



The digital security toolkit: a practical guide for safer online engagement

▼ Welcome section

▼ Introduction

This toolkit was created during the Erasmus Plus training course **“Raising the level of digital security among European young adults”** (2023-1-EL02-KA153-YOU-000119724). The training took place from **10th to 18th October 2024 in Corfu, Greece** and brought together **28 youth workers, educators, and NGO leaders** from **Greece, Romania, Germany, North Macedonia, Ukraine, Estonia, and Türkiye**, supported by **one facilitator and one trainer**.

The project was made possible through the collaboration of several partner organizations:

- **Youth Line Greece (Greece)**
- **Asociația MULTIKULTI (Romania)**
- **Association for Education and Development of Young People – EduArt Skopje (North Macedonia)**

- **Civic Organization "Development and Initiative" (Ukraine)**
- **Avatud Ühiskond MTÜ (Estonia)**
- **Martı Gençlik Derneği (Türkiye)**
- **Youth Line Germany (Germany)**

The goal of this toolkit is to help youth workers and young people **stay safe online**. It includes **simple tips, tools, and advice** on how to **protect personal data, avoid online risks, and use digital tools safely**.

Whether you are learning about digital security for the first time or want to improve your skills, this toolkit will help you **understand important online safety practices** and **share this knowledge** with others.

 **This project is funded by the Erasmus Plus program of the European Union.**



▼ Why digital security matters: surprising facts


Here are some surprising facts about digital security that highlight why staying safe online is so important. These quick insights will help you understand the risks and motivate you to build better digital habits.

🛡️ **Did you know that 90% of successful cyberattacks start with a phishing email?**


Hackers rely on tricking people into clicking fake links or sharing personal information. This is why learning to recognize phishing scams is essential.

🔒 **A strong password with at least 12 characters is 10,000 times harder to crack than a shorter one.**


Short and simple passwords are easy for hackers to guess. Using a password manager helps you create strong, unique passwords for all your accounts.

 **Backing up your files can save you from losing important data in a cyberattack.**

Ransomware attacks often lock your files and demand money to unlock them. With backups, you can restore your data without paying.

 **Using public Wi-Fi without a VPN is like shouting your private information in a crowded room.**

Hackers can easily intercept your data on public networks unless you use a VPN to encrypt your connection.

 **Apps with end-to-end encryption, like Signal Messenger, ensure only you and the recipient can read your messages.**

This type of encryption makes your conversations private and secure from hackers or third parties.

▼ **Cybersecurity trends: future challenges and emerging threats**

Digital security is constantly evolving, and new challenges emerge as technology advances. Understanding these trends can help you prepare for future risks and make informed decisions about your online safety.

AI-generated phishing attacks

Artificial intelligence (AI) is making phishing scams more advanced and harder to detect. Hackers can now create highly convincing fake emails, messages, or websites that look legitimate. Some even use voice or video deepfakes to impersonate trusted individuals.

Why it matters:

- AI-generated phishing is more personalized, increasing the chances of people falling for the scam.
- Traditional warning signs, like poor grammar, are becoming less common.

How to prepare:

- Be cautious, even with professional-looking messages.
- Verify requests for sensitive information through trusted methods, such as a phone call or direct communication.
- Use anti-phishing tools like NextDNS to block malicious websites.

Securing IoT (Internet of Things) devices

Smart devices like speakers, fitness trackers, and home appliances are convenient but often lack proper security. Hackers can exploit these devices to access private networks or data.

Why it matters:

- Many IoT devices have weak or unchanged default passwords.
- Compromised devices can be used to launch larger attacks on other systems.

How to prepare:

- Change the default passwords of your IoT devices immediately.
- Use a separate Wi-Fi network for IoT devices to reduce risk.
- Regularly update device software to fix vulnerabilities.

Updates on EU digital safety regulations

The European Union continues to lead efforts in improving digital safety and user rights. New regulations focus on protecting personal data, combating online harm, and ensuring secure communication.

