



Digital Security Guideline



Author:

Nino Gamisonia

March, 2024

Table of Contents

[Table of Contents](#)

[Foreword](#)

[Chapter 1: Introduction](#)

[Understanding the Importance of Digital Security](#)

[Why Digital Security Matters:](#)

[Recognizing the Evolving Landscape of Cyber Threats](#)

[Types of Cyber Threats:](#)

[Embracing a Proactive Approach to Safeguarding Your Digital Life](#)

[Proactive Digital Security Practices:](#)

[Chapter 2: Risk Management](#)

[Identifying Potential Risks and Vulnerabilities](#)

[Conducting a Risk Assessment:](#)

[Assessing the Impact of Security Breaches](#)

[Establishing a Risk Mitigation Strategy](#)

[Risk Mitigation Strategies:](#)

[Chapter 3: Password Management](#)

[Creating Strong and Unique Passwords](#)

[Characteristics of a Strong Password:](#)

[Utilizing Password Managers for Enhanced Security](#)

[Implementing Two-Factor Authentication \(2FA\)](#)

[Chapter 4: Device Security](#)

[Keeping Operating Systems and Software Up to Date](#)

[Importance of Updating:](#)

[Using Reputable Antivirus \(RU\) and Anti-Malware Tools](#)

[Securing Your Devices with Passwords \(RU\) or Biometric Authentication](#)

[Setting Strong Passwords for Device Access:](#)

[Smartphone Security](#)

[Regularly Update Software](#)

[Chapter 5: Data Management](#)

[Backing Up Important Data Regularly](#)

[Creating Regular Backups:](#)

[Encrypting Data and Communications](#)

[Being Mindful of Data Sharing Practices](#)

[Cloud Storage Security](#)

[Chapter 6: Identity Management](#)

[Monitoring Your Digital Footprint](#)

[Digital Footprint Management:](#)

[Avoiding Oversharing on Social Media](#)

[Privacy Tips:](#)

[Managing Online Accounts Responsibly](#)

[Account Management Best Practices:](#)

[Chapter 7: Secure Communication](#)

[Using Encrypted Messaging Apps](#)

[Benefits of Encrypted Messaging:](#)

[Popular Encrypted Messaging App:](#)

[Verifying the Authenticity of Communication Channels](#)

[Authentication Verification Steps:](#)

[Being Cautious About Sharing Sensitive Information via Email](#)

[Email Security Best Practices:](#)

[Phishing Awareness](#)[Chapter 8: Phishing](#)[Recognizing Phishing Attempts](#)[Common Phishing Indicators:](#)[Verifying the Legitimacy of Emails and Links](#)[Reporting Phishing Incidents](#)[Reporting Steps:](#)[Example: Social Media Phishing](#)[Chapter 9: Public Wi-Fi and Network Security](#)[Avoiding Sensitive Transactions on Public Wi-Fi](#)[Risks of Public Wi-Fi:](#)[Using Virtual Private Networks \(VPNs\) for Security](#)[Configuring Home Networks Securely](#)[Home Network Security Tips:](#)[Secure Home Office Network](#)[Chapter 10: Emerging Threats and Future Considerations](#)[Staying Informed About New Cyber Threats](#)[Sources of Information:](#)[Adapting Security Practices to Evolving Technologies](#)[Conclusion: A Secure Digital Future](#)

Foreword

Welcome to the ever-evolving world of digital security! In today's highly connected environment, safeguarding your online presence is more crucial than ever. This guide empowers you, the average user, with the knowledge and tools to navigate the digital landscape with confidence. We'll delve into essential practices to shield yourself from

cyber threats, from crafting unbreakable passwords to foiling phishing attempts. Remember, digital security is an ongoing process, but with this guide as your companion, you'll be well-equipped to protect your valuable information and online identity.

By following the guidelines outlined in the guide, you'll be better equipped to navigate the digital landscape securely. Remember, digital security is a shared responsibility, and your proactive efforts contribute to a safer online environment for everyone.

