that spreads across networks without user intervention.
- **Trojan Horses:** Disguised as legitimate software but secretly perform malicious actions.
- **Spyware**: Secretly monitors user activity and steals sensitive information.
- Ransomware: Encrypts a victim's files and demands payment for their release.
- **Rootkits**: Provides attackers with administrator-level access to infected systems, making them difficult to detect.
- **Adware**: Delivers unwanted advertisements, sometimes bundled with spyware.

Real-World Example: In 2017, the WannaCry ransomware attack affected over 200,000 computers in 150 countries. This malware exploited a Windows vulnerability, encrypting users' data and demanding Bitcoin payments to restore access.

Phishing Attacks and Social Engineering

Phishing is a cyberattack method that uses deceptive emails, messages, or websites to trick users into revealing personal or financial information.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Types of Phishing Attacks

- **Email Phishing:** Fraudulent emails designed to mimic legitimate organizations and lure victims into revealing sensitive information.
- **Spear Phishing**: Highly targeted attacks aimed at specific individuals or organizations.
- **Whaling**: Phishing attacks directed at high-profile targets, such as executives and government officials.
- **Smishing**: Phishing via SMS or messaging apps.
- **Vishing**: Voice phishing over phone calls to extract sensitive data.

Example: A cybercriminal might send an email posing as a bank representative, requesting account details under the pretense of security verification. If the victim provides the information, the attacker gains access to their bank account.

Distributed Denial-of-Service (DDoS) Attacks

A DDoS attack is a method used by hackers to overwhelm a website or network with excessive traffic, causing it to crash or become unusable.

How DDoS Attacks Work

- Attackers use botnets (networks of infected computers) to flood a target server with traffic.
- The targeted server is unable to process legitimate requests, resulting in service disruption.
- Some attackers demand ransom payments to stop the attack.

Example: In 2016, the Mirai botnet DDoS attack took down major websites such as Twitter, Netflix, and Reddit by targeting the DNS provider Dyn, making many popular sites inaccessible for hours.

Insider Threats

An insider threat occurs when an individual within an organization—such as an employee, contractor, or business partner—maliciously or negligently causes harm to the organization's digital infrastructure.

Types of Insider Threats

- **Malicious Insiders:** Employees who intentionally steal or compromise data.
- **Negligent Insiders:** Employees who inadvertently expose sensitive information through poor cybersecurity practices.
- **Compromised Insiders:** Employees whose accounts are taken over by hackers.

Example: In 2013, former NSA contractor Edward Snowden leaked classified U.S. government documents, exposing mass surveillance programs.

Zero-Day Exploits

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

A zero-day attack targets vulnerabilities in software that are unknown to the vendor and, therefore, have no existing fix or patch.

Example: In 2021, Microsoft disclosed a zero-day vulnerability in its Exchange Server software that allowed hackers to gain unauthorized access to corporate email systems.

1.2.4. Preventing and Mitigating Cyber Threats

To defend against cyber threats, organizations and individuals must implement robust cybersecurity measures.

Best Practices for Individuals

- Use strong, unique passwords and enable multi-factor authentication (MFA).
- Avoid clicking on suspicious links or downloading unknown attachments.
- Keep software and operating systems regularly updated.
- Use antivirus and anti-malware programs to detect threats.
- Be cautious when sharing personal information online.

Best Practices for Organizations

- Implement firewalls and intrusion detection systems.
- Conduct regular security audits and penetration testing.
- Educate employees on cybersecurity awareness and phishing prevention.
- Encrypt sensitive data to protect against breaches.
- Establish a rapid incident response plan to mitigate attacks.

Cyber threats continue to evolve, becoming more sophisticated and damaging over time. Whether through malware, phishing, DDoS attacks, or insider threats, cybercriminals find new ways to exploit vulnerabilities. By understanding these threats and implementing proper cybersecurity practices, individuals and organizations can strengthen their defenses and reduce their risk of falling victim to cyberattacks.

1.2.5. The Damages of Cyber Threats and Attacks

Cyberattacks can cause widespread damage by targeting information technology infrastructure. These damages can have significant impacts on individual, corporate, and national levels. Today, critical sectors such as banking, healthcare, education, defense, and commerce face severe losses when exposed to cyber threats.

Damages of Cyber Threats for Individuals

Personal Data Theft and Identity Loss

Cyber attackers can commit identity theft by intercepting individuals' credentials, credit card numbers, bank accounts and private messages.

Cybercriminals can steal individuals' identity information, credit card numbers, bank accounts, and private messages, leading to identity theft.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Example: A person may fall victim to a phishing attack in which they are tricked by a fake banking email and share their credit card information with the attackers, putting their accounts at risk of being emptied.

Potential Damages:

- Access to bank accounts
- Creation of fake identities for illegal activities
- Sale of personal and private information on the dark web
- Hacking of social media accounts

Financial Losses and Fraud

Phishing attacks and fraud attempts can lead individuals to suffer financial losses. Cybercriminals can cause monetary harm by hijacking bank accounts or stealing credit card information.

Example: A person might fall victim to a fraudulent e-commerce website, where their credit card details are stolen and unauthorized transactions are made from their bank account.

Potential Damages:

- Large expenditures made using stolen credit cards
- Losses from investment and cryptocurrency fraud
- Illegal loans taken out from banks in the victim's name

File Loss Due to Ransomware

Ransomware attacks encrypt users' files, preventing access and demanding a ransom payment to decrypt them. If the payment is not made, the files may be permanently deleted.

Example: The 2017 WannaCry attack affected over 300,000 computers worldwide, causing millions of dollars in damage.

Potential Damages:

- Loss of photos, documents, projects, and work files
- Being forced to pay a ransom
- Disruption of business continuity

Psychological and Emotional Effects

Individuals who fall victim to cyberattacks may experience stress, fear, and insecurity. Those whose personal information is leaked are particularly vulnerable to social and psychological harm.

Example: Cyberbullying and threatening messages can lead to mental health issues such as depression and anxiety.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Potential Damages:

- Feelings of insecurity and fear
- Withdrawal from social media platforms
- Mental health problems

1.2.6. Damages of Cyber Threats for Companies

Significant Financial Losses and Waste of Business Resources

A cyberattack can cause companies to lose millions of dollars and halt their operational processes. Cybercriminals can put companies in a difficult situation by stealing trade secrets or blocking systems.

Example: The 2013 Target Data Breach resulted in the loss of credit card information for 40 million customers, and the company was forced to pay $18 million in compensation.

Potential Damages:

- Loss of customer trust
- Loss of competitive advantage
- High legal penalties and compensation claims

Reputation Loss and Erosion of Customer Trust

A company that has its customer data stolen or suffers service outages may experience a significant loss of trust, causing customers to turn to competitors. When a company's security is breached, consumers lose confidence in the brand and seek alternative solutions.

Example: Facebook's 2019 data breach exposed the personal data of 530 million users, severely damaging user trust.

Potential Damages:

- Decrease in sales and customer loyalty
- Drop in stock value
- Damage to the brand's image

Legal and Regulatory Consequences

Companies are required to comply with data protection laws to safeguard customer information. When a data breach occurs, governments and regulatory bodies can impose hefty fines on companies.

Example: Companies that fail to comply with the General Data Protection Regulation (GDPR) can face fines reaching millions of euros.

Potential Damages:

- Large fines imposed by the government

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

- Customer lawsuits and compensation payments
- Termination of agreements with business partners

1.2.7. Damages of Cyber Threats for States and National Security

National Security Threats and Cyber Warfare

Some countries can cause large-scale damage by attacking the critical infrastructure of other nations (such as electrical grids, water resources, telecommunications systems, etc.). Cyber warfare can be just as destructive as traditional warfare, but with lower costs.

Example: The 2010 Stuxnet attack on Iran's nuclear facilities is one of the most significant cyberattacks targeting physical infrastructure.

Potential Damages:
-Theft of state secrets
-Collapse of critical infrastructure
-Hijacking of military systems

Election Interference and Threats to Democracy

State-sponsored hacker groups can infiltrate election systems to manipulate outcomes, spread fake news, or alter election results.

Example: It has been alleged that Russia used cyberattacks to influence the 2016 U.S. Presidential Election process.

Potential Damages:

- Alteration of election results
- Social chaos and unrest
- Erosion of public trust in democracy

1.3. Impact of Cyber Threats on Society

Cyber threats and attacks can have serious consequences at all levels, from individuals to governments. Individuals should be more vigilant in protecting their personal information, companies need to take measures to ensure data security, and governments must develop security strategies to protect critical infrastructure.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Chapter 2
Creating and Managing Strong Passwords

2.1. Introduction

In the current cyber world, passwords are the most important guardians to personal and organizational information. They are the most widely used form of authentication and are used to safeguard information in both professional and personal spheres. Despite the advancement in cybersecurity solutions, the password is the mainstay in cyber protection infrastructure.

Many people -among them members of an aging workforce -have difficulty practicing good password hygiene. They use poor passwords, reuse them on platforms, and don't update or safely store them properly. In this chapter, we will examine the need for strong password practices, provide theoretic and practical insight, and address the special concerns facing aging adults in the online world.

Purpose of the Chapter: At the conclusion of this chapter, learners will comprehend the importance of passwords in cybersecurity, know how to properly construct and manage them, and know how to incorporate tools such as password managers and multi-factor authentication into practice.

2.2. Theoretical Framework / Key Concepts

Understanding Password Security is based on cryptographic principles and user behavior. Systems are protected by passwords as the first line of defense against intruders. Weak or identical passwords are a significant risk and are frequently compromised by intruders through methods like brute-force attacks or phishing attacks.

2.2.1. Key Terms and Concepts:

- **Password strength:** Represents the level of difficulty to guess or break a password. It improves with size, complexity, and randomness.
- **Entropy**: An indication of randomness in a password. An increased value of entropy means more protection against attacks
- **Credential Stuffing:** A type of cyber attack when stolen user credentials are used to access user accounts on numerous websites.
- **Password Hashing:** An operation that hashes passwords into unreadable text strings. Stolen hashed passwords are impossible to decrypt, even if tampered with.
- **Two-Factor Authentication (2FA) / Multi-Factor Authentication (MFA)**: Introduces extra layers to the login procedure that makes unauthorized access very difficult**.**

2.2.2. Common Threats to Password Security:

- **Phishing Attacks:** Fraudulent communications trick users into revealing credentials.
- **Keyloggers:** Malicious software that records keystrokes to capture passwords.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

- **Brute Force Attacks:** Systematically trying all possible combinations to guess a password.
- **Social Engineering:** Manipulating individuals into giving away confidential information.

Ageing Workforce Considerations: Older adults tend to feel cognitive load or unfamiliarity with novelty tools. Clear instructions, visual aids, and practice are necessary to enhance their digital competency. Ageing populations would rather use mnemonic methods or visual cueing and these need to be integrated into learning modules.

2.3. Practical Applications

Building Strong Passwords Key Characteristics:

- Minimum 12–16 characters
- Mix of uppercase and lowercase letters
- Numbers and special symbols
- No personal information (e.g., names, birthdays)
- Unique for each platform

Examples: **Strong**: Tg9!rP$xZ1@Lm4Q
Weak: qwerty, John123, password1

2.3.1. Strategies for Remembering Passwords:

- Use memorable phrases or acronyms: "My cat has 3 toys!" → Mch3T!
- Combine unrelated words and numbers: Banana!Dog42$Tree
- Create song lyric passwords: Use the first letter of each word from a favorite song lyric combined with numbers/symbols

Using Password Managers

A password manager securely stores and retrieves complex passwords using encryption. It simplifies the process of remembering multiple credentials while increasing security.

Popular Tools:

- **Bitwarden**: Open-source, user-friendly, browser and mobile support
- **LastPass**: Freemium model with automatic sync
- **1Password**: Intuitive design and family sharing options
- **KeePass**: Offline, highly secure, ideal for tech-savvy users

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

How to Set Up a Password Manager:

- Download the app/browser extension
- Create a strong master password
- Enable 2FA for extra protection
- Import or manually enter your credentials
- Regularly update entries and check for breaches

Multi-Factor Authentication (MFA)
MFA adds another verification layer to login credentials. Recommended for email, banking, and cloud services.

Common MFA Methods:

- One-time passwords (OTPs) via SMS or email
- Authenticator apps (e.g., Google Authenticator, Authy)
- Biometrics (fingerprint, face scan)
- Hardware tokens (YubiKey)

Case Study 1: Digital Security Workshop for Seniors A training workshop was organized for adults aged 55+ to improve their password hygiene. Participants learned to:

- Create secure passwords using phrase-based methods
- Install Bitwarden and set up an account
- Enable MFA on Gmail and social media platforms

Feedback showed increased confidence and willingness to adopt new tools. The approach used visual step-by-step guides and peer collaboration.

