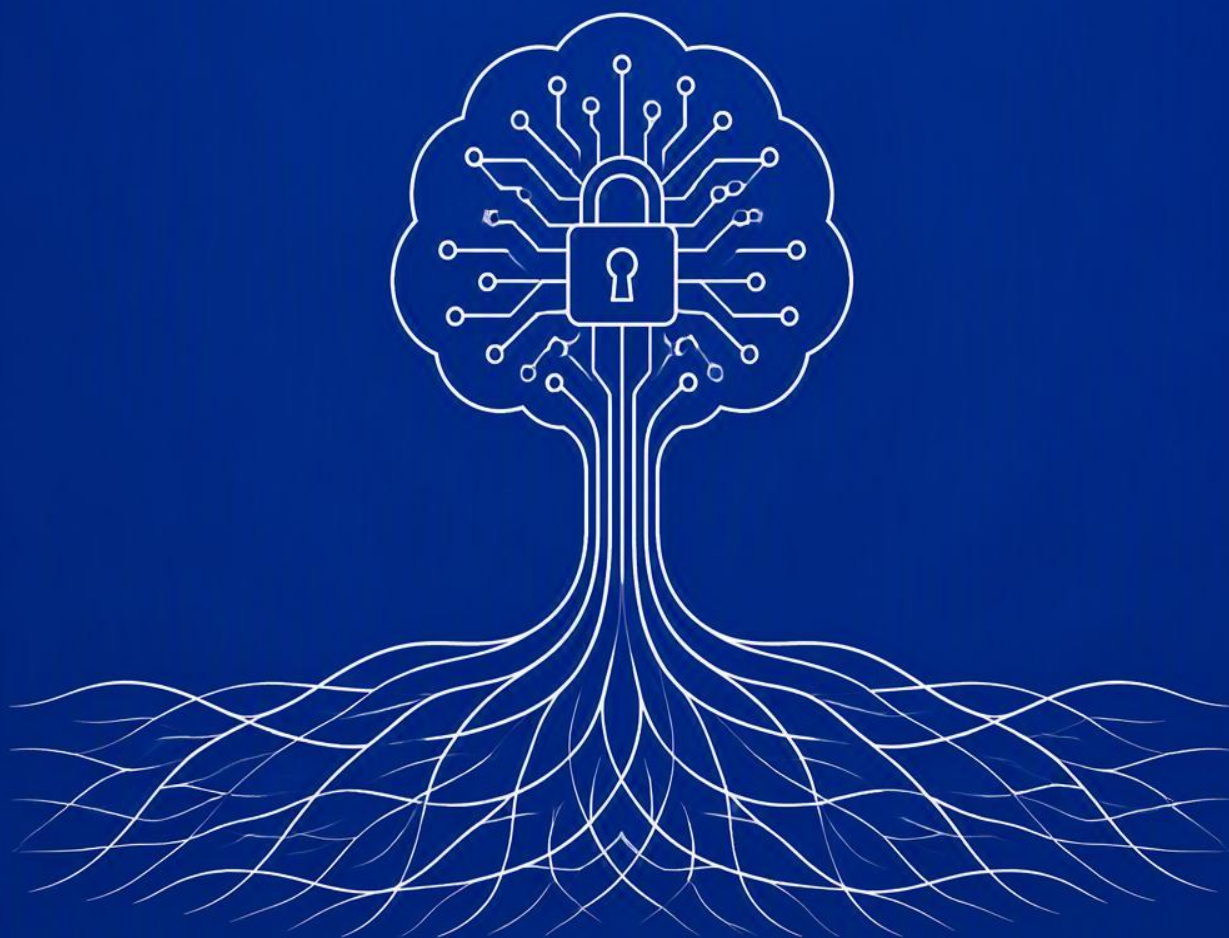




**Co-funded by
the European Union**

Digital Security Guidelines for Civil Society Organizations



These digital security guidelines for civil society organizations were developed within the framework of the project Fostering CSOs' Resilience to Shrinking Spaces and Strengthening their Capacities through Individual Mentoring and Value Mainstreaming in Hungary and Slovakia (FOREST), jointly implemented by the Alternative Communities Association (ACA), Partners for Democratic Change Slovakia (PDCS), and the Transatlantic Foundation (TF).

Author: Lukáš Zorád

Translation: Dimitar Keranov, PhD

Published: August 31, 2026



**Co-funded by
the European Union**

The FOREST project is co-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 the European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Contents

1	How to Use This Guide.....	4
2	Basic Principles of Online Security:	4
3	Data Breaches	5
4	Passwords.....	5
5	Data Encryption	7
5.1	Encrypting Devices.....	7
5.1.1	For Android:.....	8
5.1.2	For Windows (Professional Version Only):	8
5.1.3	For Mac OS X:.....	9
6	Malware	9
6.1	How Can Malware Get to You?	10
6.2	How Can We Protect Ourselves Against Malware?.....	10
6.3	How Can You Avoid Phishing and Recognize It in the First Place?.....	11
6.4	Social Engineering	12
6.5	Types of Malware	12
7	IP Address and VPN.....	13
7.1	Ways Someone Can Obtain Your Internet Protocol (IP) Address	13
7.2	Virtual Private Networks (VPN).....	14
8	Security on Social Networks and Privacy Settings.....	16
9	Resources	18
	Annex 1: Social Media Exercise.....	19
	Annex 2: Draft Security Plan.....	20

1 How to Use This Guide

The chapters set out tips and concrete steps toward better digital security for civil society organizations. It is not necessary to read the whole guide at once; when implementing individual steps, it is enough to choose the relevant chapter. For example, if I want to install a virtual private network (VPN) to protect personal data and prevent hacking attacks, I will look at the VPN chapter.