Why digital security is important for women's organizations and women groups?

Digital security is crucial for small women's organizations and groups for several reasons:

Protecting Sensitive Information

Women's organizations often deal with sensitive information related to their members, clients, or beneficiaries. This could include personal details, medical records, or information about survivors of violence. Ensuring digital security safeguards this data from unauthorized access or breaches.

Preventing Harassment and Intimidation

Women's groups may face online harassment, threats, or intimidation from individuals or groups opposed to their work or ideology. Strong digital security measures can help prevent unauthorized access to communication channels, websites, or social media accounts, reducing the risk of harassment or hacking.

Maintaining Confidentiality and Privacy

Many women seek support from these organizations for sensitive issues such as domestic violence, sexual assault, or reproductive health. Ensuring the confidentiality and privacy of communications and data is essential to building trust and encouraging women to seek help without fear of exposure.

Preserving Organizational Integrity

Women's organizations often advocate for social or political change, which can make them targets for cyber attacks or attempts to discredit their work. By implementing robust digital security measures, these groups can protect their websites, social media platforms, and online presence from hacking, defacement, or misinformation campaigns.

Ensuring Operational Continuity

Dependence on digital tools and platforms for communication, fundraising, and organizing means that any disruption due to cyber attacks or data breaches can severely impact the operations of women's organizations. Investing in digital security helps ensure the continuity of their work and services.

Complying with Legal Requirements

Depending on the jurisdiction, there may be legal requirements regarding the protection of personal data, especially sensitive information related to health or identity. Failure to implement adequate digital security measures could result in legal consequences or liabilities for women's organizations.

In summary, digital security is essential for women's organizations and groups to protect sensitive information, prevent harassment and intimidation, maintain confidentiality, preserve organizational integrity, ensure operational continuity, and comply with legal requirements.

Chapter 1: Introduction

Understanding the Importance of Digital Security

In today's digital world, our lives are deeply connected to the internet. We work online, we shop online, connect with friends on social media, and manage our finances through digital platforms. While the convenience is undeniable, it comes with the responsibility of safeguarding our digital presence. Digital security is not just about protecting your devices; it's about safeguarding your identity, personal information, and online activities from potential threats.

Why Digital Security Matters:

Protection Against Cyber Threats:

- Malware, phishing attacks and other cyber threats are pervasive. Digital security measures act as a shield against these dangers.

Safeguarding Personal Information:

- Your online presence is a treasure trove of personal information. Digital security ensures that this information remains confidential and out of the wrong hands.

Preserving Financial Security:

- As more financial transactions move online, securing your digital presence becomes critical to prevent identity theft and unauthorized access to your financial accounts.

Maintaining Trust and Privacy:

- Trust is the foundation of the digital world. Digital security practices help maintain trust in online interactions and preserve your right to privacy.

Recognizing the Evolving Landscape of Cyber Threats

Cyber threats are dynamic, constantly evolving to exploit vulnerabilities in technology and human behavior. Recognizing the types of threats you may encounter is the first step in developing effective digital security habits.

Types of Cyber Threats:

Malware: (RU)

- Software designed to harm your device or steal sensitive information.
- Example: A seemingly innocent download could contain malware that compromises your device's security.

Phishing Attacks: (RU)

- Deceptive attempts to trick individuals into divulging personal information.
- Example: An email posing as your bank, requesting login details.

Ransomware:

- Malicious software that encrypts your files and demands payment for their release.
- Example: Clicking on a seemingly harmless link can unleash ransomware, encrypting your important files.

Identity Theft:

- Unauthorized use of personal information for fraudulent activities.
- Example: Criminals using your stolen identity to open credit card accounts in your name.

Social Engineering:

- Manipulating individuals to divulge confidential information.
- Example: A phone call from someone claiming to be from a tech support company, requesting access to your computer.