Case Study 2: Avoiding Catastrophe through Prevention Anna is an administrative assistant who is 60 years old. She got her email spoofed by a phishing attack. She had used the same password on five platforms. She adopted the use of a password manager and applied MFA to all major accounts once her IT team jumped in and helped her out. Her incident highlights the significance of proscriptive behavior.

Tools to Check Password Safety

- **https://haveibeenpwned.com**: Check if your credentials were compromised in a breach
- **Password Strength Checkers**: Built into most managers or available online

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

2.3.2. Organizational Policies

Companies can protect their workforce by:

- Requiring complex passwords
- Encouraging regular updates (e.g., every 90 days)
- Blocking use of previous passwords
- Offering password manager subscriptions

2.3.3. Recommended Practices for Older Employees:

- Use a single master password to unlock all others
- Avoid writing passwords on paper
- Keep recovery options (e.g., phone number, backup email) updated
- Attend refresher courses on digital security annually

2.4. Summary

Passwords form the basis of online protection of individual identity. Poor password practices are one of the most avoidable cyber threats. Digital literacy solutions should be made available to the ageing population and should account for the specific learning aspects relevant to older adults.

The future will involve more use of biometric authentication solutions, but passwords will continue to be an important access option. It is therefore important to excel in password creation, administration, and secure storage—and supplement these with multi-factor authentication.

Discussion Questions:

- How can digital training be made more accessible for older adults?
- What are the pros and cons of password managers compared to traditional memory methods?
- Could biometric systems replace passwords entirely in the future?
- What role should employers play in managing employee password practices?

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

References and Further Reading

AlHusain, R., Alkhalifah, A., 2022. Evaluating knowledge-based security questions for fallback authentication. PEERJ COMPUTER SCIENCE. https://doi.org/10.7717/peerj-cs.903

Gray, J., Franqueira, V.N.L., Yu, Y., 2016. Forensically-Sound Analysis of Security Risks of using Local Password Managers. 2016 IEEE 24TH INTERNATIONAL REQUIREMENTS ENGINEERING CONFERENCE WORKSHOPS (REW). https://doi.org/10.1109/REW.2016.58

Griffin, P.H., 2014. Telebiometric Authentication Objects. COMPLEX ADAPTIVE SYSTEMS, Procedia Computer Science. https://doi.org/10.1016/j.procs.2014.09.011

Maclean, R., Ophoff, J., 2018. Determining Key Factors that Lead to the Adoption of Password Managers. 2018 INTERNATIONAL CONFERENCE ON INTELLIGENT AND INNOVATIVE COMPUTING APPLICATIONS (ICONIC).

Radescu, R., Davidescu, A., 2010. Security and Confidentiality in the Easy Learning on-line Platform. PROCEEDINGS OF THE 5TH INTERNATIONAL CONFERENCE ON VIRTUAL LEARNING, ICVL 2010, Proceedings of the International Conference on Virtual learning.

Zeba, S., Amjad, M., 2023. Distribution and tracking current live location of recognised criminal face at decentralised blockchain through image. INTERNATIONAL JOURNAL OF INTERNET PROTOCOL TECHNOLOGY. https://doi.org/10.1504/IJIPT.2023.133028

Zhou, L., Bao, J., Watzlaf, V., Parmanto, B., 2019. Barriers to and Facilitators of the Use of Mobile Health Apps From a Security Perspective: Mixed-Methods Study. JMIR MHEALTH AND UHEALTH. https://doi.org/10.2196/11223

National Cyber Security Centre. (2021). Password Guidance. https://www.ncsc.gov.uk/collection/passwords

Microsoft Security. (2022). Multi-factor Authentication. https://www.microsoft.com/security/blog

SANS Institute. (2023). Password Managers: Safety and Best Practices. https://www.sans.org

Symantec. (2021). Internet Security Threat Report. https://www.broadcom.com

Cyber Aware. (2023). Secure Your Accounts. https://www.cyberaware.gov.uk

Have I Been Pwned. (2024). Data Breach Check. https://www.haveibeenpwned.com

OWASP Foundation. (2023). Authentication Cheat Sheet. https://owasp.org

ENISA. (2022). Cybersecurity for the Elderly. https://www.enisa.europa.eu

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Chapter 3
Personal Data Protection Techniques

3.1. Introduction

The concept of privacy from the legal perspective might have a difficult and flexible expression.

In general, it is considered both the physical and psychological integrity of a person but from international perspective it faces many problems (James Michael. Privacy and Human Rights 1 UNESCO, 1994) as the term "physical and psychological integrity" is influenced by different legal and cultural background. That is why this area faces international fragmentation, especially when compared between European and American legal interpretations.

The Internet and the way it dramatically entered social relations and transformed the old order also led to a changed perception what is private and what needs to be protected.

After studying this unit, you should be able to:

- Discuss the concept of personal data
- Know the modern day principles of protection of personal data;
- Know different legal regimes for protecting privacy;
- Know the rules for organizations;
- Know how to protect your personal data.

3.2. The Concept of Personal Data

According to the EU Commission personal data is any information that relates to an identified or identifiable living individual (data subject). Different pieces of information, which together can lead to the identification of a particular person, may also be considered personal data. Personal data that has been de-identified, encrypted or pseudonymized but can be used to re-identify a person also remains personal data.

Personal data is automatically considered to be name, surname and birth number.

Personal data can be divided to:

- **Real** - data associated with a specific natural person.
- **Completely anonymous** - it is not possible to determine the original data subject.
- **Partially anonymous** - if certain conditions are met, it is possible to trace a specific person (health care, etc.)
- **Identification data** - name, surname, date of birth, place of birth, birth number, account number, etc.
- **Address data** - permanent address, temporary address, employer's address.
- **Descriptive data** - employment, education, property, difficulty determining what can be considered personal data.
- **Sensitive data** - health, sexual orientation, etc. Human rights may be violated during the processing of such data, and the law views their use through a stricter lens, as their misuse can have serious consequences

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

3.3. Personal Data Protection Legislation Brief History

During the 1970s, Western countries began to respond to the need to enshrine personal data protection in valid legislation. In 1980 OECD issued guidelines on data protection, reflecting the increasing use of computers to process business transactions. In 1981 The Council of Europe adopted the Data Protection Convention (Treaty 108), rendering the right to privacy a legal imperative.

The evolution of personal data protection in the EU started on the adoption of European Data Protection Directive in 1995, establishing minimum data privacy and security standards, upon which each member state based its own implementing law.

Then in 2011 a Google user sued the company for scanning her emails and two months after that, Europe's data protection authority declared the EU needed "a comprehensive approach on personal data protection" and work began to update the 1995 directive.

The GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) entered into force in 2016 after passing European Parliament, and as of May 25, 2018, all organizations were required to be compliant.

3.4. Key Definitions Brought by GDPR

- **Personal data** — any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. Pseudonymous data can also fall under the definition if it's relatively easy to ID someone from it.
- **Data processing** — Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing… so basically anything.
- **Data subject** — The person whose data is processed. These are your customers or site visitors.
- **Data controller** — The person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you.
- **Data processor** — A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations. They could include cloud servers or email service providers.

3.5. Principles of the GDPR

- **Lawfulness, fairness and transparency**
  According to GDPR Article 5(1)(a) "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, transparency')". This principle specifies that organizations must ensure their practices around data collection don't compromise the law and that their use of data is transparent to data subjects.
- **Purpose limitation**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

GDPR Article 5(1)(b) states that: "Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes" which means that organizations must only gather personal data for a specified purpose. They must outline what is the goal of collecting, and only collect data for the time that they need to carry out this goal.

- **Data minimization**
  Article 5(1)(c) states that: "Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization)." According to the GDPR, organizations should only retain the smallest amount of data needed for their requirements. Organizations cannot collect personal data for the possibility that it could be useful later on.
- **Accuracy**
  Article 5(1)(d) states that: "Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')". To fulfil this requirement organizations must review information they hold about individuals regularly. Data subjects can ask that incomplete or inaccurate data be fixed or erased within 30 days.
- **Storage limitation**
  Article 5(1)(e) states that: "Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')". After an organization no longer requires personal data, for the reason for which it was gathered, it should be deleted.
- **Integrity and confidentiality**
  Article 5(1)(f) states that: "Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').". The security of the information that is retained is essential. The organization should make sure that all the proper measures are set to safeguard personal information. This may include safeguarding from internal threats, including accidental damage or loss, unauthorised use, and from external threats, for example cyber attacks.
- **Accountability**
  Article 5(2) of the GDPR states that "The controller shall be responsible for, and be able to demonstrate compliance with [the other data protection principles]". The last principle notes that organizations should take responsibility for the data they retain and

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

show compliance with all the principles. This indicates that organizations should be able to provide evidence of the measure they have taken to ensure compliance.

3.6. Consumer Rights Under GDPR

- **Right to access** – to see or obtain their personal data that has been collected
- **Right to rectification** – to have incomplete or incorrect data about them corrected
- **Right to erasure** – to request deletion of their personal data (also referred to as the "right to be forgotten")
- **Right to restriction of processing** – limiting what personal data about them can be processed and for what purposes
- **Right to object (to processing)** – to opt out of having their data processed at all
- **Right to be informed** – regarding rectification, erasure, or restriction of processing
- **Right to data portability** – to receive a copy of their data in a reasonably usable format to be taken elsewhere
- **Right regarding automated individual decision-making, including profiling** – to opt out of the use of technologies to make decisions regarding the use
- **Legal base for processing personal data -** legally acceptable reasons for companies or other organizations to collect and process personal data. the data subject (e.g. user) has given consent to fulfil or prepare a contract with the data subject to comply with a legal obligation to which the data controller (e.g. company) is subject to protect the vital interests of the data subject or of another natural person in the public interest, or where the data controller is exercising official authority legitimate interests pursued by the data controller or a third party, e.g. for individual, commercial or societal benefit. Legitimate interest is often used to justify data processing, but can be difficult to prove adequately. The safest legal basis for many types and purposes of data processing is obtaining and securely managing user consent, as with a consent management solution.

3.7. Data Security from the Perspective of Data Retainer

The measures that are to be taken by the organization so as to comply with the GDPR requirements vary from technical measures such as two-factor authentication on accounts where personal data are stored, or contracting with cloud providers that use end-to-end encryption; to organizational measures such as staff trainings, data privacy policy , or limiting access to personal data.

Organizations that face a data breach have 72 hours to tell the data subjects or face penalties. (This notification requirement may be waived if the organization use technological safeguards, such as encryption, to render data useless to an attacker.).

Organizations are also asked to have Data Protection Officers (DPO). To appoint DPO is needed under these circumstances:

- **Public authority** — The processing of personal data is done by a public body or public authorities, with exemptions granted to courts and other independent judicial authorities.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

- **Large scale, regular monitoring** — The processing of personal data is the core activity of an organization who regularly and systematically observes its "data subjects" (which, under the GDPR, means citizens or residents of the EU) on a large scale.
- **Large-scale special data categories** — The processing of specific "special" data categories (as defined by the GDPR) is part of an organization's core activity and is done on a large scale.

DPO must have the technical expertise to conduct GDPR assessments and a legal understanding of privacy laws in all jurisdictions in which their organization operates. Tasks of the DPO vary from receiving comments and questions from data subjects related to the processing of their personal data and the GDPR, monitoring an organization's compliance with the GDPR and any other applicable EU member state data protection provisions, train staff on compliance, and perform audits, to performing data protection impact assessments (Article 35 GDPR).

Organizations that breach GDPR face serious penalties. Fines under the GDPR can be up to 4% of a company's global annual turnover or €20 million, whichever is highest. Size of fines is generally determined by the nature, severity and duration of the violation. Additional penalties can include being required to amend or cease data processing. Data privacy violations can also have a significant negative effect on users' trust and a company's reputation.

Although GDPR is a very useful and effective tool to set rules to operation of organization in the field of data protection it does not provide private right of action, so individuals cannot sue companies that violate data privacy. This is governed by the civil proceedings laws of each EU country.

3.8. ePrivacy Regulation

The ePrivacy Directive (EPD) was first passed in 2002. It was amended in 2009 and is colloquially known as the 'cookie law'. Its biggest impact after it was implemented was on the cookie consent pop ups. The ePrivacy Directive works with the GDPR, and in some cases actually overrides it, concerning the confidentiality rules surrounding electronic communications and tracking users.

The ePrivacy Regulation will replace the current ePrivacy Directive. The European Parliament intended to release the ePrivacy Regulation at the same time as the GDPR in 2018 but it did not happen. In February 2021, the EU Council of Ministers agreed on a new version of the EU legislation, albeit still in draft form and the negotiations continue among EU countries due to the complexity of the proposed ePrivacy regulation.