2 Basic Principles of Online Security:

To be safer online, we can remember these four principles. They help us understand what is happening, what impact it may have, and what steps we need to take to stay safe or reduce potential harm.

1) **Anything you put on the internet stays on the internet and is not anonymous.**

Information published on the internet is very difficult to remove completely. Photos, comments, posts, or documents can be copied, archived, or saved by other people without your knowledge. Even if you use a nickname or an anonymous account, the combination of different pieces of data often makes it possible to identify a specific person. It is therefore good to consider before publishing whether the information could cause problems for you in the future.

2) **The weakest link in cybersecurity is the human factor.**

Most successful cyberattacks do not begin by breaking technology but by deceiving people. Attackers exploit inattention, curiosity, time pressure, or trust in order to obtain passwords, sensitive data, or access to systems. Even the best technical protection can fail if a user clicks on a fraudulent link or provides information to an unauthorized person. Safe user behavior is therefore just as important as good-quality software.

3) **Be prepared for hackers to attack you—it has certainly happened before and it will happen again.**

Complete protection against attacks does not exist. Every user, organization, or company is a potential target of automated or targeted attacks. It is therefore important not only to try to prevent attacks but also to prepare for the situation when they occur. Regular updates, backups, strong passwords, and multi-factor authentication significantly reduce the damage an attack can cause.

4) **Privacy secured by design is more reliable than promised privacy.**

When protecting privacy, it is better to rely on technical solutions than on service providers' declarations. If communication is encrypted, data is minimized, and security measures are built directly into the system, protection does not depend only on the operator's goodwill. Promises about privacy protection may change over time, while technical safeguards provide a concrete and verifiable level of protection.

3 Data Breaches

You can check whether you have an account that was compromised as a result of a data breach on <https://haveibeenpwned.com/>, which is now also integrated directly into the Firefox web browser, where you can set up security alerts in case your password or your data is leaked. Simply enter your email address or username to find out whether your password is unsecured.

If you find that data from your accounts has leaked (it will appear in red, and the text will tell you exactly which of your data has leaked onto the dark web), follow the suggested steps. In most cases, it is enough to change the password, sign the account out of all devices, and, if the account is important, secure it with two-factor authentication.

<https://monitor.firefox.com/>

<https://haveibeenpwned.com/>

<https://haveibeenpwned.com/Passwords>

4 Passwords

Passwords are an important part of securing so many things we use—from our social media to our email to our banking. They are often the first and only barrier between your information and anyone who could read it, use it, or destroy it without your consent. You can use the most advanced security tools, but if your password is weak or if you allow it to fall into the wrong hands, they will not help you.

For example, have you ever used any of these passwords?

- 1 - 123456 (the most common password since 2018)
- 2 - 123456789
- 3 - qwerty
- 4 - password (down two places; for a long time it was in second place)
- 5 - 1234567
- 6 - 12345678
- 7 - 12345
- 8 - iloveyou
- 9 - 111111
- 10 - 123123
- 11 - abc123

Digital Security Guidelines for Civil Society Organizations

12 - qwerty123

13 - 1q2w3e4r

14 - admin

15 - qwertyuiop

16 - 654321

17 - 555555

18 - lovely

19 - 7777777

20 - welcome

You can view the complete ranking of the most common passwords and how it has changed over time here:

https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

If you use any of these passwords, you must change them. Why?

Because adversaries use lists of the most common passwords to gain access to your account. Another risk is password reuse. Services are sometimes hacked and passwords are stolen. This means that if you used the same password for two services and the first service is breached, an adversary will try to use that password for the second service. If you reused the password, they may gain access to your accounts.

How to create strong passwords?

Check how easy it is to crack your password: <https://howsecureismypassword.net/>

Tips/rules for creating a strong password

- **Password length is more important than using symbols/numbers/uppercase and lowercase letters** (For example, the password Jacob38! is a weak password; it takes only 8 hours to decode it)
- **Use a phrase, or a full sentence:** “my favorite cult book is about a blue robot” (2 triginillion years)
- **Do not reuse the same passwords anywhere**
- **Do not sign in through other applications** (Facebook, Gmail), even if it is convenient
- **Turn on two-factor authentication for truly important accounts** (banks require it; email accounts, Facebook)

More good advice is at: <https://www.eset.com/sk/blog/domaca-it-bezpecnost/ako-vytvorit-nepriestrelne-heslo/>

A password manager as a solution for not forgetting passwords:

You can also use KeePassXC <https://www.keepassx.org/>, Bitwarden <https://bitwarden.com/> or the paid service 1password <https://1password.com/haveibeenpwned/ohno/>.