Embracing a Proactive Approach to Safeguarding Your Digital Life

Digital security is not a one-time task but an ongoing process. Adopting a proactive mindset is crucial for staying ahead of potential threats and minimizing risks.

Proactive Digital Security Practices:

Stay Informed:

- Regularly update yourself on the latest cybersecurity threats and best practices.

Use Strong, Unique Passwords:

- Create complex passwords and avoid using the same password across multiple accounts.

Keep Software Updated:

- Ensure that your operating system and applications are regularly updated to patch vulnerabilities.

Implement Two-Factor Authentication (2FA):

- Add an extra layer of security to your accounts by enabling 2FA whenever possible.

Be Mindful of Online Activities:

- Think twice before clicking on suspicious links or sharing sensitive information online.

Invest in Security Tools:

- Consider using reputable antivirus software, password managers, and virtual private networks (VPNs) for enhanced protection.

By understanding the importance of digital security, recognizing the evolving threat landscape, and adopting proactive practices, you lay a solid foundation for a secure digital experience. The following chapters will delve deeper into specific aspects of digital security, providing actionable insights and examples for each topic.

Chapter 2: Risk Management

Identifying Potential Risks and Vulnerabilities

Digital security is a dynamic process that involves identifying and managing potential risks and vulnerabilities. By understanding the landscape of threats, you can develop effective strategies to protect your digital assets.

Conducting a Risk Assessment:

Asset Identification:

- Identify the digital assets you want to protect, including personal information, financial data, and digital devices.

Threat Identification:

- Identify potential threats such as malware, phishing, or unauthorized access to your accounts.

Vulnerability Assessment:

- Assess the weaknesses in your digital security, such as outdated software, weak passwords, or unsecured Wi-Fi networks.

Assessing the Impact of Security Breaches

Understanding the potential impact of a security breach helps prioritize your efforts and resources. Different types of breaches can have varying consequences.

Financial Impact:

- Consider the potential financial losses resulting from unauthorized access to your bank accounts or credit card information.

Privacy Concerns:

- Evaluate the impact on your personal privacy if sensitive information is exposed or misused.

Reputation Damage:

- Recognize the potential harm to your online reputation if your accounts are compromised, leading to unauthorized activities.

Data Loss:

- Assess the impact of losing important data, especially if it's irreplaceable or critical for your work.

Establishing a Risk Mitigation Strategy

Once you've identified potential risks and assessed their impact, it's time to develop a risk mitigation strategy to minimize the likelihood of security breaches and their potential consequences.

Risk Mitigation Strategies:**Regular Backups:**

- Regularly backup important data to prevent data loss in case of a security incident.

Educate Yourself:

- Stay informed about common cyber threats and learn how to recognize them to avoid falling victim to scams.

Use Security Software:

- Employ reputable antivirus software and keep it up to date to detect and remove malware.

Secure Your Wi-Fi:

- Set a strong password for your Wi-Fi network and enable WPA3 encryption to prevent unauthorized access.

Secure Physical Devices:

- Keep your devices physically secure, especially mobile devices that are more susceptible to loss or theft.

Regularly Update Software:

- Ensure that your operating system, applications, and security software are regularly updated to patch vulnerabilities.

By proactively identifying risks, assessing their potential impact, and implementing effective risk mitigation strategies, you can significantly enhance your digital security posture. In the following chapters, we will delve into specific aspects of digital security, providing practical tips and examples to guide you through each topic.

Chapter 3: Password Management

Creating **Strong and Unique Passwords**

Passwords are the first line of defense in protecting your online accounts. Creating strong and unique passwords is essential for preventing unauthorized access.

Characteristics of a Strong Password:

Complexity:

- Use a mix of uppercase and lowercase letters, numbers, and special characters.
- Example: `P@ssw0rd!`

Length:

- Aim for a minimum of 12 characters to increase the complexity of the password.
- Example: `SecureP@ss123!`

Unpredictability:

- Avoid easily guessable information, such as names, birthdays, or common words.

- Example: Instead of 123456, use something like B#lueT!ger91.