According to the new ePrivacy Regulation the personal data is any information related to a natural person or "data subject" that can identify them, directly or indirectly (e.g. name, address, email address). This definition also includes indirect identifiers such as device ID numbers, IP addresses, mobile location IDs, cookies, and other tracking technologies.

3.9. Ways how to protect your personal data

Create strong passwords

When creating a password, think beyond words or numbers that a cybercriminal could easily figure out, like your birthday. Choose combinations of lower and upper-case letters, numbers,

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

and symbols and change them periodically. It's also better to create a unique password instead of using the same password across multiple sites—a password manager tool can help you keep track.

Don't overshare on social media
We all have that one friend who posts too many intimate details of their life online. Not only can this be annoying, but it can also put your personal information at risk. Check your privacy settings so you are aware of who's seeing your posts, and be cautious when posting your location, hometown, birthday, or other personal details.

Adjust your privacy settings
Mobile devices, browsers, sites, apps, and other web-enabled items such as video games and cameras often have adjustable privacy settings. For devices, this may include the ability to control everything from location tracking to screen locks. For browsers, users can often control things like cookies and pop-ups, while apps and websites such as social media sites generally allow users to control what personal information others can see about them. Never rely on default settings. Review and adjust your privacy settings regularly as they can change from time to time.

Use free wi-fi with caution
A little online shopping never hurt anyone…or did it? Most free public Wi-Fi networks have very few security measures in place, which means others using the same network could easily access your activity. You should wait until you're at home or on a secure, password-protected network before whipping out that credit card.

Watch out for links and attachments
Cybercriminals are sneaky, and will often compose their phishing scams to look like legitimate communications from a bank, utility company, or other corporate entity. Certain things like spelling errors or a different email address than the typical sender can be a clue that the email is spam.

Check to see if the site is secure
Before entering personal information into a website, take a look at the top of your browser. If there is a lock symbol and the URL begins with "https," that means the site is secure. There are a few other ways to determine if the site is trustworthy, such as a website privacy policy, contact information, or a "verified secure" seal.

Consider additional protection
Install anti-virus software, anti-spyware software, and a firewall. For additional protection, you may want to consider cyber insurance, which can keep you and your family safe if you fall victim to a cyberattack.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

3.10. Summary

The protection of personal data is a cornerstone of digital rights in the 21st century. As digital technologies become increasingly embedded in our daily lives, understanding how personal data is collected, processed, and protected is essential—both for individuals and organizations. This unit covered the fundamental principles of personal data protection, key components of the General Data Protection Regulation (GDPR), and practical techniques for securing personal information.

We explored the legal bases for data processing, outlined the responsibilities of organizations in safeguarding data, and discussed individuals' rights under GDPR. Furthermore, we reviewed best practices for maintaining personal security online, such as using strong passwords and avoiding unsafe Wi-Fi networks.

Understanding these elements empowers both the ageing workforce and wider public to participate safely in the digital world. This knowledge also supports organizations in complying with legal standards, building trust with users, and avoiding serious legal or reputational consequences.

Discussion Questions:

- Why is it important for organizations to limit the collection of personal data?
- What challenges might arise in enforcing data protection laws across different legal systems?
- How can individuals ensure they are exercising their data privacy rights effectively?

References and Further Reading

European Commission. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR). Retrieved from https://eur-lex.europa.eu

James Michael. (1994). Privacy and Human Rights 1. UNESCO.

Organisation for Economic Co-operation and Development (OECD). (1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved from https://www.oecd.org

Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Treaty 108). Retrieved from https://www.coe.int

European Data Protection Supervisor. (n.d.). Data protection in the EU. Retrieved from https://edps.europa.eu

European Commission. (n.d.). Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications (ePrivacy Regulation). Retrieved from https://ec.europa.eu

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Chapter 4
Online Fraud and Identity Theft Prevention

4.1. Introduction

Rapid digitalisation and increasing online presence of individuals have not only brought about benefits but also cybersecurity threats and dangers. Online fraud and identity theft have become two of the greatest concerns facing internet users. As more activities (e.g. shopping, banking, and socialising) move to the digital space, cybercriminals exploit the increasing online presence of individuals to mislead them and profit from their personal information (FBI, 2023). According to the Federal Trade Commission (FTC), complaints related to online scams and identity theft increase year by year, which highlights the growing sophistication of fraud tactics and the public's reliance on online services (FTC, 2024). Therefore, understanding how fraudsters and malicious parties operate and learning strategies to safeguard personal data are essential steps for anyone wishing to maintain financial stability and digital peace of mind.

Online fraud encompasses a wide range of deceptive practices, from phishing emails to elaborate social engineering schemes that trick victims into disclosing sensitive data. Cybercriminals often operate internationally, which makes it difficult for law enforcement agencies to track and prosecute them (Interpol, 2025). This global reach amplifies their threat – for example, a seemingly harmless link in a text message could, for instance, lead to malware installation or gaining unauthorised access to bank accounts. Identity theft, which represents a subset of online fraud, involves the unauthorised acquisition and fraudulent use of individual's personal information (e.g. social security numbers, credit card details, email addresses) to commit crimes, apply for loans, or make purchases in the victim's name (FBI, 2023).

Thanks to widespread digitalisation, hackers and scammers exploit the interconnectedness of online platforms. They often abuse data breaches and weak security practices of platforms to collect personal profiles and data. Once they have even fragments of personal data, they can be combined to impersonate victims, which can lead to serious financial and reputational harm.

Types of common scams

Modern and established cybercriminals often tailor their methods and attacks to exploit human psychology and systemic vulnerabilities. For example, phishing and spear phishing remain particularly effective, using emails, text messages, or social media posts that appear authentic but are riddled with malicious links or requests for personal data. Another widespread cyberattack involves tech support impersonation – in such cases, the fraudsters pretend to be reputable companies, institutions or government agencies, offering urgent assistance with "compromised" accounts or devices (FTC, 2024). In recent years, **financial and investment frauds have also rapidly increased, gaining success from excitement around new technologies to win over beginner investors or scare investors about the potential threats to their investment accounts.**

Victims of online fraud often suffer immediate monetary losses, however in some cases, the consequences of online fraud can go beyond the financial realm – being a victim of online

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

fraud may lead to emotional distress, including anxiety and loss of trust in digital services (Wang et al., 2024).

Certain populations, such as older adults or those less familiar with technology, may be at higher risk. Criminals frequently target older users, exploiting their low awareness of cyberthreats, limited technical expertise and digital literacy (FBI, 2023).

The aim of this chapter is to provide readers with knowledge and overview of how to identify, resist, and report online fraud and identity theft. The following parts of the chapter highlight the warning signs of common scams and practical measures that individuals can adopt to protect themselves in the online world.

4.2. Recognising signs of fraud

Cybercriminals continuously keep refining and amening their methods to exploit individuals' trust, curiosity, or lack of technical knowledge and awareness of potential threats. It is essential for whoever is present online to be able to recognise the indicators of potential scams and frauds. **From the persuasive tactics employed in phishing emails to the intricate nature of fake websites, understanding how these schemes operate can help users detect scams and fraud early and take immediate protective steps** (FBI, 2023; Apple, 2025).

Scams often rely on psychological pressure or trickery to encourage quick responses. For example, email or pop-up windows claiming that an account is to be suspended rely on urgency tactics, which push recipients to act without verifying the request (FTC, 2024). Scammers may also demand unusual forms of upfront payment, such as gift cards or wire transfers, while insisting that these methods are faster or more secure; however, they are almost impossible to trace or recover. Moreover, offers that seem too good to be true, like unclaimed lottery winnings or guaranteed high-return investments, are another hallmark of fraudulent activity.

Phishing techniques and social engineering

Phishing remains one of the most pervasive methods of online fraud. Criminals send emails or text messages pretending to be trusted entities – they often include legitimate-looking logos, URLs that closely mimic reputable websites, or messages designed to stir fear or urgency. Some fraudsters employ spear phishing, during which they target specific individuals or organisations using personalised details scraped from social media or data breaches (FBI, 2023). These messages might reference a recent purchase, subscription or event, making the message more convincing.

Beyond digital communications, phone call frauds capitalise on **call spoofing** technology. This method enables scammers to mimic official phone numbers or caller IDs. They may claim to be from government agencies, tech support lines or financial institutions, pressuring victims to disclose sensitive information or perform immediate financial transactions (FTC, 2024). Moreover, **social engineering thrives on emotional manipulation** – fraudsters and scammers tend to leverage fear-based appeals (e.g., threats of arrest) and trust-based tactics (e.g., impersonating a friend in need) to dampen one's rational judgment and secure compliance with their asks. Some of the most common threats targeting individuals are highlighted in table 4.1.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Table 4.1. Most common forms of cyberattacks used to gather personal information

	What are they?	How to recognise them?
Spam	Are unrequested email or junk messages. Can be easy to spot, but still can be harmful when opened, as they can prompt the download of malicious software or virus or request the input of personal data and log in credentials.	• Unknown sender, often with email addresses containing numbers and odd words • Subject that is usually a scam topic • Contain, often urgent, calls to action and request personal information
Phishing	Occurs when an email is sent from an online criminal, but it is disguised as an email from a legitimate, trustworthy sender (e.g., bank or other service provider). The messages or emails are meant to lure the recipient into revealing sensitive or confidential information or impact the recipient in other negative ways. Phishing usually relies on successful social engineering.	• Requests for your username and/or password (credible institutions will not request personal information via email) • Time sensitive threats (e.g., your account will be closed if you do not respond immediately) • Spelling and grammar mistakes • Vague or missing information in the "from" field or email signature • Sender address is a random email address • Impersonal greetings, e.g. "Dear Mr. account holder" • Unexpected files or downloads • Links that don't refer to the sender or sender's organisation (can hover above the link to see the actual URL) • Emails about accounts that you don't have, such as eBay or PayPal, or banks that you don't have accounts with • Emails "from" celebrities • Asks you to reply to "opt out" of a service or plays on human emotions to evoke sympathy, kindness, fear, worry, anxiety.
Spoofing	Is a cyberattack during which a criminal masks their origin as a someone else or an organisation with the aim to steal personal or business information. Spoofing does not hack a sender's account, but it makes an email look like it is coming from the sender, making the recipient more likely to trust the email. It is often used to help to increase the success of phishing attacks.	• Anonymous sender, or masked behind an organisation, the sender does not match the email address • The information in the email signature, e.g., telephone number, doesn't align with what is known about the sender • A well-planned phishing attack will often spoof an email address or domain name that the target trusts to make the message seem legitimate
Pharming	Cyberattack where a malicious, fraudulent website resembles a legitimate website. Pharming attacks aim to convince recipients to interact with fake websites to harvest usernames, passwords and personal data. Pharming often requires the criminal to gain unauthorised access to a system.	• Check the website's URL – almost all major websites handling personal information have URLs begins with **https** (i.e., have a secure connection). If the URL has only http, the connection isn't secure and the site can be unsafe • Spelling of the URL has errors – fake URLs may add a dash between words where the real website has none, or the spelling may be altered by a character – e.g. "examplewebsite.com" and "examp**1**ewebsite.com." where "l" is replaced with number "1".

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

- The look of the website may be odd or look different – e.g. the shape, colour or position of the login buttons may seem off.

Source: Texas Tech University. Scams – Spam, Phishing, Spoofing and Pharming.; Valimail. Complete Guide to Phishing: Techniques & Mitigations; Avast Academy: What Is Pharming and How to Protect Against It.

Fake websites and credential harvesting

Creating fake websites that look almost identical to legitimate ones is another common strategy among cybercriminals. Such "cloned" sites can fool unsuspecting users into entering login details, financial information or other personal data when demanded (CISA, 2021). While many legitimate sites use HTTPS certificates – which can be distinguished by a padlock icon in the browser's address bar – to protect data in transit; however, scammers can also obtain basic certificates, which can mislead visitors into assuming the site is secure.

For example, a sign of fraudulent websites is a slightly altered domain name, such as "*amozn.com*" instead of "*amazon.com*". Criminals may redirect victims to these clone sites via phishing emails, social media ads or pop-up banners. Credential harvesting occurs when the victim willingly inputs information, like email addresses and passwords, into a spoofed login form. Then, the attackers can use the stolen credentials for malicious activities, ranging from unauthorised purchases to large-scale identity theft (Identity Theft Resource Center, 2025).

Example: Phishing email disguised as a bank alert

A user receives an email bearing their bank's logo, warning of "suspicious activity" on their account. The message includes a link to verify personal details.