And always use two-factor authentication.

5 Data Encryption

Encryption is a way to increase the security of a message or file by encoding its contents so that only someone with the correct encryption key or password can decrypt and read it.

What does encryption do?

It protects your data from being accessed or manipulated by anyone who should not see it.

In communication, encryption also helps ensure that we are speaking with the right person and not with an impostor.

How can I encrypt data?

VeraCrypt is a good, free, open-source encryption tool. Like a safe, VeraCrypt creates an encrypted container on your computer or hard drive into which you can put as many files as you want.

Remember:

- You must always close the encrypted container for it to work
- Adversaries who cannot break your encryption may try to steal your password and gain access that way
- Make sure you use very strong passwords and also follow the instructions in the malware course

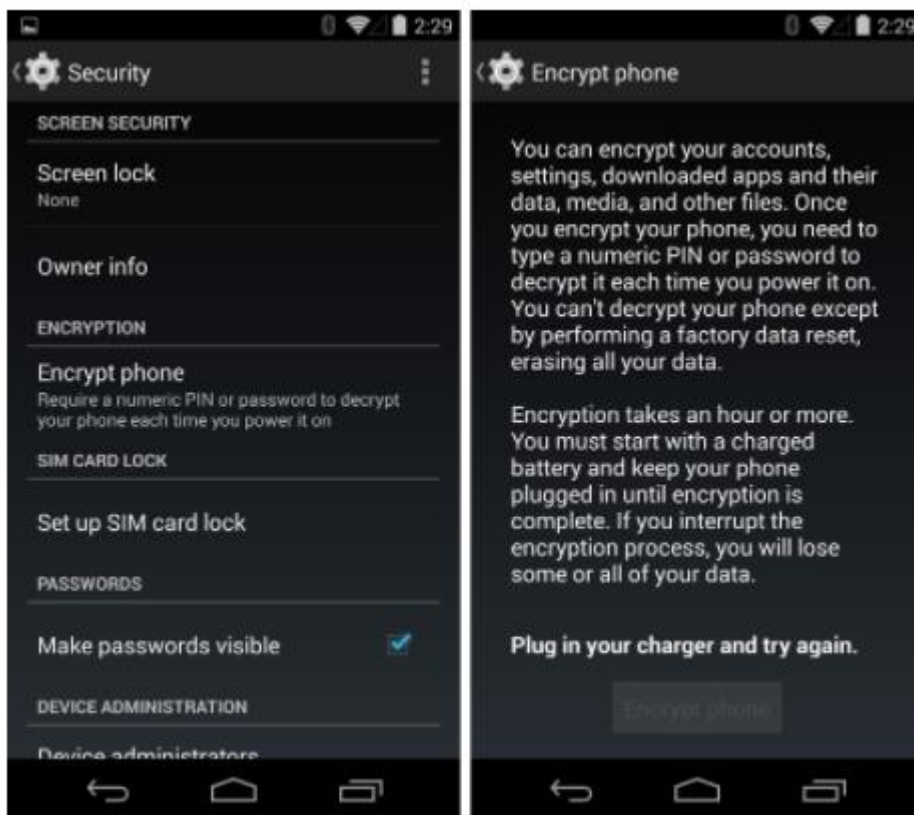
5.1 Encrypting Devices

Encrypting your devices, such as your computer and phone, is important. Without it, anyone who gains physical access to your device can easily access all your information. Many devices now have built-in full-device encryption that you can turn on to prevent this.

Below, we will show how to turn on encryption on Windows, Mac OS X, and Android phones.

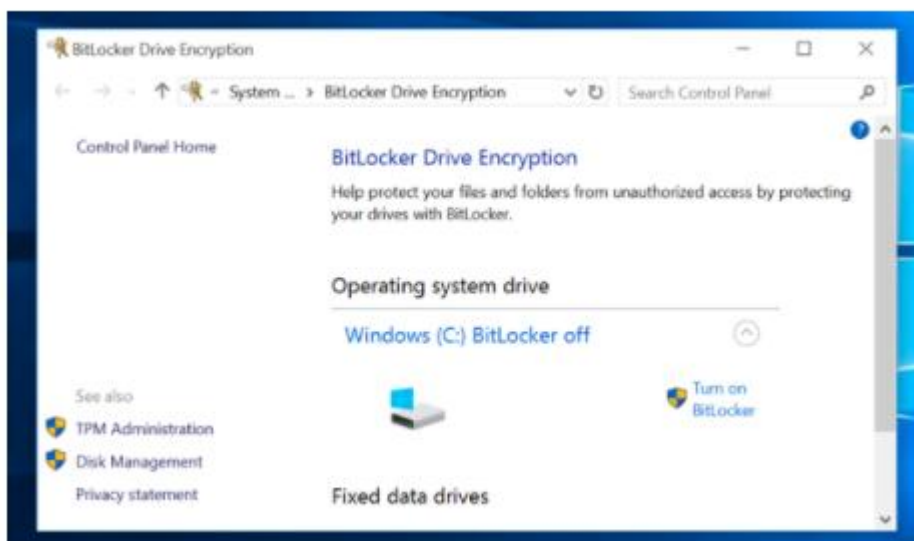
All Apple iPhones updated to the latest software version have encryption turned on automatically.