Utilizing Password Managers for Enhanced Security

Managing numerous complex passwords can be challenging. Password managers offer a convenient solution by securely storing and generating strong, unique passwords for each of your accounts.

How Password Managers Work:

- Password managers store your login credentials in an encrypted vault, requiring you to remember only one strong master password.

Benefits of Using a Password Manager:

- Eliminates the need to remember multiple passwords.
- Generates strong, unique passwords for each account.
- Enhances security by encrypting stored passwords.

Popular Password Managers:

- [1Password](#) and [Bitwarden](#).

Implementing Two-Factor Authentication (2FA)

Even with strong passwords, an extra layer of protection should be added through two-factor authentication (2FA). This involves a secondary verification step, typically a code sent to your mobile device.

How 2FA Works:

- After entering your password, a unique code is sent to your registered mobile device or email.
- Example: You log in with your password and receive a code on your phone that you also need to enter.

Types of 2FA:

- SMS codes, authentication apps (e.g., Google Authenticator), biometric verification.
- Recommended to use Google Authenticator or other apps like Authy.

Why Use 2FA:

- Adds an additional barrier, even if your password is compromised.

By creating strong and unique passwords, utilizing password managers, and implementing two-factor authentication, you significantly enhance the security of your online accounts. In the next chapters, we'll explore additional aspects of digital security, including device security and data management, to ensure a comprehensive approach to safeguarding your digital life.

Resources in ENG and RU

[My Passwords](#)

[LOCK YOUR DIGITAL DOOR](#)

[How to Use Bitwarden](#)

[How to Use 1Password](#)

[How to Setup and Use Google Authenticator](#)

[Как создать надежный пароль](#)

[Зачем использовать менеджер паролей](#)

[Зачем использовать двухфакторную аутентификацию](#)

[Как Установить и Использовать Google Authenticator](#)

Chapter 4: Device Security

Keeping Operating Systems and Software [Up to Date](#)

Maintaining the security of your devices starts with ensuring that your operating system (OS) and software are up to date. Software updates often include important security patches that protect against known vulnerabilities.

Importance of Updating:

Security Patches:

- Updates address vulnerabilities that could be exploited by malicious software.

Performance Improvements:

- Updates often include enhancements that improve the overall performance and stability of your device.

Compatibility:

- Ensure compatibility with new applications and features.

Using Reputable [Antivirus \(RU\)](#) and Anti-Malware Tools

Antivirus and anti-malware tools act as a second line of defense, providing real-time protection against malicious software.

Key Features:

- Real-time scanning of files and websites.
- Detection and removal of malware, viruses, and other threats.

Reputable Options:

- Consider using well-known antivirus software such as Norton, McAfee, or Windows Defender.

Regular Scans:

- Schedule regular scans to ensure continuous protection.

Securing Your Devices with [Passwords \(RU\)](#) or Biometric Authentication

Implementing strong access controls to your devices is essential in preventing unauthorized access and protecting your personal information.

Setting Strong Passwords for Device Access:

Avoid Common Passwords:

- Refrain from using easily guessable passwords like "password" or "123456."

Use a Mix of Characters:

- Combine uppercase and lowercase letters, numbers, and symbols.

Biometric Authentication:

- If available, use fingerprint or facial recognition for added security.

Smartphone Security

App Permissions:

- Review and manage app permissions to control access to your personal information.

Find Phone:

- Activate Find My Phone features in case your device is lost or stolen.

Biometric Authentication:

- Use fingerprint or facial recognition for security.

Regularly Update Software

Automatic Updates:

- Enable automatic updates for your operating system and software whenever possible.

Manual Checks:

- Periodically check for updates if automatic updates are not available.

Third-Party Applications:

- Keep all installed applications, including browsers and plugins, updated.

By keeping your operating system and software up to date, using reputable antivirus tools, and securing your devices with strong passwords or biometric authentication, you create a robust defense against various digital threats. In the following chapters, we'll explore data management and identity management to further strengthen your digital security posture.