- Red flags include a **generic greeting**, **slight grammatical errors**, and a **domain name that differs from the bank's official URL** (one can hover above the link to see the URL). Upon manual inspection, the link leads to a cloned site asking for account credentials and social security information.

Recognising the inconsistencies, the user contacts the bank's customer service via a verified phone number and confirms the email is fraudulent, which prevents their account from being compromised.

Example: Romance scam via social media

An individual befriends a seemingly genuine profile on a social network. Over time, the scammer confesses affection towards the individual and shares personal stories.

Eventually, the scammer requests money to cover an emergency medical expense, promising to repay it. Emotional manipulation easily convinces the victim to send funds repeatedly.

After realising, the communication abruptly ends once the victim stops sending money. The victim reports the incident to the platform and local authorities; however, in such scenarios, recovering the funds is unfortunately challenging.

Protecting Sensitive Information

In addition to spotting obvious red flags, one of the most effective ways to mitigating being the victim of fraud is limiting personal data available online that could potentially be harvested.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Disclosing birth dates, addresses and phone numbers, or even photos and other information in posts, on social media can allow scammers to impersonate individuals or guess their security question answers (Kaspersky, 2025). Even small, seemingly negligible details (like pet names or favourite sports teams) can be used to crack password recovery prompts. Therefore, it is often recommended to adopt a **"pause and verify" mindset to online presence** – if a [particularly an unexpected] message or phone call requests private details or urges immediate action, it is often best to hang up, close the email, exit the website and verify the request through an official, trusted channel (FBI, 2024).

4.3. How to safeguard against identity theft

Identity theft arises when criminals obtain and misuse personal information to commit fraud under someone else's name. As cyber threats and their level of sophistication evolve, protecting oneself against identity theft requires vigilance, from adopting proactive security habits to monitoring financial accounts for suspicious transactions (ENISA, 2022). Below is a summary of simple protective measures and how they can be used to mitigate being the victim of online fraud.

Using strong passwords and multi-factor authentication

Simple precautions like **using unique passwords for different accounts and enabling multi-factor authentication** can significantly reduce exposure to identity theft (Microsoft, 2025). Multi-factor authentication adds a second layer of validation, in the form of a code sent via text or a biometric scan, thereby stalling attackers who may have guessed or stolen a password. For example, password managers (e.g., NordPass, TotalPassword, Dashlane) can help to simplify the creation and storage of complex passwords, ensuring that every account has a distinct password that is difficult for criminals to compromise.

Using secure devices and networks

It is crucial to keep **the software and operating systems on phones, computers, tablets and other personal devices updated** for fixing known security vulnerabilities of devices (CISA, 2021). In addition, installing reputable antivirus programs and firewalls can help to detect malicious activity early on. When using public Wi-Fi, individuals should avoid accessing sensitive accounts unless connected through a VPN (virtual private network), which encrypts traffic and obscures data from potential eavesdroppers (NIST, 2018; Putra, 2025). If possible, it is recommended to rather use phone data or hotspot your data to other devices you are using.

Minimising data sharing

Limiting the personal details shared online can substantially hinder identity thieves' ability to piece together a complete profile. Before filling out web forms or social media bios, one should always consider whether the requested information is truly necessary. Moreover, **deleting old accounts and unsubscribing from outdated email lists or advertisements** prevents dormant data repositories from becoming convenient targets. Even small measures, like removing birth dates or addresses from social media profiles can reduce vulnerability to information abuse for uncovering answers to common security questions.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Monitoring financial, investment and personal accounts

Monitoring bank statements, investment account statements, credit card transactions and utility bills for unusual charges are ways to detect unusual transactions and account misuse and theft (Diverge IT, 2024). Even small, recurring transactions or debits may indicate that the thieves are testing compromised details before launching more harmful attacks. Many banking apps and online portals allow users to set up **real-time alerts for transactions surpassing a certain threshold**, which enables users to take swift responses to suspicious activity. In addition, setting up multi-factor authentication can help secure one's accounts, thus mitigating the potential damage in case the login information have been compromised. For older adults or high-risk individuals, it can be helpful to arrange for trusted relatives or friends to help review statements.

In addition, if applicable, it is important to **regularly review credit reports**, as doing so can help to detect fraudulent activity. For example, in the United States, individuals can request free copies of their credit reports from the main credit bureaus (FTC, 2024). Unfamiliar credit applications, new loans or unexplained inquiries can signal identity theft. Promptly identifying and refuting the inaccuracies with the credit bureau and reporting the issue with financial institutions can prevent further damage of being a victim of identity theft.

Responding to suspicious activity

If one suspects that their identity has been stolen or personal bank, or investment, accounts have been misused or compromised, it is important to **act fast to prevent extensive harm**. Once a breach is detected, it is crucial to **change the passwords for all accounts sharing the same or similar credentials. Running a thorough malware scan** on the affected device helps to ensure that no keyloggers or trojans remain active (NIST, 2018). In more severe cases – such as large-scale data breaches and leaks, affected individuals may receive notifications from service providers prompting them to increase their vigilance, monitor accounts and change their passwords (ENISA, 2022).

The fraud should also be reported to targeted institutions and service providers. Moreover, victims of identity theft should file a report with local law enforcement agencies and, if relevant, notify relevant government agencies if a social security number is compromised (FBI, 2023). Thorough documentation and evidence of every fraudulent transaction or activity can prove invaluable when disputing charges and mitigating any adverse consequences.

Methods for ensuring safe online behaviour

It is suggested to **use VPNs (virtual private networks)**, which provide users an encrypted tunnel for internet traffic, which safeguards data transmitted over public or untrusted networks. By masking IP addresses and encrypting information transferred, VPNs hinder malicious actors from accessing usernames, passwords, or personal details (Microsoft, 2025; Putra, 2025). Users should select reputable VPN services that are transparent about their logging policies and security features – for example, NordVPN, Surfshark, ExpressVPN, Norton, Proton VPN. It is also important to not trust free VPN providers, as they may not offer full security.

Authentication Apps and Hardware Tokens

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Whenever possible, **multi-factor authentication should be used to secure accounts**, by issuing codes via text, phone calls or authenticator apps. Multi-factor authentication offers advanced login security by generating time-sensitive codes that must be entered alongside a password (CISA, 2021). Popular authentication apps are for example Google Authenticator, Microsoft Authenticator, or Authy can hardware tokens, such as YubiKeys, supply an additional "something you have" factor. Even though these measures may seem technical, they significantly reduce the risk of unauthorised access to accounts, which is particularly useful for sensitive accounts like email, cloud storage, or financial services.

Password managers also represent a useful tool that can help secure accounts. However, while password managers streamline credential management, they also require thoughtful use. Particular attention must be placed to protecting the password manager's "master password" – it should be protected with the same level of security as a bank PIN code or physical vault key (BBB, 2023). Moreover, it is crucial to periodically review stored credentials to remove obsolete entries and ensure that all active passwords follow recommended complexity guidelines (e.g., at least 12 characters, numbers, mixed case, symbols, etc.). Enabling multi-factor authentication on the password manager itself adds another layer of security if the device with the app is stolen or lost.

Example: Early detection of unfamiliar charges
A consumer notices a 2-euro test charge on their credit card statement. By contacting the card issuer immediately and requesting an account freeze, the consumer prevents any large-scale fraudulent purchases. These days, the cards can be also frozen in mobile banking apps, which allows for speedy response. In addition, the spending limit can also be reduced to prevent large transactions from being made.
Key takeaway: Even small discrepancies and activity can signal bigger identity theft attempts, thus highlighting the importance of proactive monitoring.

Example: Protecting a stolen smartphone
After losing a phone, the owner quickly uses a remote-wipe feature offered by the device's manufacturer. This action blocks and deletes all data from the phone, including stored passwords and personal messages.
As next steps, the owner changes their email, social media and banking credentials, which helps them to ensure that the lost device cannot grant unauthorised access to these services.
Key takeaway: Having "Find My Device" or equivalent services enabled, along with backup security measures, can mitigate losses if physical devices go missing.

Sources: N26. How to protect yourself when your phone is lost or stolen.; Apple. If your iPhone or iPad was stolen.; Google. Find, secure, or erase a lost Android device.

By integrating measures of using strong passwords, having vigilant financial oversight, responding quickly to incidents and maintain mindful online behaviour, individuals can significantly lower their vulnerability to identity theft and account misuse. While no approach guarantees absolute immunity from cyber-attacks, **building multiple layers of defence** helps individuals to detect and mitigate fraudulent activity before it escalates, ultimately preserving both financial well-being and peace of mind (BBB, 2023).

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

4.4. Summary

Online fraud and identity theft continue to pose significant threats as criminals develop more sophisticated attacking methods and exploit gaps in users' awareness or security practices. From phishing emails to sophisticated credential-harvesting websites, cyberthreats are now present in almost every aspect of digital life (FBI, 2023). Therefore, recognising the red flags serves as the first line of protection, empowering individuals to detect scams before major harm can occur (FTC, 2024).

However, awareness alone is not enough. It is crucial to implement effective prevention measures, such as maintaining strong passwords, enabling multi-factor authentication, and monitoring accounts for even small irregularities (ENISA, 2022). In addition, individuals should limit the amount of personal information they make public, as online profiles often provide more data than users realise.

All in all, safeguarding personal information is an ongoing process that requires both vigilance and adaptability. As technology advances, so do cybercriminals' tactics, which makes it essential to stay updated on new threats and best practices. Through consistent monitoring, timely responses to suspicious activity, and a willingness to invest in robust security measures, individuals can secure their online presence and their financial and mental well-being.

References and Further Reading

AARP. (2022). 2022 TECH TRENDS AND THE 50-PLUS. Available at: https://www.aarp.org/content/dam/aarp/research/surveys_statistics/technology/2021/2022-technology-trends-older-americans.doi.10.26419-2Fres.00493.001.pdf

Apple. (2025). Recognize and avoid social engineering schemes including phishing messages, phony support calls, and other scams. Available at: https://support.apple.com/en-us/102568 [Accessed: Feb 2, 2025].

BBB. (2023). Scam Tracker. Risk Report. Better Business Bureau. Available at: https://bbbmarketplacetrust.org/wp-content/uploads/2024/04/2023-BBBScamTracker-RiskReport-US-040224.pdf

CISA. (2021). Understanding Website Certificates. Cybersecurity & Infrastructure Security Agency. Available at: https://www.cisa.gov/news-events/news/understanding-website-certificates

Diverge IT. (2024). Top Strategies for Financial Fraud Prevention: Checklist for Fraud Protection. Available at: https://www.divergeit.com/blog/financial-fraud-prevention

ENISA. (2022). Threat Landscape 2022: Overview of Current and Emerging Cyberthreats. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

FBI. (2024). 2023 Internet Crime Report. Federal Bureau of Investigation. Available at: https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

FTC. (2024). Consumer Sentinel Network Data Book 2023. Federal Trade Commission. Available at: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2023

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Identity Theft Resource Center. (2025). 2024 Data Breach Report. Available at: https://www.idtheftcenter.org/wp-content/uploads/2025/01/ITRC_2024DataBreachReport_Final.pdf
Interpol. (2025). Cybercrime. Available at: https://www.interpol.int/en/Crimes/Cybercrime [Accessed: Feb 2, 2025].
Interpol. (2025). Coordinating a global response to cyberthreats. Available at: https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-threat-response [Accessed: Feb 2, 2025].
Interpol. Financial crime – don't become a victim! Available at: https://www.interpol.int/en/Crimes/Financial-crime/Financial-crime-don-t-become-a-victim [Accessed: Feb 2, 2025].
Kaspersky. (2025). Top 15 internet safety rules and what not to do online. Available at: https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online [Accessed: Feb 2, 2025].
Microsoft. (2025). Microsoft Digital Defense Report 2024. Available at: https://www.microsoft.com/en-us/security /microsoft-digital-defense-report-2024
NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
Putra, I. B. (2023). Public Wifi Risks - Cyber Security. Available at: https://www.linkedin.com/pulse/public-wifi-risks-cyber-security-ichsan-budiman-putra-mos-mtcna/ [Accessed: Feb 2, 2025].
Wang, J., Zhang, L., Xu, L., & Qian, X. (2024). The dynamic emotional experience of online fraud victims during the process of being defrauded: A text-based analysis. Journal of Criminal Justice, 94, 102231.