5.1.1 For Android:



1. Go to Settings
2. Go to Security
3. Select Encrypt phone

5.1.2 For Windows (Professional Version Only):



1. Go to Control Panel
2. Open BitLocker
3. Select "Encrypt"

5.1.3 For Mac OS X:



1. Go to System Preferences
2. Security & Privacy
3. Select FileVault

Remember:

- For encryption to work, you must always shut down your computer or lock your phone
- Your security is only as strong as your password
- Make sure you use very strong passwords
- Also follow the instructions in the malware course

6 Malware

Malware is a general umbrella term for several types of malicious software that a potential attacker may try to get onto your device (mobile phone, tablet, laptop, or PC).

You have certainly heard terms such as computer virus, worm, Trojan horse, spyware, and ransomware. These are all types of malware (from the English term “malicious software”) whose purpose is to get into your device and steal information from it, or to prevent you from accessing your information in order to extort you. Malware allows attackers to control your device remotely. It can access your sensitive data and payment cards, send emails and messages in your name, spread malicious code further, and so on. Here are a few examples of what an attacker can do:

- **Install a “keylogger” on your device.** It records everything you type on the device. This way, the attacker can read, for example, your passwords (this is also why passwords are usually hidden behind symbols such as dots or asterisks).
- **Take screenshots.** This means the attacker takes a picture of your screen every few seconds, allowing them to reconstruct exactly what you were doing and permanently store, for example, your personal conversations or photos that you think only you can see.
- **Search through your documents.**
- **Access your webcam and microphone,** allowing them to make recordings from your home, office, and so on.
- **Delete your documents.**
- **Encrypt your documents** and force you to pay a ransom if you ever want to access them again.
- **Access your system devices** and change them at will.

6.1 How Can Malware Get to You?

- Through infected hardware, such as a USB flash drive. There are known cases from various conferences where participants received infected USB drives among promotional materials.
- By clicking on an unknown malicious link through which a virus is downloaded to your device; for example, through a fake advertising banner.
- By downloading an email attachment.
- Through “drive-by downloads”—malware that starts downloading automatically when you visit a compromised or booby-trapped website.
- Through unlicensed “cracked” software. Attackers usually exploit the fact that people want to try new software for free and download it without paying the official distributor, or simply do not have enough money (Windows is a common example). Although not all free software on the internet is malicious, downloading it exposes you to a higher risk of downloading infected software.

6.2 How Can We Protect Ourselves Against Malware?

The way malware reaches us also gives us answers about how to protect ourselves.

- Install antivirus software with a good reputation; free antivirus versions also exist. Antivirus companies today detect up to 300,000 new and previously unknown malicious code samples every

day and can help you catch the most basic malicious code before you click on it. Regular antivirus updates are important; ideally, leave automatic regular updates enabled.

- Use licensed software and allow regular updates. Every piece of software may have potential security holes waiting to be discovered. Reliable companies therefore regularly release “patches” that protect your software from exploitation of known security vulnerabilities.
- Be very careful about “phishing”. Be careful with this form of attack because attackers may often pretend to be someone you know and trust and send you malware from an address similar to your friend’s address, either as a link or as an email attachment. Since this is one of the most common forms of attack, we will discuss it in more detail below.
- Watch out for social engineering: psychological manipulation of people into giving us confidential information. Social engineering can be good or bad; more details are provided below.

6.3 How Can You Avoid Phishing and Recognize It in the First Place?

You receive an email or a private message on social media. If it is from someone you do not know, or from someone from whom you are not expecting a message, immediately verify whether it is a legitimate contact. It is much worse when you receive a malicious attachment or link from someone you know or trust. This means the attacker has broken into that person’s account and is sending emails or messages under their name. Even here, however, you can work with the likelihood of whether you were expecting such a message from that person. For example, if you receive a strange attachment or link from your boss or your mother, without any specific explanation, and you know that this is not the style of email you usually receive from them, you should automatically be suspicious. More sophisticated attacks today even copy the style and manner of communication we are used to, and in such cases recognizing phishing is truly difficult.

The good news is that for malware sent to you through phishing to work, it must get onto your device, and we can prevent that.

Another form of phishing is to obtain your login and password through websites you regularly visit, such as Gmail, Facebook, or online newspapers you read. Usually, you receive a fake email pretending to be a message from the service provider with an urgent request to change your password and a link where you can do so. If you do this in panic and in a hurry, you give your password to the attackers. They can then completely lock you out of your service and, of course, access your data. Two-factor authentication can help protect you especially in this case.

Recommendation: Take a short quiz about malware and phishing and pay attention to the details. Feel free to take the quiz 2–3 times in a row, because this kind of training will increase your sensitivity to fraudulent emails and help you develop practice and habits around the details you need to notice. Quizzes available at:

- [Chapter 6 - Phishing and Social Engineering: Staying Vigilant Online | ResilienceLab.online / Quiz-chapter-6-phishing-and-social-engineering | ResilienceLab.online](#)
- <https://phishingquiz.withgoogle.com>

6.4 Social Engineering

Social engineering is psychological manipulation of people into giving us confidential information. It can happen online (for example, by phone) or offline (for example, in an office, at reception, etc.) Someone may pretend to be a postal worker, delivery service worker, or repair technician—in short, someone who does not arouse suspicion. If they physically get access to one of your devices, it is easier for them to access your other devices and bypass your security settings; this is also why all devices need to have different layers of protection activated, such as a password, PIN, and so on. Never allow a stranger, no matter how trustworthy they appear, to do anything on your device: for example, if they ask whether they can send an email or make a phone call from it.