Examples of recent initiatives:

- **GDPR (General Data Protection Regulation):** Sets strict guidelines for data privacy and user control.
- **Digital Services Act (DSA):** Targets harmful content, fake news, and illegal activity on digital platforms.
- **Digital Education Action Plan (2021-2027):** Encourages stronger digital skills, including cybersecurity awareness.

How to prepare:

- Stay informed about EU regulations and ensure compliance in your work.
- Choose tools and platforms that align with EU safety standards.

Rise of ransomware and advanced malware

Ransomware attacks, which lock files until a payment is made, are becoming more targeted and sophisticated. Hackers often target vulnerable sectors like healthcare, education, or individuals with critical data.

Why it matters:

- Recovery can be costly, and paying the ransom doesn't guarantee file restoration.
- Advanced malware can bypass outdated defenses.

How to prepare:

- Back up your important files regularly and store them securely offline.
- Use antivirus software, like Avast AV, to detect and block threats.
- Be cautious of suspicious links or downloads.

Growing importance of cybersecurity education

As digital threats become more complex, educating individuals about online safety is critical. Empowering people to recognize risks and take preventive steps is key to building a safer digital environment.

How to contribute:

- Organize workshops or training sessions on digital safety.
- Share resources, like this toolkit, to increase awareness in your community.

▼ Glossary of key terms

This glossary provides simple definitions for important digital security terms. Use it to better understand the concepts and tools mentioned in this toolkit.

Anonymous browsing: Using tools, like the Tor Browser, to hide your identity and location while online. This method ensures greater privacy but requires advanced tools to achieve full anonymity.

Cybersecurity: The practice of protecting systems, networks, and programs from digital attacks. It involves using tools and practices to secure personal and professional information.

Digital footprint: The trail of data you leave behind when using the internet, such as search history, social media activity, and uploaded files. Managing your digital footprint is essential for online privacy.

Encryption: A method of securing information by converting it into a code, so only authorized users with the correct key can access it. Encryption protects data during transmission and storage.

End-to-end encryption: A system where only the sender and recipient can read messages. Even the messaging app's servers cannot access the content of your conversations.

Firewall: A security tool that blocks unauthorized access to a computer or network. It acts like a digital barrier, allowing safe traffic while keeping out potential threats.

Malware: Harmful software, such as viruses, spyware, or ransomware, designed to damage your computer or steal personal information.

Password manager: A tool that creates, stores, and auto-fills strong, unique passwords for all your accounts, helping to protect them from hackers.

Phishing: Fake emails, messages, or websites designed to trick you into sharing personal information like passwords, credit card numbers, or other sensitive data.

Private browsing: A browser mode that doesn't save your browsing history, cookies, or search data during your session. However, it doesn't hide your identity or location.

Ransomware: A type of malware that locks your files and demands a payment (ransom) to restore access.

Two-factor authentication (2FA): An extra layer of security for online accounts that requires a second verification step, like entering a code sent

to your phone, in addition to your password.

VPN (Virtual Private Network): A service that encrypts your internet connection and hides your IP address, making your online activity private and secure.

▼ What is digital security?

Digital security is about protecting your personal information and online activities from hackers, scams, and other online threats. It involves using tools and safe practices to make sure your private data, like passwords, personal messages, or work documents, stays safe from people who want to steal or misuse it.

Every time we use the internet—whether it's to check emails, shop online, or share on social media—we leave a digital footprint. This information can be accessed by others if it's not protected properly. Digital security helps you take control of your online safety and reduces the risks of cyberattacks.

Digital security is important because it protects not only your personal information but also the people and organizations you work with. Here's why:

- **Protects personal and work information:** If your private information falls into the wrong hands, it can be used to harm you or others. Digital security ensures that your passwords, personal data, and work files are safe from hackers.
- **Keeps young people safe online:** Young people are especially vulnerable to online risks, like scams or cyberbullying. Digital security gives them tools and knowledge to avoid unsafe situations and build good online habits.
- **Stops identity theft, phishing, and cyberbullying:** Hackers can use stolen data to pretend to be you (identity theft) or trick you into giving away sensitive information (phishing). Cyberbullying can also happen when private messages or images are shared without permission. By staying secure online, you reduce the chances of these threats.