Additional resources

ABC News in Depth. (2021). How to avoid falling victim to an online financial scam. Available at: https://www.youtube.com/watch?v=QXbF46RvY5k
EUCPN. How online fraud works and how to prevent it. Available at: https://eucpn.org/sites/default/files/document/files/2302_ENG_PAPER_Online%20fraud_LR.pdf
Macmostvideo. (2024). 10 Common Internet Scams and How To Avoid Them. Available at: https://www.youtube.com/watch?v=CDhAOvsyw2s
Microsoft. Protecting yourself from identity theft online. Available at: https://support.microsoft.com/en-us/office/protecting-yourself-from-identity-theft-online-6019708f-e990-4894-9ca7-fdb53ee70830
Money Coach. (2016). How to Prevent Identity Theft. Available at: https://www.youtube.com/watch?v=qBDCnKfExw4
TEDx. (2017). How data brokers sold my identity | Madhumita Murgia. Available at: https://www.youtube.com/watch?v=AU66C6HePfg
TEDx (2022). What an Identity Theft Victim Can Teach Us About Cybercrime | Sandra Estok. Available at: https://www.youtube.com/watch?v=v46TAoZl1XI

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Chapter 5
Safe Internet Browsing

5.1. Introduction

The internet is an indispensable asset used daily by people to access work opportunities, education, entertainment, and social interaction. But it brings with it numerous cyber threats that compromise privacy, financial details, and online identity. Internet browsing by many is an ordinary task that one performs without an awareness of the risks that lurk with every click and open the doors to malware attacks, phishing schemes, identity thefts, and breaches.

Specifically, the elderly can be more susceptible to these dangers through several factors that include poor digital literacy, lack of awareness with contemporary internet security protocols, and the nature of evolving cyber threats that usually adversely exploit knowledge gaps that exist because of generational differences. It thus becomes important that people are aware of the security options presented by their internet browsers, know how to set the options to provide maximum protection, and how to protect themselves against typical internet dangers.

This chapter focuses on **safe internet browsing** practices with an emphasis on **browser security settings and configurations**. By the end of this chapter, readers will be equipped to:

- **Understand the risks associated with internet browsing** and why secure browsing is essential.
- **Learn how to adjust security settings** in different browsers to enhance protection against various online threats.
- **Identify and mitigate risks such as malware, phishing, and tracking** through proper browser configurations.
- **Apply these techniques in real-world scenarios**, enabling safer online experiences.

The goal of this chapter is to provide both the theoretical foundation and practical tools necessary for anyone seeking to navigate the internet securely.

5.2. Theoretical Framework / Key Concepts

To comprehend how to secure internet browsing, it's essential to first understand some of the fundamental concepts that underpin browser security and the mechanisms by which threats are introduced to users.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

5.2.1. Browser Security and Its Role in Safe Browsing

A browser is the main software to access the internet. While surfing on the internet, the browser serves like an intermediary taking the user to and from the content on websites. The browser gets and shows the content on the web and handles user interaction on the webpages. Nevertheless, an improperly set-up browser can become an entry point to several types of cyber-attacks too.

New-generation web browsers are equipped with several built-in safety features to protect users against malware, phishing schemes, and data breaches. Unfortunately, not everyone knows about these features or how to set them up to make their browsing more secure.

5.2.2. HTTPS (Hypertext Transfer Protocol Secure)

One of the greatest internet-browsing security protocols is HTTPS. Webpages that employ HTTPS (instead of outdated HTTP protocol) encrypt data being transmitted between the site and the browser. The encryption makes it so that log-in details, payment data, and personal data cannot be intercepted by malicious third parties during transmission.

Without HTTPS, any information you send across the internet, including your passwords, your credit card details, and your personal info, becomes vulnerable to hackers' access. Therefore, browsing without HTTPS is unsafe by nature.

5.2.3. Cookies and Tracking Technologies

Cookies are tiny text files that websites save on the user's device to maintain records of the user's browsing habits. Cookies are usually benign and used to maintain login details and preferences; however, they can sometimes be used to track users on several websites to gather data or display advertising material.

Most people know about cookies, but most people don't know that some types of cookies (third-party cookies) are privacy-compromising because they enable advertisers or malicious parties to track individuals from site to site and create a profile about what one does without one's awareness or permission.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

5.2.4. Phishing and Social Engineering

Phishing is a form of cyber-attack whereby attackers masquerade as a reputable organization (such as a bank, social networking platform, or respected company) to obtain user-sensitive data like passwords, card details, or personal information by deceiving users. Phishing attacks are mostly perpetrated through emails but may also take place through pop-up windows, fake websites, or telephone calls.

Phishing websites usually resemble legitimate ones, complete with recognizable logos and URLs, and are made to trick people into submitting confidential information. One way to fight phishing is to make sure that the browser's anti-phishing tools are activated.

5.2.5. Malware and Malicious Websites

Malware refers to any software meant to destroy a system or to steal data. It is delivered through what appears to be harmless websites, malvertising, or attachments to emails. It can vary from viruses and trojans to ransomware that encrypts your files or devices until one pays up.

5.2.6. Browser Extensions and Add-ons

Browser extensions and add-ons are little software programmes that supplement the browser's capabilities. Some are benign and provide important features (ad blockers or password manager being some examples), but others can include security threats, particularly if you download them from unreliable sources or capture personal data without asking you.

5.3. Practical Applications

5.3.1. Adjusting Browser Security Settings:

In this section, we'll explore how to adjust the security settings in various popular browsers to maximize protection against threats like phishing, malware, and data breaches.

Google Chrome

- **Enable Safe Browsing:**
  Google Chrome comes with a built-in **Safe Browsing** feature that warns users when

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

visiting potentially harmful websites. To enable this feature, go to **Settings > Privacy and Security > Security**, and choose **Standard Protection** or **Enhanced Protection** for better security. Enhanced Protection automatically sends data to Google to help identify and block dangerous websites.

- **Block Pop-ups and Redirects:** Pop-ups are commonly used for advertising purposes, but they can also be exploited by malicious websites to download malware or redirect users to phishing sites. To block pop-ups, go to **Settings > Privacy and Security > Site Settings**, then under **Content**, select **Pop-ups and redirects** and toggle it to **Blocked**.
- **Manage Cookies and Site Data:** Chrome allows you to control how cookies are handled. To manage cookies, go to **Settings > Privacy and Security > Cookies and Other Site Data**. You can opt to block third-party cookies, delete browsing data automatically, or use **Incognito Mode** for private browsing sessions.
- **Install Security Extensions:** Google Chrome has a wide variety of security extensions available in the Chrome Web Store. Extensions like **uBlock Origin** (for blocking unwanted ads) and **HTTPS Everywhere** (to ensure secure connections) can enhance your browsing security.

Mozilla Firefox

- **Activate Enhanced Tracking Protection (ETP)** Firefox's Enhanced Tracking Protection (ETP) feature blocks known trackers that monitor your browsing activity across the web. This setting can be accessed via **Settings > Privacy & Security > Enhanced Tracking Protection**, where you can toggle protection on or off.
- **Enable HTTPS-Only Mode:** To ensure all your connections are encrypted, activate **HTTPS-Only Mode**. This mode can be enabled by going to **Settings > Privacy & Security**, then selecting **HTTPS-Only Mode** to prevent non-secure connections.
- **Phishing and Malware Protection:** Firefox includes built-in phishing protection that blocks dangerous websites. To ensure this feature is active, navigate to **Settings > Privacy & Security**, and ensure the option for **Block dangerous and deceptive content** is selected.

Microsoft Edge

- **Turn on SmartScreen Filter:** Microsoft Edge has the **SmartScreen** filter that helps block phishing websites and

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

malware downloads. To activate it, go to **Settings > Privacy, Search, and Services** and ensure that **Microsoft Defender SmartScreen** is turned on.

- **Control Cookies:** Edge provides several levels of cookie blocking. To manage cookies, go to **Settings > Cookies and Site Permissions > Manage and Delete Cookies** and configure your preferences.

5.3.2. Implementing Phishing Protection

Phishing attacks are one of the most common ways cybercriminals attempt to steal sensitive information. Most modern browsers offer anti-phishing tools to help identify and block malicious sites.

- **Phishing Warnings in Google Chrome:** Chrome's phishing detection alerts you when you attempt to visit a suspicious site. It checks the URL and warns you if it appears to be a known phishing site. Additionally, Chrome's **Safe Browsing** feature works in conjunction with this to keep your data safe.
- **Phishing Warnings in Mozilla Firefox:** Firefox not only warns users about potential phishing websites, but it also integrates with the **Google Safe Browsing** service, which provides updated lists of dangerous sites. Users can check their settings under **Privacy & Security > Security** to ensure this feature is enabled.
- **Phishing Warnings in Microsoft Edge:** Similar to other browsers, Microsoft Edge uses **Microsoft Defender SmartScreen** to protect against phishing and malware. This feature can be found and activated in **Settings > Privacy, Search, and Services > Microsoft Defender SmartScreen**.

5.3.3. Enhancing Privacy through Browser Extensions

While many users install browser extensions to improve their browsing experience, some of these tools can enhance security and privacy as well. Examples of security-focused extensions include:

- **AdBlock Plus:** Blocks intrusive ads that can lead to malware infections.
- **LastPass:** A password manager that ensures you are using strong, unique passwords for each website.
- **HTTPS Everywhere:** Forces the browser to use secure HTTPS connections where possible.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

5.4. Summary

In conclusion, protecting your online surfing experience is all about knowing the risks surrounding internet activity and taking practical measures to counter them. Browser protection options are important in protecting users from being victims of phishing and malware attacks and violation of privacy. Proper configuration of the browser, the activation of built-in protection features, and the application of safety-enhancing extensions are all measures through which users can benefit from a safer and more secure online experience.

References and Further Reading

Chen, G., Johnson, M.F., Marupally, P.R., Singireddy, N.K., Yin, X., Paruchuri, V., 2009. Combating Typo-Squatting for Safer Browsing. 2009 INTERNATIONAL CONFERENCE ON ADVANCED INFORMATION NETWORKING AND APPLICATIONS WORKSHOPS: WAINA, VOLS 1 AND 2. https://doi.org/10.1109/WAINA.2009.98

Dauce, F., Loveluck, B., Ostromooukhova, B., Zaytseva, A., 2019. FROM CITIZEN INVESTIGATORS TO CYBER PATROLS: VOLUNTEER INTERNET REGULATION IN RUSSIA. LABORATORIUM-RUSSIAN REVIEW OF SOCIAL RESEARCH. https://doi.org/10.25285/2078-1938-2019-11-3-46-70

European Union Agency for Cybersecurity (ENISA). (2020). Online Safety for Seniors.

Georgiadou, A., Xinogalos, S., 2023. Prospective ICT Teachers' Perceptions on the Didactic Utility and Player Experience of a Serious Game for Safe Internet Use and Digital Intelligence Competencies. COMPUTERS. https://doi.org/10.3390/computers12100193

Ilangakoon, S.D., Jayakody, J.A.D.C.A., 2016. Awareness of Sri Lankan Internet Users on Web Browsing Related Threats and Vulnerabilities. 2016 IEEE INTERNATIONAL CONFERENCE ON INFORMATION AND AUTOMATION FOR SUSTAINABILITY (ICIAFS): INTEROPERABLE SUSTAINABLE SMART SYSTEMS FOR NEXT GENERATION, International Conference on Information and Automation for Sustainability.

Google Chrome Help. (2021). Managing Cookies. Retrieved from https://support.google.com

Mozilla Firefox Help. (2021). Enhance Privacy and Security. Retrieved from https://support.mozilla.org

Symantec. (2022). Phishing and Malware: What You Need to Know. Retrieved from https://www.broadcom.com

Retrieved from https://www.enisa.europa.eu

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

NortonLifeLock. (2022). Browser Security: Best Practices for Safe Browsing. Retrieved from https://www.norton.com

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Chapter 6
Antivirus Software and Firewalls

6.1. Introduction

In today's digital age, where cyber threats are growing more sophisticated, protecting your devices and personal data is more important than ever. Two essential tools in digital security are antivirus software and firewalls. Understanding what they do, how they work, and how to use them effectively can greatly reduce the risk of malware, hacking, and identity theft.

6.2. Choosing and Using Antivirus Tools Effectively

Antivirus software is designed to detect, block, and remove malicious software such as viruses, ransomware, spyware, and trojans. With so many options available, selecting the right antivirus tool depends on your needs, device, and level of experience.

Key Features to Look for:

- Real-time protection: Scans files and programs as they run.
- Automatic updates: Keeps the virus database current with the latest threats.
- Email protection: Scans attachments and links for malicious content.
- Web protection: Warns or blocks access to unsafe websites.
- System performance impact: A good antivirus should be effective without slowing down your computer.

6.3. How Antivirus Software Works

Modern antivirus software uses multiple techniques:

- **Signature-based detection** – compares files against a database of known threats.
- **Heuristic analysis** – examines behavior and code patterns to detect unknown threats.
- **Sandboxing** – runs suspicious files in a virtual environment to monitor behavior.
- **Cloud-based scanning** – checks files against cloud databases for up-to-date threat detection.
- **Machine learning** – improves detection capabilities by learning from large data sets of malware behavior.