Take special care with unknown USB drives that someone has supposedly forgotten somewhere. Our curiosity may lead us to want to see what is on the USB drive and unknowingly run malware on our device, giving hackers access.

6.5 Types of Malware

Stalkerware or spyware is an application that allows an attacker to spy on your device or to track your location and other data without your consent. It should be noted that many legal applications, such as Gmail, Facebook, chat services, and so on, automatically collect this information about you unless you manually deactivate it. Some applications of this kind may be installed without an icon, so you can easily overlook them and your device may be monitored remotely.

Adware (advertising-supported software) is software that automatically downloads and displays advertisements on your device. It generates revenue for developers every time an advertisement is displayed or clicked. It often spreads as a “bundled” bonus with free programs or applications.

A **virus** is a malicious program that copies itself and inserts its code into other files or programs.

A Trojan horse, or informally a **trojan**, is a type of malicious software that disguises itself as a harmless or useful program in order to deceive the user. Unlike classic computer viruses, it does not reproduce itself or infect other files but relies on the user unknowingly downloading and running it.

A computer worm is a type of malicious software that can replicate itself and spread across computer networks without requiring any user action. Unlike a classic virus, it does not need to “attach” itself to another program.

Ransomware is a type of malicious software that gets into your computer or network unnoticed. It then blocks access to your device or encrypts your files and the attackers demand payment of a ransom, most often in cryptocurrency, to unlock them.

A rootkit is an insidious type of malicious software that allows an attacker to gain control over a computer while hiding its presence. It hides from ordinary antivirus programs and task managers by integrating deep into the operating system or its kernel.

A keylogger is a software program or physical hardware device that secretly records every keystroke on a keyboard. Its main purpose is spying and stealing sensitive data, such as passwords, credit card numbers, and private messages.

7 IP Address and VPN

7.1 Ways Someone Can Obtain Your Internet Protocol (IP) Address

1

By borrowing your device: When someone works on your device, they can simply visit WhatIsMyIPAddress.com and that is it.

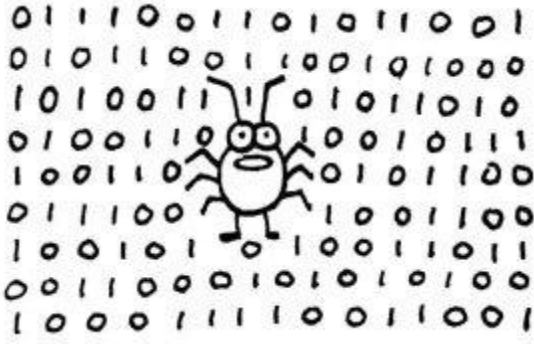
2

By breaking into your Wi-Fi network. If you allow any guest to use your Wi-Fi, they can find out your IP address.

3

By looking at your email: Fortunately, most email services no longer display your IP address, but smaller providers sometimes may. Try this tool and see what anyone can find out about you: [trace email tool](#).

4



Through an HTML bug. This little bug is not malicious and is not a virus. It is a piece of code inserted, for example, into an image in an email. When you view it, simply by opening the email, the bug tells the sender that you have read the email and also reveals your IP address. There are services that help people set up such bugs, such as WhoReadMe.com.

5

Web server logs. Every time you visit a website, you leave your IP address there. It is something like your digital passport for an online connection. The website may, if its administrator has set it up that way, have an overview of all IP addresses that have visited it. For websites, this is useful information because it lets them see whether a particular IP address visits regularly, how many random visits they have, and where visitors come from.

6

Internet forums and comments under blogs and articles: Again, it is very useful for site administrators to know your IP addresses because they can block you if you violate the rules of a given site; for example, when you spam a forum under different user names but the administrator sees that it is coming from one and the same IP address.

7

Through social networks (Facebook, Twitter, Instagram, Snapchat, etc.) IP addresses are not shown between users, but site administrators know your IP address. Also, when you click on an advertisement on social media, your IP address is captured.