By understanding and practicing digital security, you can stay safe online, protect your identity, and create a safer digital environment for everyone.



- ▼ **Tools to stay safe online**
 - ▼ **VPNs (Virtual Private Networks)**

A **VPN (Virtual Private Network)** is a tool that protects your online activity by hiding your internet connection. It creates a secure, private “tunnel” between your device and the internet, making it harder for hackers, advertisers, or websites to track what you do online. A VPN also hides your IP address, which can prevent others from knowing your location or identity.

Using a VPN is very important when you are on **public Wi-Fi networks**, like in a café, library, or airport. Public networks are not secure, and hackers can easily intercept your data. A VPN helps protect your sensitive information, such as passwords, financial details, or work files.

Why should you use a VPN?

- **To keep your browsing private:** A VPN stops websites and advertisers from tracking your online activity.
- **To protect personal data on public Wi-Fi:** Hackers often target public networks, but a VPN encrypts your connection, making it much safer.
- **To access restricted content:** In some countries, certain websites or services are blocked. A VPN lets you connect to the internet as if you are in another location, giving you access to what you need.
- **To keep your location hidden:** A VPN hides your real IP address, so your location remains private.

Examples of when to use a VPN

- **When working remotely:** If you’re handling sensitive work files on your laptop, a VPN ensures they stay secure.
- **When traveling:** Access websites, apps, or services that may be restricted in another country.
- **When shopping online:** Prevent hackers from stealing your payment information.
- **When using public Wi-Fi:** Protect your data at airports, hotels, or cafes.

Recommended tools

1. **ProtonVPN** (protonvpn.com)

- **Why use it?** ProtonVPN is free, secure, and easy to use. It offers strong encryption and a beginner-friendly interface.

2. Mullvad VPN (mullvad.net)

- **Why use it?** Mullvad VPN is highly privacy-focused. It doesn't require personal information to create an account and allows anonymous payments like cash.

▼ Password managers

A **password manager** is a tool that helps you create, save, and use strong passwords for all your online accounts. Instead of trying to remember many complicated passwords, you only need to remember one master password to access your password manager. This makes it easier to stay secure without using weak or repeated passwords.

Using a password manager protects your accounts from hackers who try to guess or steal your passwords. It can also generate random, strong passwords for each website or app you use, which makes your accounts much harder to hack.

Why use a password manager?

- **Keeps your passwords safe:** Stores your passwords in a secure, encrypted vault.
- **Saves time:** Auto-fills your usernames and passwords for quick logins.
- **Protects against weak passwords:** Creates strong, unique passwords that are hard to guess.
- **Reduces risk:** Prevents using the same password on multiple sites, which is a common security problem.

How does it work?

1. Install the password manager on your device or browser.
2. Add your passwords for websites and apps.
3. Use the auto-fill feature to log in securely without typing passwords manually.

Recommended tool

BitWarden (bitwarden.com)

- **Why use it?** BitWarden is free, secure, and works on all devices, including phones, laptops, and browsers. It is open-source, which means its code is reviewed by security experts.

▼ Two-factor authentication (2FA)

Two-factor authentication (2FA) adds an extra layer of security to your online accounts. Instead of just using a password, 2FA requires a second step to confirm your identity. This could be a code sent to your phone, an email, or a notification from an app. Even if someone steals your password, they can't access your account without this extra verification.

Why use 2FA?

- **Extra protection:** Makes it much harder for hackers to access your accounts.
- **Secures important accounts:** Adds safety to accounts like email, social media, and banking.
- **Prevents password-only hacks:** Even if your password is stolen, 2FA keeps your account safe.

How does it work?

1. Enable 2FA in your account settings (e.g., Gmail, Facebook, or Instagram).
2. Choose your verification method (e.g., SMS code, email, or app-based code).
3. When logging in, enter your password first, then the verification code sent to your device.