Resources in ENG and RU

[Device Security \(RU\)](#)

[How to Use USB Sticks Safely \(RU\)](#)

[How to Keep Your Computer Safe and Secure \(RU\)](#)

[5 Signs That Your Phone Has Been Hacked \(RU\)](#)

[STRENGTHEN YOUR SCREEN LOCKS](#)

[DECLUTTER YOUR PHONE WITH AN APP CLEANSE](#)

[GIVE YOUR DEVICE A FRESH START](#)

[Советы по безопасности смартфонов](#)

[Защита украденного устройства в iPhone](#)

[ПОЗАБОТЬТЕСЬ О ВАШЕМ НОВОМ ТЕЛЕФОНЕ](#)

[КОНТРОЛИРУЙТЕ ДАННЫЕ В ВАШЕМ СМАРТФОНЕ](#)

Chapter 5: Data Management

[Backing Up](#) Important Data Regularly

Data loss can occur due to various reasons, including hardware failure, accidental deletion, or cyber attacks. Regularly backing up your important data is crucial for safeguarding against these unforeseen events.

Creating Regular Backups:

Backup Frequency:

- Schedule regular backups based on the frequency of data changes.

Backup Locations:

- Use 3-2-1 rule for data backup. Principles of the 3-2-1 backup rule: 3: Keep 3 copies of your data. 2: Store the data copies on 2 different devices or media types. 1: Store 1 copy of data offsite, on cloud storage.

Automated Backup Systems:

- Utilize automated backup tools to streamline the process.

Encrypting Data and Communications

Encryption adds an extra layer of protection to your sensitive data, ensuring that even if unauthorized access occurs, the data remains unreadable.

File Encryption:

- For Full Disk Encryption enable [BitLocker \(RU\)](#) on Windows 10/11 Pro and [FileVault \(RU\)](#) on Mac

Secure Communication Channels:

- Choose communication channels that prioritize encryption for [data sharing \(RU\)](#)

Being Mindful of Data Sharing Practices

Understanding and controlling how and with whom you share your data is fundamental to maintaining digital security and privacy.

Cloud Storage Security

Two-Factor Authentication:

- Enable two-factor authentication for your cloud storage accounts.

Private Sharing Settings:

- Set files and folders to private when sharing through cloud services.

Audit Sharing Permissions:

- Periodically review and update sharing permissions for shared documents.

By incorporating regular data backups, encryption practices, and mindful data sharing habits, you strengthen your ability to recover from data loss and protect your sensitive information. In the subsequent chapters, we'll explore identity management and secure communication to further enhance your overall digital security.

Resources in ENG and RU

[Data Management \(RU\)](#)

[Why You Should Make Backups and Where You Should Keep Them \(RU\)](#)

[How to Backup Your Mac \(RU\)](#)

[Делаем резервные копии](#)

Chapter 6: Identity Management

Monitoring Your Digital Footprint

Your digital footprint consists of the trail of data you leave behind through online activities. Monitoring and managing this footprint is essential for maintaining control over your personal information.

Digital Footprint Management:

Google Yourself:

- Regularly search for your name online to see what information is publicly available.

Review [Social Media \(RU\)](#) Profiles:

- Regularly review and update privacy settings on your social media accounts.

Audit Online Accounts:

- Periodically review and close unnecessary online accounts to minimize exposure.

Avoiding Oversharing on Social Media

Social media platforms are a common source of personal information leaks. Being cautious about the information you share can prevent unauthorized access and protect your privacy.

Privacy Tips:

Limit Personal Details:

- Avoid sharing sensitive personal information such as addresses, phone numbers, and e-mails.

Be Cautious About Check-Ins:

- Consider the implications of sharing your location on social media.

Review Friend Lists:

- Regularly review and manage your friend or connection lists.

Managing Online Accounts Responsibly

Your online accounts, from email to banking, are valuable targets for cybercriminals. Managing them responsibly is crucial for overall digital security.