9

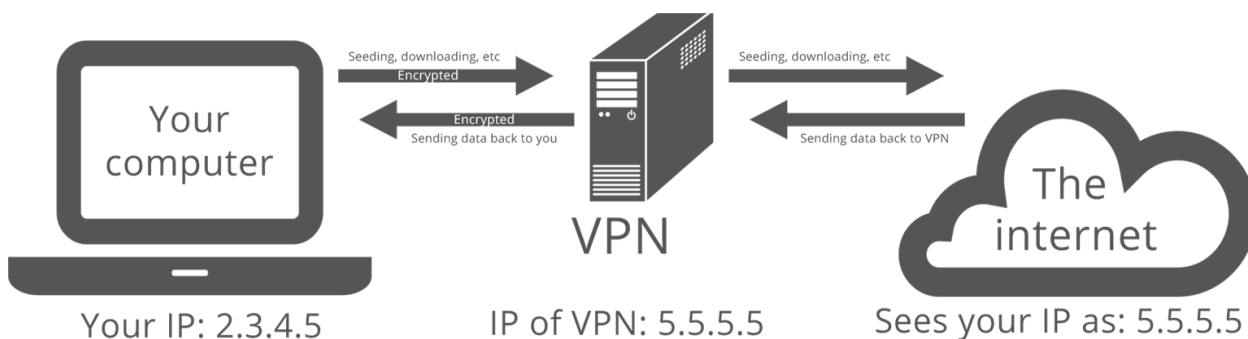
Through chat applications such as WhatsApp or Viber: when you click on a link in a message, you are taken to a website that captures your IP address. Such tracking links can be created, for example, on grabify.link or iplogger.org.

7.2 Virtual Private Networks (VPN)

The recommended way to protect your IP address, and therefore other details of your online presence, is to use a VPN, a kind of private and encrypted tunnel through which your information and online activities

flow. How it works is shown in the image below. Under normal circumstances, your device connects to the internet through your internet service provider (ISP), where your IP address is visible. If, however, you connect through a VPN server, that server changes your IP address as well as your geographic location and encrypts, or hides, your online activity and the flow of data and information. A VPN also encrypts the websites you visit through the Domain Name System (DNS), meaning stalkers or targeted advertising will not know your browsing history.

TechSoup Europe recommends using Proton VPN because, from a security perspective, it is one of the highest-rated VPNs, and also because its core server is physically secured. This means that even if an attacker reaches or hacks the VPN server, they will find only encrypted data on it. Proton VPN itself does not have access to your data. There are other VPN software options. Below are basic tips on what to look out for when choosing a VPN.



I am choosing a VPN—what should I look at?

Paid VPNs naturally offer better services than free versions, but every VPN is different. When choosing one, pay attention to the following:

Ratings by professional reviewers, who do not work for any of these companies. It is always good to verify sources across several rankings and reviews. There are many online, and this kind of checking does not take that long.

Shared IP addresses: Choose a VPN that offers shared IP addresses, meaning that several devices from different users will have the same IP address. The more such anonymous users there are, the more private your browsing is, because it is impossible for an attacker to distinguish who is who.

Servers: The more servers a company has available, the better the connection quality will be.

Encryption: At the time of writing, the most secure encryption is AES-256 (Advanced Encryption Standard), which is practically unbreakable because it uses more encryption combinations than there are stars in the universe, figuratively speaking.

Protocol: Avoid weaker protocols such as PPTP and choose the more reliable OpenVPN instead.

Data logs: Choose a VPN that does not store your data, meaning it does not record your online activities. You can find out whether it does so in its policy.

Free trial version: You can try a VPN before you start using it.

8 Security on Social Networks and Privacy Settings

Social networks bring various benefits to our lives, such as easier coordination of activities with friends, family, or colleagues. Many organizations have long promoted their activities and content through social media, and their message can reach a large number of people. However, using social networks also brings various risks. In this chapter, we will look at these risks and show basic ways to prevent or minimize them.

Most social networks are free. With this model, it usually applies that when something is free, the users of social networks and their data become the product: data about their behavior, privacy, interests, and so on. When you press the “I accept” button when signing up for a social network, you usually agree that these companies have the right to collect your personal data in exchange for their services. As a result, they can track your activity and also have access, for example, to the pages of the organizations that you manage.

What do social networks see/know?

- Who we are friends with
- Who we talked to and what we talked about
- When we talk to them
- When we spend time on the social network
- When and where we are located
- What type of information we follow and what interests us
- What we buy
- And much more

Metadata is usually used for the more targeted advertising and content that social networks offer you, which does not necessarily have to be bad. However, metadata also has its dark sides. In various countries, governments use it to monitor civic activists, but other people can also get access to this metadata. Attackers

Digital Security Guidelines for Civil Society Organizations

can break into your account in different ways through hacking or phishing and take control of it. They can use it in various ways, for example to share disinformation about you and as if from you, or to send malware in order to access other people's sensitive data, which they may use for blackmail.

To minimize these risks, you can adjust your security settings.

Principles for using social networks and recommendations for privacy settings:

- Limit the visibility of your posts (public vs. private)
- Have separate work and private accounts
- Limit the number of personal and sensitive posts
- Keep groups closed and check whom you allow into them
- Do not publish details about activists' meetings; certainly do not publish the meeting location unless it is necessary
- Turn off location sharing (location settings)
- Never allow a social network to remember your banking details
- If you do not know someone, never accept their friend request
- Watch out for fake accounts that look like your friends. If you receive a friend request from someone you know, verify whether it is really them, ideally by phone. Attackers often pretend to be your friends.
- Share as little as possible; do not share personal information
- Be aware of privacy and security settings—limit them
- Do not tag photos; at least not public ones
- Have a private account and a work account for managing pages
- Secure both accounts well and use two-factor authentication
- Do not use Facebook to sign in to other applications!!! Because of the potential leak of personal information and data
- Many digital security experts would say: do not use social networks at all; and if you already do, do not “like” anything, do not express yourself in any way, be anonymous, and so on (the extreme approach)

Today, under public or legal pressure, social networks allow better control over your personal data. From time to time, check whether your personal privacy and security settings are up to date and whether anything new has appeared there.