Recommended tool

Twilio Authy (authy.com)

- **Why use it?** Twilio Authy is simple to set up and supports many popular services. It also lets you back up your codes securely, so

you won't lose access even if you lose your phone.

▼ Phishing and malware protection

Phishing and malware are two of the most common online threats. **Phishing** is when someone tricks you into sharing sensitive information, like passwords or bank details, through fake emails or websites. **Malware** refers to harmful software that can infect your computer or phone, steal your data, or damage your files.

To stay safe, it's important to use tools that protect you from these threats. These tools can block dangerous websites, scan for viruses, and prevent malware from infecting your device.

Why is it important?

- **Stops harmful websites and ads:** Prevents you from clicking on dangerous links that could steal your information.
- **Protects against phishing emails:** Blocks fake emails that look like they're from trusted companies.
- **Keeps your devices clean:** Scans and removes viruses and other harmful software.

Recommended tools

1. NextDNS (nextdns.io)

- **Why use it?** NextDNS blocks access to dangerous websites, trackers, and malicious ads. It works in the background to ensure your browsing stays safe.

2. MalwareBytes (malwarebytes.com)

- **Why use it?** MalwareBytes scans your device for viruses and removes harmful files. It's an easy way to keep your computer and phone secure.

How to protect yourself

1. Avoid clicking on links from unknown emails or messages.
2. Double-check the sender's email address before responding.

3. Use tools like NextDNS and MalwareBytes to block and remove threats.

▼ Firewalls

A **firewall** is a security tool that helps protect your computer or device from unauthorized access. It acts like a barrier, blocking harmful traffic from entering your network and keeping hackers from accessing your personal information.

Firewalls are an important part of staying safe online. Most modern devices, like computers and smartphones, come with built-in firewalls. However, you need to make sure they are turned on and properly configured.

Why is a firewall important?

- **Blocks hackers:** Stops unauthorized users from accessing your computer or network.
- **Protects sensitive information:** Prevents your personal or work data from being stolen.
- **Stops harmful software:** Blocks suspicious traffic and prevents malware from spreading.

How to activate your firewall

1. **Windows:** Go to your settings, search for "Firewall," and make sure it is turned on.
2. **MacOS:** Open "System Preferences," go to "Security & Privacy," and enable your firewall.
3. **Smartphones:** Most phones have automatic security features, but you can check in your settings to ensure your firewall is active.

▼ Automatic updates

Automatic updates ensure that your devices and apps stay secure by automatically downloading and installing the latest security fixes and improvements. These updates fix vulnerabilities that hackers could exploit, making your system safer and more reliable.

While it can be tempting to skip updates, leaving your devices out of date increases the risk of cyberattacks. Turning on automatic updates saves time

and ensures you are always protected, without needing to remember to check for updates manually.

Why are automatic updates important?

- **Fixes security problems:** Updates close vulnerabilities that hackers might exploit.
- **Improves performance:** Keeps your devices running smoothly with the latest features and bug fixes.
- **Protects sensitive data:** Ensures your information is safe from newly discovered threats.

How to turn on automatic updates

1. For your operating system:

- **Windows:** Go to "Settings," click on "Update & Security," and enable automatic updates.
- **MacOS:** Open "System Preferences," go to "Software Update," and check "Automatically keep my Mac up to date."

2. For your apps:

- On most smartphones and tablets, go to your app store settings (e.g., Google Play or Apple App Store) and enable automatic app updates.

3. For your browser:

- Make sure automatic updates are enabled in your browser settings (e.g., Chrome, Firefox, or Edge).

▼ Antivirus software

Antivirus software is a tool that scans your computer or device for viruses and removes harmful files. It helps protect your system from threats like malware, spyware, and ransomware, which can steal your data or damage your files.

While following good security practices like using strong passwords and enabling automatic updates reduces risks, antivirus software adds an extra

layer of protection. It can detect and stop harmful programs before they cause serious problems.