Account Management Best Practices:**Strong, Unique Passwords:**

- Ensure each account has a strong, unique password.

Regular Password Updates:

- Periodically update passwords, especially for critical accounts.

Security Questions:

- Use unique answers to security questions to prevent easy guessing.

Enable Two-Factor Authentication:

- Secure your email account with an additional layer of protection.

Beware of Phishing Emails:

- Be cautious about clicking on links or providing information in unsolicited emails.

Regularly Review Connected Apps:

- Periodically check and remove third-party apps connected to your email.

By proactively managing your digital footprint, avoiding oversharing on social media, and responsibly managing online accounts, you minimize the risk of identity theft and unauthorized access to your personal information. In the upcoming chapters, we'll explore secure communication and strategies to defend against specific threats, such as phishing attacks.

Resources in ENG and RU

[Digital Identity Management \(RU\)](#)

[What is the digital footprint you leave online?](#)

[DEGOOGLE YOUR LIFE](#)

[FORTIFY YOUR BROWSER TO REDUCE YOUR TRACES \(RU\)](#)

[How to Protect Your Privacy on Twitter \(RU\)](#)

[How to Protect Your Privacy on Instagram \(RU\)](#)

[Избавляемся от метаданных](#)

[Слишком личное. Чем вы рискуете, публикуя информацию о себе в интернете](#)

[ИЗБАВЬТЕСЬ ОТ СЛЕЖКИ GOOGLE](#)

Chapter 7: Secure Communication

Using Encrypted Messaging Apps

[Communicating securely \(RU\)](#) is vital to protect the confidentiality of your conversations.

Encrypted messaging apps offer end-to-end encryption, ensuring that only the intended recipient can access the content.

Benefits of Encrypted Messaging:

Privacy Assurance:

- Messages are unreadable to anyone except the sender and recipient.

Protection Against Interception:

- Guards against eavesdropping by malicious entities.

Secure File Sharing:

- Many encrypted messaging apps also allow secure file sharing.

Popular Encrypted Messaging App:

[Signal](#):

- Known for its strong encryption and privacy features.

Verifying the Authenticity of Communication Channels

Before sharing sensitive information, it's crucial to ensure that the communication channel is legitimate. Verifying authenticity helps protect against phishing and impersonation attempts.

Authentication Verification Steps:

Check Sender Information:

- Verify the email address or phone number of the sender.

Use Official Websites:

- Access official websites directly instead of clicking on links provided in emails.

Confirm Identities:

- Confirm the identity of the person or organization requesting information.

Being Cautious About Sharing Sensitive Information via Email

Emails are a common target for phishing attacks. Being cautious about sharing sensitive information via email helps prevent falling victim to scams.

Email Security Best Practices:

Avoid Clicking on Suspicious Links:

- Hover over links to preview the URL before clicking.

Check Email Sender:

- Verify the sender's email address for legitimacy.

Use Email Encryption:

- Consider using email encryption services for sensitive communications.

Phishing Awareness

Phishing Email Indicators:

- Watch out for generic greetings, urgent requests for personal information, or unexpected attachments.

Report Suspicious Emails:

- Report phishing emails to your email provider.

Educate Others:

- Share phishing awareness tips with friends and family.

By using encrypted messaging apps, verifying communication channels, and being cautious about sharing sensitive information via email, you enhance your ability to communicate securely and protect your personal data from potential threats. In the next chapters, we'll delve into the specifics of phishing attacks and strategies to counter emerging threats in the digital landscape.

Resources in ENG and RU

[Secure Communication \(RU\)](#)

[How to Encrypt Email](#)

[Share Files Securely](#)

[Без рисков, без компроматов: как сделать Signal чуть безопаснее](#)

[Как Зашифровать Электронную Почту](#)

Chapter 8: Phishing

Recognizing Phishing Attempts

Phishing attacks are deceptive attempts to trick individuals into revealing sensitive information.