9 Resources

Free digital security training and quizzes: [Home](#) | [ResilienceLab.online](#)

Recommended reading on the risks of using social networks, their security, privacy, and other aspects of social media use:

- SCHNEIER, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton & Company, 2015. ISBN 978-0-393-35217-7.
- SCHNEIER, Bruce. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. New York: W. W. Norton & Company, 2018. ISBN 978-0-393-60960-8.
- MITNICK, Kevin and Robert VAMOSI: *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data*. New York: Little, Brown and Company, 2017. ISBN 978-0-316-38050-8.

Used resources:

- How to choose the right VPN: <https://blog.avast.com/cs/jak-si-vybrat-tu-spravnu-vpn>
- What is my IP address: <https://whatismyipaddress.com/get-ip> (shortened)
- Staying Safe Online by ESET: <https://bezpecnenanete.eset.com/sk/>
- Cybersecurity Glossary: <https://www.koop.cz/kyberbezpecnost-slovník>
- Kaspersky Resource Center: <https://www.kaspersky.com/resource-center>
- Visualization of the Largest Data Breaches:
<https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
- Keylogger: What It Is and How to Protect Yourself From It, 5 March 2025: <https://gdpr-slovensko.sk/keylogger-co-to-je-ako-funguje-a-ako-sa-pred-nim-chranit/>
- Rootkits in the Digital World: Threats and How to Protect Yourself, 9 March 2026:
[Rootkity v Digitálnom Svete: Hrozby a Ako sa Chránit'](#)

Annex 1: Social Media Exercise

What are you willing to upload to social media and why?

What do I usually share on social media? (Examples)	What benefits does it bring me? What do I gain from it?	What are the risks/disadvantages?
Photos (including personal ones, for example from holidays, family celebrations, and similar events)	Attention from friends and acquaintances I do not have to explain separately to everyone where I was and what I did there	Envy from others Someone knows that I am not at home now (burglars) A lot of personal information that can be misused (for example, where children go to school)
Photos of children	Sharing with distant family and friends	Misuse of photos Theft of photos Children's identity is revealed
Photos from work	Prestige, name recognition, advertising, brand building Raising awareness	N/A
Various personal dilemmas	I gain insight from people I do not normally talk to and whom I would not otherwise meet	I have no control over who reads it and when they may bring it up against me
When I am looking for/need something.	I can get it faster I get different opinions from people I trust	Everyone knows what I need; for example, that I am renovating my apartment
Political views/social views	A broader range of opinions	

What are you not willing to upload to social media, and why?

What I would never upload to social media	Why?
Intimate photos	Blackmail 9.1.1.1.6 Mobbing

Annex 2: Draft Security Plan

Security Plan (Organization Name)

List of People Involved in Implementing the Security Plan

People involved in designing and implementing cybersecurity measures			
Name	Role	Tel.	E-mail

IT Assets

Networks, storage, servers, and devices.

Important data we store, whether on an email server, in the cloud, or in Salesforce.

Sensitive data—credit card numbers and other protected data about target groups.

Security equipment—firewall, antivirus software, protective techniques (data encryption and backup).

Shared tools—for example, VPN, cloud monitoring, password manager.

Asset management table

Type of information	Location (device/online service)	Value (high, medium, low)	Relevant threats	Needed:
Passwords		High	If used without authorization: lockout from online services, loss of current data that has not yet been backed up, and possible takeover of the organization's online activities	<i>Install/purchase Bitwarden and train people how to use it</i> <i>Create a password database</i>
Folders containing sensitive data (contracts, payroll data, financial administration)		High	GDPR violation.	
Cloud file-sharing folders		Medium	Leakage of organizational data and content	
Folders		High	Lockout	
Mobile phones	Organizational/personal	High	Mixing personal and organizational matters, Leakage of sensitive information Control over communication	
USB drives		Low	Partial data leakage Potential GDPR violation	
Laptops + other devices / tablets		Medium		
Social media managed through a private account		Medium	Leakage of passwords and data Monitoring of internal communication Sharing malicious content under our name Stalking	

Digital Security Guidelines for Civil Society Organizations

			Doxxing Reputational damage	
Social media managed through an organizational account		Medium	Sharing malicious content under our name	
Other? Shared software (Salesforce, Miro, accounting software, etc.)		Medium	Various threats	

Measures for Detecting Threats to IT Assets

Decentralized antivirus software

Do you use a free antivirus version? Everyone individually? Shared paid antivirus?

Settings for shared accounts to send alerts about unusual sign-ins (unusual location, unusual device).

Which address receives these alerts?

Minimum requirements: Microsoft Defender enabled in Microsoft Windows, together with firewall protection and ongoing file scanning.

Optional settings: backup to Microsoft Cloud.