6.4. Types of Antivirus Software

Standalone Antivirus Programs

- Basic protection against malware.
- **Examples**: Microsoft Defender, AVG AntiVirus Free

Internet Security Suites

- Bundled with firewall, VPN, parental controls, and password managers.
- **Examples**: Norton 360, Kaspersky Internet Security

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Cloud-based Antivirus

- Light on system resources; relies on cloud scanning.
- **Examples**: Panda Cloud Antivirus

Enterprise Antivirus Solutions

- Tailored for organizations with centralized management.
- **Examples**: Symantec Endpoint Protection, Sophos

Tips for Using Antivirus Software Effectively:

- Keep it updated: An outdated antivirus is almost as bad as having none.
- Run regular scans: Schedule weekly or daily scans for full system checks.
- Don't install multiple antivirus programs: They may conflict with each other and reduce overall protection.
- Watch for warnings: Pay attention to alerts and take appropriate action.

6.5. Popular Antivirus Programs

- **Free Options:** Avast Free Antivirus, AVG, Microsoft Defender
- **Paid Options:** Norton, McAfee, Bitdefender, Kaspersky

6.5.1. Comparison of Popular Free Antivirus Programs

- Below is a brief overview of three widely-used free antivirus programs: Avast Free Antivirus, AVG AntiVirus Free, and Microsoft Defender. Each has strengths and limitations depending on the user's needs.

Avast Free Antivirus

Avast Free Antivirus is a popular and well-established antivirus solution offering solid protection against malware, spyware, ransomware, and phishing. It includes additional tools like a Wi-Fi security scanner and a password manager.

- Pros:
- Strong malware detection rates.
- Includes extra features (e.g., software updater, Wi-Fi inspector).
- Intuitive and easy-to-use interface.
- Available on Windows, Mac, and Android.
- Cons:
- Can be resource-heavy (slows down older PCs).
- Frequent pop-ups encouraging users to upgrade to premium.
- Previously faced criticism for selling user data (program shut down).

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

AVG AntiVirus Free

AVG, which is owned by the same company as Avast, offers robust malware protection with a focus on simplicity and performance. It shares the same core engine as Avast but with a different interface and slightly fewer extra tools.

- Pros:
- Excellent virus and malware detection.
- Low system impact—great for older or lower-powered devices.
- Real-time protection and email scanning.
- Clean, user-friendly interface.
- Cons:
- Ads promoting paid version.
- Fewer extra tools compared to Avast.
- Occasional reminders to install other AVG products.

Microsoft Defender

Built into Windows 10 and 11, Microsoft Defender provides integrated antivirus and anti-malware protection. It updates automatically via Windows Update and is deeply integrated with the operating system.

- Pros:
- No need to install anything—built into Windows.
- Minimal system impact.
- Good overall protection for average users.
- Integrated with Windows Firewall and security settings.
- No ads or upgrade nags.
- Cons:
- Fewer features than third-party antivirus software.
- Not as effective at detecting zero-day threats compared to top competitors.
- Interface is less user-friendly for beginners.

6.5.2. Recommendations for Different Users

User Type	Recommended Antivirus	Why?
Beginners/Home Users	Microsoft Defender, AVG Free	Simple, reliable, integrated with Windows
Advanced Users	Bitdefender, ESET, Kaspersky	Customization, strong protection
Budget-Conscious Users	Avast Free, Panda Dome Free	Decent free protection

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Small Businesses	Norton Small Business, Sophos	Centralized management, scalability

6.6. Understanding and Setting Up Firewalls

A firewall acts as a digital barrier between your device or network and the internet. It monitors incoming and outgoing traffic and blocks suspicious activity. Think of it as a security guard that checks everyone coming in or out of a building.

Types of Firewalls:

- **Software Firewalls:** Installed on individual devices (e.g., Windows Firewall).
- **Hardware Firewalls:** Built into routers or standalone devices; used in homes and businesses.
- **Cloud-based Firewalls:** Often used by businesses to protect online infrastructure.

How to Set Up a Firewall:

Windows Users:

- Go to Settings > Privacy & Security > Windows Security > Firewall & Network Protection. Make sure it's turned on for all networks (public, private, domain). Customize settings if needed to allow or block specific apps.

Mac Users:

- Go to System Settings > Network > Firewall. Turn it on and configure rules for apps or services.

Router Firewalls:

- Access your router settings via a web browser. Enable the firewall and adjust settings if necessary (refer to the user manual).

Best Practices:

- Always keep your firewall enabled.
- Use both a firewall and antivirus together for layered protection.
- Limit unnecessary inbound connections, especially from unknown devices or sources.
- Regularly check firewall logs (for advanced users) to monitor suspicious activity.

6.7. Summary

Antivirus software and firewalls are essential components of a strong cybersecurity setup. While antivirus protects your device from threats, firewalls help prevent unauthorized access. Using both tools together—and using them properly—greatly increases your digital safety. Whether you're working from home, shopping online, or just browsing, these tools can give you peace of mind in an increasingly connected world.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

References and Further Reading

AVAST Software. (n.d.). Avast Free Antivirus. Retrieved from https://www.avast.com/free-antivirus-download

AVG Technologies. (n.d.). AVG AntiVirus Free. Retrieved from https://www.avg.com/en-eu/free-antivirus-download

Bitdefender. (n.d.). Bitdefender Antivirus Solutions. Retrieved from https://www.bitdefender.com

Kaspersky. (n.d.). Kaspersky Antivirus Software. Retrieved from https://www.kaspersky.com

McAfee. (n.d.). McAfee Antivirus Software. Retrieved from https://www.mcafee.com

Microsoft. (n.d.). Microsoft Defender Antivirus in Windows. Retrieved from https://support.microsoft.com/en-us/windows/microsoft-defender-antivirus-in-windows

NortonLifeLock Inc. (n.d.). Norton Antivirus. Retrieved from https://us.norton.com/products/norton-antivirus

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Chapter 7
Social Engineering Attacks and Prevention

7.1. Introduction

In today's lesson, we will focus on social engineering attacks. Cybersecurity is not only about technical measures but also involves protecting the human factor. Therefore, social engineering attacks are carried out not through technological vulnerabilities but by exploiting human weaknesses.

What We Will Learn Today:

- What is social engineering and why is it so dangerous?
- Why do attackers target people?
- What role does social engineering play in the world of cybersecurity?

7.2. What is Social Engineering?

Are cyberattacks carried out solely through software and technical security vulnerabilities? If your answer is "yes," you're mistaken. Cyberattacks can be carried out not only through technical methods but also by distracting people, gaining their trust, or manipulating their emotions. These types of attacks are called social engineering attacks.

Social engineering is a type of cyberattack where attackers manipulate human psychology to steal personal information, system login credentials, or financial data.

The Key Point:

These attacks do not target a software vulnerability directly, but rather aim at human distractions and trust.

A real-life example: An attacker may pose as a bank employee, technical support team member, or a government official to deceive users.

For example: "Hello, we're calling from XXX Bank's fraud prevention team. We've detected suspicious activity on your account. For your security, please share your ID number and password."

This type of call may seem legitimate, but it is actually a fake attack. If the victim shares their information, the attackers can misuse it to log into the account and cause financial losses.

In Summary:

- The attacks exploit people's fear, trust, curiosity, and carelessness.
- They deceive individuals into sharing their information willingly.
- Unlike traditional cyberattacks, they do not require a system vulnerability.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

7.3. Why Is Social Engineering Used?

So, why do cyber attackers prefer to manipulate people instead of using complex technical methods? Here are a few key reasons:

7.3.1. The Human Factor is Weaker Than Security Systems

Is hacking a computer system harder than deceiving a person? Yes, in many cases, deceiving a person is much easier than bypassing a security system.

For example: Instead of hacking through a company's firewall, a hacker may deceive an employee by saying, "I'm from the IT department, I need to perform an update on your system. Please give me your username and password." This way, they can directly obtain the information.

- Advanced security software can detect and block malicious codes.
- However, a person must be aware to recognize an attack.. That's why attackers aim to bypass security systems by exploiting human errors.

7.3.2. Social Engineering Attacks Carry Lower Risks

Directly attacking a computer system is a high-risk endeavor for cybercriminals. Most advanced security systems can immediately detect unauthorized access and block attacks. However, when information is obtained by deceiving a person, tracking the attacker and capturing them can be much more difficult.

Example: Instead of attempting to infiltrate a government system, a hacker may deceive an employee to obtain login credentials. This way, they can access the system without leaving a trace.

When comparing Social Engineering Attacks to other types of attacks:

- They require less technical knowledge.
- It is possible to execute the attack without leaving a trace.
- The risk of legal action is lower.

7.3.3. No Matter How Advanced Technology Becomes, Humans Can Be Manipulated

Today, AI-powered cybersecurity systems, encryption techniques, and firewalls have advanced significantly. However, human nature remains unchanged. People tend to trust, may be careless, can submit to authority, and act out of curiosity. Attackers exploit these weaknesses to bypass cybersecurity systems.

Example: A hacker might deceive an employee in a company via email, saying, "Click the link below to access this confidential company document." A curious employee who clicks the link could inadvertently allow malware to infiltrate the system.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

-Human nature is inherently prone to trust and make mistakes.
-Cyber attackers exploit these weaknesses to gain access to systems.

7.4. Why is Social Engineering a Major Threat in Cybersecurity?

Social engineering attacks create significant security vulnerabilities for individuals, companies, and governments. Technological security measures can be ineffective against human error.

Why is it a major threat?

- High success rate: People can't always tell whether emails or phone calls are fraudulent.
- Can bypass corporate security measures: No matter how strong a system is, if inside information is leaked, all security walls are rendered useless.
- Works quickly and silently: Attacks can happen unnoticed, and when systems are affected, it's often too late.

7.4.1. Why is Social Engineering a Threat That Needs Attention?

- Social engineering attacks are one of the simplest but most effective attack methods.
- An attacker can bypass all security measures by manipulating victims without needing technical skills.
- Therefore, not only software security but also raising awareness among individuals is an important part of cybersecurity.

7.4.2. Examples of social engineering attacks

In this lesson, we will explore the most common examples of social engineering attacks in detail. In our previous lesson, we learned what social engineering is and how attackers manipulate human psychology.

The learning objectives:

- Understand the most common types of social engineering attacks
- Better grasp these attacks through real-life examples
- Raise awareness to secure our own safety

Phishing Attacks – The Most Common Social Engineering Method

Phishing attacks aim to obtain sensitive information from individuals by using emails, SMS, or fake websites.

- **How It Works?**
  Attackers try to deceive victims by sending messages that appear trustworthy but are fake. Often, banks, technology companies, or official institutions are impersonated. When the victim clicks on a malicious link in these messages, they unknowingly provide their login credentials to the attackers.

- **Real World Example:**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

In 2020, phishing attacks targeting the executives of Google and Facebook used fake emails, resulting in the theft of over $100 million.

- **Example Scenario:**
  A user receives an email in their inbox titled “XXX Bank Security Update.”

- **The email looks like this:**
  Dear Customer, A suspicious transaction has been detected on your account. To ensure your security, please click on the link below to verify your credentials.
  [Go to Fake Bank Website]
  Bank Security Department

- **What happens if the victim takes action?**
  If the victim clicks on the fake link and enters their bank details, those credentials will be directly captured by the attackers. The attackers can then drain the victim’s account or steal sensitive data within minutes.

- **Lesson Learned:**
  - Banks or official institutions will never ask for your password via email!
  - Always check the URL before clicking on suspicious links.
  - Never enter information on websites that don't have HTTPS!

Phone Scam (Vishing) – Voice Phishing
Vishing (voice phishing) is a social engineering attack where attackers deceive victims through phone calls.

- **How It Works?**
  The attacker pretends to be a bank employee, technical support team, or an official authority, convincing the victim to share sensitive information.

- **Real World Example:**
  In 2019, a CEO in the UK lost $243,000 after being tricked by AI-supported fake phone calls from scammers.

- **Example Scenario:**
  When someone answers their phone, they hear, "Hello, I’m calling from the security department of XXX Bank."

- **The attacker might use statements like:**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

"We've detected suspicious activity on your account! To verify your identity, you must provide your card number, expiration date, and CVV code. Otherwise, your account will be blocked!"

- **What happens if the victim takes action?**
  If the victim panics and shares their information, the attacker can use it to withdraw money from the bank account or make online purchases.

- **Lesson Learned:**
  - No bank will ever call you asking for passwords or credit card information!
  - Call the official number yourself to verify the caller.
  - Be cautious of calls that try to create panic or urgency.