Recognizing the signs of phishing is crucial for avoiding falling victim to these scams.

Common Phishing Indicators:

Generic Greetings:

- Phishing emails often use generic greetings like "Dear User" instead of your name.

Urgent Requests:

- Be cautious of emails that create a sense of urgency, pressuring you to act quickly.

Mismatched URLs:

- Hover over links to inspect the actual URL. Phishing links may appear similar but lead to malicious sites.

Verifying the Legitimacy of Emails and Links

Before clicking on any links or providing information, it's essential to verify the legitimacy of emails and associated URLs.

Verify Sender's Email Address:

- Check the sender's email address for authenticity.

Visit Official Websites Directly:

- Instead of clicking on links in emails, visit official websites directly through your browser.

Check for Secure Connections:

- Ensure that websites use "https://" for secure connections when entering sensitive information.

Helpful tool:

- Check the link and attachments for malware and ransomware on [VirusToTal](#)

Reporting Phishing Incidents

Reporting phishing incidents helps protect not only yourself but also others who may be targeted. Many email providers and organizations have mechanisms in place for reporting phishing attempts.

Reporting Steps:

Forward Suspicious Emails:

- Forward phishing emails to your email provider's abuse or phishing reporting address.

Use Reporting Tools:

- Many email services offer reporting tools within their interface.

Contact Legitimate Organizations:

- If you suspect a phishing attempt impersonating a legitimate organization, contact them directly to verify.

Example: Social Media Phishing

Fake Friend Requests:

- Be cautious of friend requests from unknown individuals, even if they appear to have mutual friends.

Verify Requests:

- Message the person through another channel to confirm the legitimacy of friend requests or messages.

Educate Connections:

- Share information about social media phishing with your connections to raise awareness.

By recognizing phishing attempts, verifying the legitimacy of emails and links, and promptly reporting incidents, you contribute to a safer online environment and protect yourself and others from falling victim to these deceptive attacks. In the following chapters, we'll explore public

Wi-Fi and network security, as well as emerging threats and considerations for the future of digital security.

Resources in ENG and RU

[How Not to Fall for Phishing](#)

[How to Recognize Phishing Attacks](#)

[TO CLICK OR NOT TO CLICK?](#)

[Too Good to Be True](#)

Can you spot when you're being phished? - [Take a Quiz](#)

[Социальная инженерия](#)

[Как защититься от фишинга](#)

[Как распознать фишинговые атаки](#)

[Как не стать жертвой фишинга](#)

Можете ли вы распознать фишинговую атаку? - [Пройти Тест](#)

Chapter 9: Public Wi-Fi and Network Security

Avoiding Sensitive Transactions on Public Wi-Fi

Public Wi-Fi networks are convenient but often lack the security measures necessary for safe online activities. Avoiding sensitive transactions on public Wi-Fi helps mitigate the risk of unauthorized access.

Risks of [Public Wi-Fi](#):

Man-in-the-Middle Attacks:

- Attackers can intercept and manipulate data between your device and the network.

Unsecured Networks:

- Public Wi-Fi networks may lack encryption, making your data vulnerable to eavesdropping.

Rogue Hotspots:

- Cybercriminals can set up rogue Wi-Fi hotspots with misleading names to trick users.

Using [Virtual Private Networks \(VPNs\)](#) for Security

A Virtual Private Network (VPN) encrypts your internet connection, providing a secure tunnel for data to travel through. This helps protect your information from potential threats on public networks.

The best VPNs route your internet connection through a remote server and conceal your actual IP address behind one that is untraceable. You can surf the web safely and in complete anonymity.

How VPNs Work:

- VPNs encrypt your internet traffic, making it difficult for third parties to intercept or tamper with your data.

Choosing a Reputable VPN Provider:

- Select a VPN service with a good reputation for privacy and security.

Activate VPN Before Connecting to Public Wi-Fi:

- Always activate your VPN before accessing public Wi-Fi networks.