User Instructions and Standard Procedures

Although some threats come from outside our organization, many of them result from the actions of our team. To improve protection, the following procedures can be introduced:

Digital Security Guidelines for Civil Society Organizations

Instructions and standard procedures				
Area	Objective/purpose of the instruction	Instruction/procedure	Intended for	Note
VPN	Reduce the risk when connecting through public Wi-Fi networks	We recommend installing Proton VPN	Anyone who connects via Wi-Fi somewhere other than work or home	
Two-factor/multi-factor authentication	Important for reducing the risk of data leakage	We recommend introducing two-factor authentication for the most important accounts (email....)		
Backup	Prevent data loss in the event of device loss, disk failure, or ransomware attack		Anyone who creates new materials and stores them on individual or local devices that are not connected to a shared network and are not synchronized with Google Drive/OneDrive, etc.	
Encryption	Prevent data leakage in the event of device loss or a ransomware attack	Data whose leakage could cause a GDPR violation or threaten the organization's operations must be stored behind password protection. Encryption can be used for individual files with a simple password, as well as for entire folders	Anyone who has, on a device they use, data whose leakage could cause a GDPR violation or threaten the organization's operations	
Software updates	Prevent unauthorized access through older security vulnerabilities	Update the operating system, antivirus software, browser, and other programs that process data requiring protection	Anyone who uses organizational data through software that may be exposed to security vulnerabilities	

Procedure for Handling a Security Incident

Prevention is only one side of the cybersecurity equation.

We also need to have a procedure ready for what to do if a security breach is detected. This may involve simple steps, such as changing passwords or restoring data, or it may involve complex data analysis and seeking legal assistance.

At a minimum, we need to isolate the security incident and quickly move the affected data offline.

Identify threats and opportunities and assess their possible impact on the organization.

When this happens:	What needs to be done:	Note
Loss/theft of a mobile phone	Block the SIM card through the mobile operator and request a replacement with the same number. Arrange a replacement mobile phone with the same number as soon as possible because of two-factor authentication. If there is suspicion that someone accessed data on the lost/stolen mobile phone, change the passwords for individually used services and also for shared accounts that may have been compromised (for example, remembered in the mobile browser).	
Loss/theft of a laptop	Depending on the level of security on the lost/stolen laptop (login password, biometric unlocking, data encryption, etc.), assess the risk that someone accessed the data on it. Based on this, change the passwords for individually used services and also for shared accounts that may have been compromised (for example, remembered in the laptop browser), restore data from backups, and set an appropriate level of protection on the new laptop.	
Computer/laptop infected with a virus	Do not connect the laptop/computer to the shared network and do not sign in to the organization's online services. Back up data to a portable USB drive (not to the	

Digital Security Guidelines for Civil Society Organizations

	internal network, and not to shared Google Drive/OneDrive), try to remove the virus, depending on the result reinstall the entire computer if necessary (factory reset), scan the backed-up data with antivirus software, and then restore it. Then change the passwords for individually used services and also for shared accounts that may have been compromised (for example, remembered in the laptop browser). Use antivirus software to check and, if necessary, erase USB drives that were inserted at least once into the infected computer.	
Compromised password (Wi-Fi, online service, computer access password, etc.)	Change the affected password immediately. Verify the integrity of the data that may have been accessed without authorization (what is missing, what was changed), and run an antivirus check. If it was a password that would allow access to multiple services (for example, a computer login password or a password-manager master password), proceed as in the case of loss/theft of a laptop.	
Ransomware attack	Disconnect the computer/laptop completely from the network. Inform others who may also be at risk so they can back up their data in time and protect their computers (computers connected to the same internal network as yours, or computers to which you transferred data via a USB drive during the period when the ransomware infection may have occurred). Consult an expert on the next steps.	

Cybersecurity Testing and Audits

Regular measures for identifying new weaknesses.

Cybersecurity audits that allow us to assess how effective the protection is and whether the security plan needs to be updated.

HaveIBeenPwned/Firefox Monitor (check the addresses of all staff members and, in the event of a data/password leak, send them information about changing their password)

<https://haveibeenpwned.com/>

<https://monitor.mozilla.org/>

Date checked and added to Firefox Monitor	Staff member	Action/note

Regular password changes (at least once a year for the most important accounts)

Date of change	Which accounts did we change?	Who changed them?

Cybersecurity Training

A reminder of the organization's standard procedures; how to identify and report suspicious behavior, emails, phone calls, and websites; and how to become familiar with new types of threats.

Employee cybersecurity training			
Training topic	Planned date (day or month)	Responsible person	Note

Security Plan Update

Security plan update			
Security plan version	Update date (month)	Person	Note

Useful links:

Free digital security training and quizzes tailored for civil society: [Home | ResilienceLab.online](#)

National Cyber Security Centre UK, <https://www.ncsc.gov.uk/section/advice-guidance/all-topics>

The Hacker News, <https://thehackernews.com/>



**Co-funded by
the European Union**

Disclaimer: The views expressed herein are those solely of the author(s).
TF, GMF, PDCS and ACA, EACEA do not take positions.

**G | M | F Transatlantic
Foundation**

<https://www.gmfus.org/transatlantic-foundation>



<https://www.pdcs.sk>



<https://altkozegy.hu>