USB Trap (Baiting) – A Trap Using Your Curiosity

Baiting is a method where attackers exploit people's curiosity to expose them to malware.

- **How It Works?**
  Attackers leave USB drives containing malicious software in company entrances or public areas. When a curious person plugs the USB into their computer, the malware runs and infects the system.

- **Real World Example:**
  In 2016, malicious USB drives were found in a parking lot by employees of the U.S. Department of Defense, and when plugged in, they infected the computers with a virus.

- **Example Scenario:**
  An employee finds a USB drive outside the office door with the label "Confidential Project Data."

  Curious, they plug it into their computer, and the malware automatically runs, sending sensitive data from the system to the attacker.

- **What happens if the victim takes action?**
  When the victim plugs in the USB, a backdoor program could be installed on their system, allowing the attacker to control the computer remotely.

- **Lesson Learned:**
  - Never plug unknown USB drives or portable disks into your computer.
  - If you need to test a device, do it in a secure virtual machine.
  - Companies should limit USB usage and enforce security policies.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Fake Help Desk (Tech Support Scam) – Impersonating a Support Team
Tech support scams occur when attackers impersonate a technical support team to deceive victims.

- **How It Works?**
  The attacker displays a pop-up message saying, "Your computer has a virus! Call us immediately!" If the victim calls the provided number, a fake technician may offer a service for a high fee or gain remote access to the victim's computer.

- **Real World Example:**
  According to Microsoft's report, 3.3 million people were affected by fake tech support scams in 2022.

- **Lesson Learned:**
  - Real tech support teams never reach out to users unsolicited.
  - Use official support channels for your operating system.

7.5. Strategies for avoiding manipulation

In this section, we'll be diving into a detailed lesson on how to protect ourselves from social engineering attacks. In previous lessons, we examined how attackers manipulate human psychology, the methods they use, and real-world examples.

The main goals:

- Recognize social engineering attacks and build awareness
- Develop protection strategies at both individual and organizational levels
- Create defense mechanisms against psychological manipulation techniques

Remember: Even the strongest firewall can be ineffective against human error. That's why the most important component of cybersecurity is awareness!

7.5.1. Awareness and Consciousness Development

The first and most important step in avoiding manipulation is to be aware and skeptical.

Cyber attackers use psychological techniques to gain people's trust. If we recognize these techniques and are aware of them, we can become more resilient to attacks.

What should we watch out for?

- Unrealistic offers: Messages like "Congratulations! You've won $1,000,000, click now!" are often scams.
- Urgency tactics: Threatening messages like "Change your password now, or your account will be closed!" are manipulation tactics.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

- Emotional manipulation: Attackers try to deceive their victims by triggering emotions like compassion, fear, trust, or excitement.

Real-life example:
An attacker might trigger the victim's fear and panic by saying, "Your father is in the hospital, you need to pay for an urgent surgery!" and convince them to send money.

How do we protect ourselves?
- Filter incoming messages through logical thinking.
- Don't rush to make decisions; verify the information.
- Always validate sources before sharing your credentials.

7.5.2. Strategies to Protect Against Phishing Attacks
Attacks through email, SMS, or fake websites are very common.

How can we recognize them?
Here are some ways to identify phishing attacks:
- Pay attention to links in emails. Before opening any suspicious URL, verify whether the address belongs to the official site.
- Examine the sender's email address. Official company email addresses typically use domains like @bank.com. If the domain is @gmail.com, @yahoo.com, or something similar, it's likely fake.
- Read the content carefully. If there are spelling mistakes or grammatical errors, the email is probably a scam.

Example: If you receive an email with a message like "Your account is in danger, reset your password immediately!" before clicking the link, try going directly to the official website to log in.

How do we protect ourselves?
- Don't click on suspicious links!
- Verify whether emails are legitimate by checking official sources.
- Banks or official organizations will never ask for your password via email!

7.5.3. Preventing Threats Through Phone and Social Media
Attackers may try to deceive you through phone calls or social media messages.

Ways to protect yourself from phone scams:
- Be cautious with calls that seem to come from banks or government officials.
- Never provide personal or financial information to anyone asking for it over the phone.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

- Call official company or bank numbers directly for verification.

Ways to protect yourself from social media scams:

- Be wary of messages from unknown individuals.
- Be suspicious of offers like gift giveaways, "easy money" schemes, or "investment opportunities."
- Be careful when sharing personal information, your location, or daily activities.

Example: If you see a message on social media saying, "Your friend is in trouble, send money immediately," first contact your friend directly to verify the situation.

How do we protect ourselves?

- Question who is calling you, and avoid sharing information immediately.
- Adjust your social media privacy settings so that only trusted individuals can see your posts.
- Be cautious of people trying to scare you or pressure you into making quick decisions.

7.5.4. Enhance Your Computer Security and Use Strong Passwords

It's crucial to take technical measures to prevent social engineering attacks.

To keep your computer and accounts secure, you should:

- Use strong and unique passwords (At least 12 characters, including uppercase letters, lowercase letters, numbers, and special characters)
- Enable two-factor authentication (2FA)
- Keep your antivirus and security software up to date
- Use password managers to generate strong and unique passwords

Example: If your password is something predictable like "123456" or "password" attackers can crack it within seconds. Create a strong combination like "Hg7$k!92X" for your password.

How do we protect ourselves?

- Use a different password for each account.
- Never share your passwords with others.
- If you think you've been attacked, change your password immediately.

7.5.5. Being Aware Against Social Engineering Manipulations

Social engineering attacks are some of the most dangerous cyber threats, targeting human psychology.

As long as you stay aware and cautious, you can protect yourself from these attacks!

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

What did we learn in this lesson?

- Awareness is the most important protection strategy.
- Be cautious of phishing, phone scams, and social media manipulations.
- Use strong passwords and technical security measures.

Final Recommendations:

- Don’t click on suspicious emails or links.
- Don’t trust people asking for information over the phone without verification.
- Increase your security awareness and educate those around you.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Chapter 8
Social Media and Mobile Device Security

8.1. Introduction

Social media and mobile devices have transformed how people communicate, do business, and engage in free time activities. A continuously growing number people, including older adults, now use smartphones and social platforms to stay in touch with relatives and access essential services, such as online banking or telehealth (Pew Research Center, 2024). While the increasing use of digital devices can enhance the social connectivity and make our lives easier, it also brings new challenges in terms of data protection and personal privacy. Many individuals are unaware of hidden risks, such as social media impersonation, malicious apps, or security concerns caused using insecure, public Wi-Fi networks (FBI, 2024).

The potential negative consequences are high especially for those who have limited technical backgrounds. Individuals with limited tech knowledge may not realise that a single oversight (e.g. using weak passwords) could expose them to fraud or identity theft. In a 2022 survey, the AARP warned that older Americans face an increased risk of cyber scams, partly because of the increasing use of social engineering tactics that exploit trust and limited awareness (AARP, 2022). However, **even experienced users are not immune to scams and frauds, as cybercriminals continually adapt their methods to bypass security measures** (ENISA, 2022).

Given the complexity of the online scams and frauds, **it is crucial that individuals adopt both preventive and responsive strategies**. Users who take the time to adjust their social media privacy settings, regularly update their device software and remain vigilant about random messages can significantly reduce their vulnerability (Microsoft, 2025).

This chapter aims to provide readers with guidance on how to secure their social media accounts and mobile devices. Providing an overview of basic privacy configurations on popular platforms and highlighting device-level safeguards (e.g., OS updates, app permissions, data backups) can help the readers to navigate the digital space more securely and confidently.

8.2. Securing social media accounts and adjusting privacy settings

More than 5 billion people use social media platforms worldwide – 86.1% of the world's population, in the age group above 18 years, is present on social media platforms (Backlinko, 2025). While, social media platforms offer endless opportunities for communication, networking and entertainment, they can also become gateways for cyber criminals and threats, especially when users leave default settings unchanged or unknowingly expose sensitive information (Bartsch and Dienlin, 2016). Therefore, understanding and customising privacy controls is crucial towards protecting personal data and reducing the likelihood of scams, identity theft, and unwanted intrusion (FBI, 2024).

Most social media platforms enable users to tailor their account visibility and thus limit access to personal information. However, **many default configurations set broad profile, or personal data, sharing, which leads to the exposure of profile details to a wide audience** (Meta, 2025). Privacy literacy, i.e., the degree to which a user understands these settings, varies greatly among social network users. Some users diligently configure their profiles so that they

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

are visible only to approved contacts, while others mistakenly believe that their profiles are protected because a platform promises "secure" features (Bartsch and Dienlin, 2016).

A **practical step for any user is to review the platform's privacy settings** – for example on Facebook, individuals can choose who sees their posts (the public, friends, or friends except…) and **can also restrict who can send them friend requests or look them up by the phone number** (Meta, 2025). Similarly, other social networks also allow users to choose whether they want to have their profiles private (protected) or public, and some social media, e.g. Instagram, provides control settings for limiting direct messages and story visibility. Taking advantage of these settings is particularly beneficial for those at heightened risk, such as seniors who might mistakenly share personal or financial details on their profiles.

8.2.1. Account security measures

The easiest approach to securing social media accounts is to **choose robust, unique passwords for each account** (NIST, 2021). Reusing passwords across multiple platforms can create a domino effect of cyber-attacks – if an attacker cracks one password, they can then test those same credentials on other sites, easily compromising other accounts. Given the complexity of managing numerous logins, password manager apps (e.g., NordPass, TotalPassword, Dashlane, LastPass) can be used to store and manage various login credentials. These tools generate strong passwords and store them securely, taking off the burden of memorising countless password combinations (Trepte and Reinecke, 2011).

In addition to a strong password, **multi-factor authentication provides an extra layer of security**. Whether the one-time code is generated via a text message, phone call, a mobile authenticator app, or a physical security key, multi-factor authentication forces attackers to overcome a second hurdle if they somehow obtain the user's password (Microsoft, 2025). Older adults who rely on simpler login schemes may initially find multi-factor authentications time-consuming and burdensome, but the added layer of security often proves invaluable (FBI, 2024).

Most social platforms offer the option to **receive notifications if a new device or unusual location logs into an account** (Bartsch and Dienlin, 2016). **Users should always enable these alerts to detect any unauthorised attempts to access the accounts.** If one receives an alert of unauthorised access attempt, it is important to promptly follow up on it by changing passwords and reviewing recent account activity. In addition, social platforms also provide the option to sign out from an account on a specific device, which represents a handy feature in case of a stolen or lost device.

Users often neglect to update their **recovery phone numbers or backup email addresses**, which poses risks to accessing accounts in case they lose access to their phone (Meta, 2025). Therefore, checking and refreshing account recovery details, at least annually, helps to ensure that account recovery procedures remain accurate. This allows users to relatively easily secure their account again in case of a breach.

8.2.2. Recognising and avoiding common social media scams

With the increasing use of social platforms, they have become prime channels for phishing. Criminals also create **fake, impersonation accounts by cloning a genuine profile's name and**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

photos before sending out friend requests. These impostor profiles can ask for loans or direct victims to fake fundraising campaigns (FBI, 2024). Everyone present on social media should exercise caution with unsolicited messages. When receiving an unsolicited message, one should double-check the sender's username and verify with friends offline if a request seems out of character

Clicking **unfamiliar or shortened URLs in comments and direct messages can also pose a lot of risks** – in compromised links, attackers embed malware payloads or direct victims to sites designed to harvest login credentials (ENISA, 2022). For example, a user may receive a message with phrases like "Check out this video of you!" leading to a strange login screen. **Hovering over links, scanning suspicious URLs with online checkers, or refusing to engage with unknown senders are some of safe habits** for all demographics, including older individuals who are more frequently targeted by scammers due to perceived vulnerabilities and unfamiliarity with potential threats (AARP, 2022).

Moreover, cyber criminals often capitalise on older adults' willingness to connect with perceived acquaintances. By **sending out fake profile friend requests**, they hope to access their victim's private posts, personal details (like birthdays or phone numbers), or run romance scams (Trepte and Reinecke, 2011). Before accepting a friend request, even from someone who appears familiar, it is often wise to examine their profile for signs of authenticity (photos, mutual friends, posts over time) or reach out via another channel to confirm their identity.

8.2.3. Personal data management practices

In s lot of cases, a **great portion of privacy threats arises from historical content** that users posted a long time ago, but left it publicly accessible (Bartsch and Dienlin, 2016). For instance, individuals may have posted addresses or detailed family information years ago, forgetting about them and leaving them to linger online. Therefore, individuals should allocate time to go through their old posts and delete or archive them – especially those containing contact information, personal schedules or images that can give away their address, friends etc. (Meta, 2025).