VPN Security tools

Pay attention to what kind of security tools your VPN uses. You may not be an expert on the difference between TCP/IP and WireGuard protocols, but you can look for three important hallmarks of strong security:

- AES-256 encryption

- A kill switch, which closes sites and apps if you lose your VPN signal
- Multihop technology, which routes your connection through not just one but multiple servers

Configuring [Home Networks Securely](#)

Securing your home network is essential for protecting all devices connected to it, from computers to smart home devices.

Home Network Security Tips:

Change Default Router Passwords:

- Use a strong, unique password for your router to prevent unauthorized access.

Enable WPA3 Encryption:

- Use the latest Wi-Fi encryption standard to secure your wireless network.

Update Router Firmware:

- Regularly update your router's firmware to patch vulnerabilities.

Secure Home Office Network

Separate Guest Network:

- Create a separate network for guests to prevent them from accessing your primary devices.

Strong Wi-Fi Password:

- Use a strong, unique password for your Wi-Fi network.

Regular Security Audits:

- Periodically review and update security settings on your home network.

By avoiding sensitive transactions on public Wi-Fi, utilizing VPNs for added security, and configuring home networks securely, you create a safer online environment for your devices and personal information. In the final chapter, we'll explore staying informed about emerging threats and considerations for the future of digital security.

Resources in ENG and RU

[Dangers of public Wi-Fi: how to use open networks safely](#)

[How to use a VPN and why you need it in 2024](#)

[«Ворота» для мошенников: как проверить Wi-Fi роутер на наличие уязвимостей](#)

[Что такое VPN?](#)

Chapter 10: Emerging Threats and Future Considerations

Staying Informed About New Cyber Threats

The digital landscape is ever-changing, and new cyber threats continually emerge. Staying informed about these threats is crucial for adapting your security practices.

Sources of Information:

Security News Outlets:

- Follow reputable security news outlets for updates on the latest threats.

Vendor Notifications:

- Stay alert to notifications from software and service providers regarding security updates.

Online Security Communities:

- Engage with online communities to discuss and share insights on emerging threats.

Adapting Security Practices to Evolving Technologies

As technology evolves, so do the methods employed by cybercriminals. Adapting your security practices to keep pace with these changes is essential.

By staying informed about emerging threats, adapting security practices to evolving technologies, and preparing for future challenges, you empower yourself to navigate the ever-changing digital landscape with resilience and vigilance. Digital security is an ongoing journey, and your commitment to learning and adapting ensures a safer digital experience for yourself and those around you.

Conclusion: A Secure Digital Future

As you continue your digital security journey, remember that cybersecurity is a shared responsibility. Share your knowledge with friends and family, contribute to creating a safer online environment, and stay curious about emerging technologies and threats.

In this ever-evolving digital landscape, your commitment to digital security is not just about protecting yourself but also about fostering a secure online community. Stay vigilant, stay informed, and enjoy a safer digital future!

Resources



<https://datadetoxkit.org/en/home>

<https://cyber-star.org/>

<https://cyber-star.org/cyberstar-index/>

[Цифровая безопасность в интернете для ребенка: памятка для родителей](#)

[Google Family Link – бесплатный способ установить родительский контроль](#)

<https://www.chayn.co/resources?themes=online-safety>

<https://ssd EFF.org/#index>

<https://www.digitaldefenders.org/>

<https://tacticaltech.org/>

<https://www.accessnow.org/help/>

<https://tacticaltech.org/resources/>

<https://surfshark.com/blog/cybersecurity>

<https://www.youtube.com/@NetworkChuck>

<https://myshadow.org/>

Digital security helpline

[Access Now](#)

[Digital Defenders Partnership](#)

[SECURITY AUDITING FRAMEWORK AND EVALUATION TEMPLATE FOR ADVOCACY GROUPS](#)

[Computer Emergency Response Team \(CERT\) for Armenian civil society – NGOs, Human Rights Defenders, Activists, journalists and independent media](#)