Another method of ensuring online safety is **reducing the amount of personal information displayed** on public profiles. While it may seem harmless to include a birthdate or hometown for nostalgia's sake, or to easily identify acquaintances, these details can be exploited to answer security questions, guess passwords, or tailor phishing schemes (FBI, 2024). A safer and recommended approach is to **reserve personal information for private and close circles**, which helps to ensure that only trusted connections can view sensitive personal details.

Many social media users install **third-party apps** (e.g. quiz games or scheduling tools) which often **request extensive permissions to access information** on profiles, friend lists or direct messages. Some of the apps may be well-intentioned, however, others aim to harvest data for foul purposes (Bartsch and Dienlin, 2016). Therefore, regularly checking app authorisations in platform settings can prevent data leaks and block suspicious access to profiles and personal information. If an app's purpose does not justify its access level (e.g., a puzzle game wanting to read private chats), revoking permissions to access social media profiles is recommended.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

By integrating the above measures, social media users can significantly reduce their risk of encountering scams, frauds or being adversely affected by data breaches (Trepte and Reinecke, 2011). Particularly for older adults, proactive adjustment can make a substantial difference in safeguarding online interactions and preserving personal security and enhance their experience with using social media platforms. **The box below highlights a practical example of adjusting Facebook privacy settings and provides a summary of best practices**.

Practical example and best practices
Adjusting Facebook Privacy

- Access Settings: From the main menu, open "Settings & Privacy," then "Privacy Checkup"
- Review who sees your posts: Modify the default posting audience to "Friends" rather than "Public"
- Limit past posts: Use the "Limit Past Posts" feature to restrict older posts to friends only
- Profile visibility: Under "Profile and Tagging," adjust who can see tags, timeline posts, and personal details
- Enable alerts: In "Security and Login," enable login alerts and two-factor authentication

Recommended Do's and Don'ts

- Do verify unknown friend requests by contacting the person offline or through a trusted channel
- Do treat unsolicited links or attachments with caution, especially if they promise sensational content
- Don't include personal identifiers (phone number, address, birthdays) in public sections of a profile
- Don't accept default privacy settings without reviewing and customising them

Source: Meta, 2025.

8.3. Safe practices for using mobile devices and apps

Mobile devices, including smartphones and tablets, are integral part of daily life of majority of people. They allow users to manage banking, health records, and personal communications from virtually any location with data coverage (Google, 2025). While these conveniences are especially valuable for allowing people to stay connected, they can also create heightened risks if security measures are neglected (Apple, 2025).

8.3.1. Device-level security

Given cyber threats evolve in time, **smartphones and tablets rely on periodic software updates** to address the newly discovered vulnerabilities that attackers could exploit (Google, 2025). For busy users who cannot keep track with updates or those who are not familiar with navigating device settings, enabling automatic updates for iOS or Android devices can help ensure critical software updates are installed timely (CISA, 2023). This is particularly important for older adults who might unintentionally postpone manual updates or overlook them, which can prolong the periods of their devices being exposed to malicious software or hacking attempts.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

When setting up a new phone or device, it **is crucial to set up locking methods**. Locking devices with a robust PIN or password, or biometric method (fingerprint, face recognition) represent foundational steps toward mobile security (NIST, 2021). While some users may prefer convenience over security, especially if they struggle to remember complex passcodes, even locking their device with a simple PIN provides a layer of protection against unauthorised access in case of theft or loss (Apple, 2025). Individuals who own multiple devices can synchronise certain security settings, e.g. passwords or facial recognition, across each device to maintain consistent safeguards (only works if the devices are running on the same operating system).

Most modern smartphones support full-disk **encryption**, which encrypts stored data so that it remains unreadable to anyone lacking the proper authentication (ENISA, 2022). Encrypting data on personal devices is crucial for protecting sensitive information such as medical records or financial details. Equally important is setting up and regularly using backup schedule using trusted cloud services (e.g., iCloud, Google Drive) or external storage. Regular backups ensure that if a device is stolen, lost, or damaged, the user can restore essential contacts, photos, and other personal data without significant disruption (Google, 2025).

8.3.2. App-level considerations

When downloading apps, **it is important to stick to using official app stores** such as the Apple App Store or Google Play Store, rather than downloading apps form third-party websites and unofficial marketplaces, which often lack consistent vetting processes for malware or privacy risks (FTC, 2024). However, **it may also happen that even among recognised app stores, some malicious apps occasionally get through automated reviews** (ENISA, 2022). Therefore, when downloading, particularly less known, apps a cautious approach is to:

- Check the publisher's credibility (e.g., known developer, official bank name)
- Review user ratings and feedback
- Review the app's permissions before installation
- Older adults may need additional guidance distinguishing between legitimate and counterfeit apps, particularly those promising "free virus cleaning", unauthorised streaming, photo or video editing.

When installing **apps that request permissions to access device features** (camera, microphone, location, contacts), **it is important to consider whether such permissions are crucial** and whether they could be misused. While some permissions may be justifiable – for instance, a ride-sharing app requiring location data – others may seem excessive, which may indicate potential data harvesting (Apple, 2025). Thus, regularly reviewing and revoking unnecessary permissions can help limit the amount of personal information exposed to third parties (Bartsch and Dienlin, 2016). For instance, a casual game that demands constant microphone access or a puzzle app seeking contact list data warrants caution.

Furthermore, **mobile banking apps and digital wallets** (e.g., Apple Pay, Google Pay) offer users convenience, however, their **use requires vigilant security practices** (Microsoft, 2025). Users should always confirm that they are using the official application from their financial institution and enable transaction notifications. Individuals who might be less

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

comfortable with app-based transactions could consider using these services alongside strong authentication methods, such as biometrics or hardware security keys, to prevent unauthorised purchases (NIST, 2021). It is suggested that the digital wallets should always be protected by authentication methods. In case of loss or theft of the device, it is important to report the device as lost/stolen and lock it, so that digital wallets become disabled.

8.3.3. Safe use of public Wi-Fi

Individuals should **always demonstrate caution when using free Wi-Fi at cafés, libraries, or airports** (i.e., free, unprotected, public WiFi)**.** Free Wi-Fi often lacks encryption, which allows attackers to intercept unprotected data passing between the device and the router (CISA, 2021; Putra, 2025). This exposes users to man-in-the-middle attacks, where cybercriminals can secretly capture login credentials or personal messages (ENISA, 2022; Putra, 2025). To prevent these risks, a VPN (virtual private network) should be used to encrypt the data in transit, obscuring browsing activity from prying eyes. Individuals, particularly older adults who travel or frequently rely on public hotspots, should be especially mindful of disabling automatic Wi-Fi connections or forgetting networks when they are no longer using them (Bartsch and Dienlin, 2016; Putra, 2025).

Example: Avoiding malicious apps
Helen, a 68-year-old retiree, noticed her smartphone battery draining unusually fast after downloading a "Phone Booster" app from a pop-up advertisement. Soon afterward, she began receiving odd text messages requesting sensitive details. She also discovered unauthorised charges on her phone bill. Investigation revealed that the newly installed app contained hidden spyware that recorded keystrokes and sent premium SMS messages without Helen's knowledge.

It is always crucial to verify app sources (official stores), scrutinise permissions, and remain alert to unusual device behaviour. Downloading fraudulent apps from third-party providers and unofficial app stores can lead to contacts getting compromised, financial losses, and the hassle of having to reset multiple online accounts. Once such app is detected, it is important to uninstall it as soon as possible, run a reputable anti-malware tool, and reset the device credentials.

Summary of best practices

- **Install updates as soon as they become available:** Turn on automatic OS and app updates to patch security flaws
- **Use secure device locks:** Set PINs, passwords, or biometrics, and avoid leaving devices unlocked or unattended
- **Limit app permissions:** Regularly review settings to revoke unneeded access (camera, location, contacts, social network profiles)
- **Verify app sources:** Download from official stores; read reviews to spot potential fraud (apps with very few reviews great should be approached with care too)
- **Enable alerts:** Activate notifications for suspicious activity in banking or financial apps
- **Be cautious when using public Wi-Fi:** Use a VPN and refrain from logging in to critical accounts when being connected to unsecured networks

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

Taken together, these approaches form a layered approach to mobile security. By combining device-level protections with cautious app usage and safe networking habits, users can diminish the vulnerabilities associated with smartphones and tablets (NIST, 2021). Careful approach to using their devices and online platforms is especially crucial for older adults, who may be unaware of the potential threats, ways of detecting them and of ways of how to address them.

8.4. Summary

Navigating social media platforms and mobile devices requires a balance between convenience and caution. This chapter explored how customising privacy settings, using strong authentication methods, and remaining mindful of what is shared online can significantly lower the risks of unauthorised access, identity theft, and being a victim of scams or fraud. These considerations become even more critical for older adults, who may be unfamiliar or unable to keep up with the fast-evolving digital threats. By taking relatively simple measures and staying vigilant, users can create layered security that deters cybercriminals.

Since technology and online scams evolve in tandem, it is crucial to continuously improve users' digital literacy and cybersecurity. Emerging tactics, such as highly targeted phishing and malicious apps disguised as helpful tools, underscore the importance of staying informed via reputable security advisories, media outlets, and community programs. Likewise, regularly reviewing social media profiles, deleting or archiving outdated posts, and monitoring device permissions helps to regulate broad data exposure. However, while no single action offers a complete immunity from cyber threats, consistently following best practices can make a big difference.

References and Further Reading

AARP. (2022). 2022 TECH TRENDS AND THE 50-PLUS. Available at: https://www.aarp.org/content/dam/aarp/research/surveys_statistics/technology/2021/2022-technology-trends-older-americans.doi.10.26419-2Fres.00493.001.pdf

Apple. (2025). Apple Platform Security. Available at: https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf

Bakclinko. (2025). Social Media Usage & Growth Statistics. Available at: https://backlinko.com/social-media-users [Accessed: Feb 1, 2025].

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. Computers in Human Behavior, 56, 147-154.

CISA. (2021). Securing Wireless Networks. Cybersecurity & Infrastructure Security Agency. Available at: https://www.cisa.gov/news-events/news/securing-wireless-networks

CISA. (2023). Preventing Web Application Access Control Abuse. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-208a

ENISA. (2022). Threat Landscape 2022: Overview of Current and Emerging Cyberthreats. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

FBI. (2024). 2023 Internet Crime Report. Federal Bureau of Investigation. Available at: https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.

FTC. (2024). Consumer Sentinel Network Data Book 2023. Federal Trade Commission. Available at: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2023
Google. (2025). Google Play Protect. Available at: https://developers.google.com/android/play-protect [Accessed: Feb 2, 2025].
Meta. (2025). Safety tools and policies. Available at: https://about.meta.com/actions/safety/topics/safety-basics/tools
Microsoft. (2025). Microsoft Digital Defense Report 2024. Available at: https://www.microsoft.com/en-us/security /microsoft-digital-defense-report-2024
NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
Pew Research Center. (2024). Social Media Use Report. Available at: https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2024/01/PI_2024.01.31_Social-Media-use_report.pdf
Putra, I. B. (2023). Public Wifi Risks - Cyber Security. Available at: https://www.linkedin.com/pulse/public-wifi-risks-cyber-security-ichsan-budiman-putra-mos-mtcna/ [Accessed: Feb 2, 2025].
Trepte, S., and Reinecke, L. (2011). Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web. Berlin: Springer.

Additional resources

Cisco. What Is Device Security? Available at: https://www.cisco.com/c/en/us/products/security/what-is-device-security.html
I am IT Geek. (2024). STOP Making These 5 Mobile Device Security Mistakes. Available at: https://www.youtube.com/watch?v=qChg4Un24D4
NCSC, UK. Device Security Guidance. Available at: https://www.ncsc.gov.uk/collection/device-security-guidance
SEO North. (2019). Social Media Safety Tips. Available at: https://www.youtube.com/watch?v=vPlWDFtP0T0
SOTI. (2024). Best Practices for Mobile Device Security & Encryption. Available at: https://www.youtube.com/watch?v=WAWsgvyqqj8
TEDx Talks. (2020). Think Cyber - How to stay safe in an online world | May Brooks-Kempler. Available at: https://www.youtube.com/watch?v=DXgYJb67Fyc
TEDx Talks. (2021). Profiling Hackers - The Psychology of Cybercrime | Mark T. Hoffmann. Available at: https://www.youtube.com/watch?v=4EyWrC41Oc4
Udemy. Social Media Security 101 - Stop The Hackers! Available at: https://www.udemy.com/course/social-media-security-101-stop-the-hackers/
Coursera. Digital Safety and Security. Available at: https://www.coursera.org/learn/digitalsafetyandsecurity

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Slovak Academic Association for International Cooperation. Neither the European Union nor the granting authority can be held responsible for them.