Why use antivirus software?

- **Detects and removes viruses:** Scans your device for harmful software and deletes it safely.
- **Protects sensitive data:** Stops viruses that can steal your personal or financial information.
- **Prevents slow performance:** Blocks malicious files that can slow down your computer.
- **Provides real-time protection:** Alerts you to potential threats as they happen.

Recommended tool

Avast AV ([avast.com](https://www.avast.com))

- **Why use it?** Avast AV is a free and reliable antivirus solution. It offers real-time protection, regular updates, and an easy-to-use interface.

▼ Practical scenarios

VPNs (Virtual Private Networks)

Scenario: Katya, a youth worker, is at a conference and connects to the hotel's free Wi-Fi to join an online workshop. A hacker on the same network intercepts her data. When Maria logs into her email, the hacker gets her login details.

Lesson: If Katya had used a VPN, her internet traffic would have been encrypted, and the hacker wouldn't be able to see her data. Always use a VPN when on public Wi-Fi.

Phishing and malware protection

Scenario: Kiril gets an email that looks like it's from his bank. It asks him to click a link to confirm his account. The email looks real, but Kiril checks the sender's address and notices it doesn't match the bank's official website. He realizes it's fake.

Lesson: Hackers use fake emails to steal information. Always check the sender's email address and don't click on links you don't trust. Tools like NextDNS can block harmful websites.

Password managers

Scenario: Angelica uses the same password for her email, social media, and bank account. A hacker gets access to her social media account and uses the same password to log into her email and bank account.

Lesson: Using a password manager like BitWarden helps you create strong, unique passwords for every account, so one stolen password won't harm all your accounts.

Two-factor authentication (2FA)

Scenario: Ligas email password is stolen in a data breach. But her account is protected with two-factor authentication, so the hacker cannot log in without the code sent to Ligas phone.

Lesson: 2FA adds an extra layer of security to your accounts, even if your password is stolen.

Firewalls

Scenario: Dimitris downloads an app from an unknown website. The app installs malware that tries to access Dimitris private work files. Luckily, Dimitris firewall blocks the suspicious activity and warns him.

Lesson: Firewalls stop unauthorized access and protect your system from harmful activity. Always keep your firewall turned on.

Automatic updates

Scenario: Fred delays installing updates on her laptop because she doesn't want to restart it. A week later, hackers exploit a weakness in her outdated system to install ransomware that locks all her files.

Lesson: Updates fix security problems in your system. Turn on automatic updates so your devices stay protected.

Secure messaging

Scenario: David shares important project details over a messaging app that isn't encrypted. Later, he finds out the app was hacked, and his conversation was leaked.

Lesson: Using secure apps like Signal ensures your messages are private and safe from hackers.

▼ List of useful tools

VPNs (Virtual Private Networks)

- [ProtonVPN \(Free\)](#)
- [Mullvad VPN](#)
- [Windscribe VPN \(Free\)](#)
- [ExpressVPN \(Premium\)](#)
- [NordVPN \(Premium\)](#)

Password managers

- [BitWarden \(Free\)](#)
- [1Password Teams \(Premium\)](#)
- [Dashlane Business \(Premium\)](#)

Two-factor authentication (2FA)

- [Twilio Authy](#)

Phishing and malware protection

- [NextDNS](#)
- [MalwareBytes](#)

Antivirus software

- [Avast AV \(Free\)](#)
- [Microsoft Defender \(Free, Windows\)](#)

Secure messaging

- Signal Messenger

Tools for youth workers and educators

- Be Internet Awesome
- Common Sense Education
- Padlet
- Mentimeter

▼ Safe browsing and communication

▼ Browsing safely

Private browsing

Private browsing is a feature that prevents your browser from saving your search history, cookies, and other data during your session. However, it does **not hide your identity** or protect your location. Websites and internet service providers (ISPs) can still track your activity.

When to use it:

- On shared devices, to avoid leaving your browsing history behind.
- To prevent websites from keeping cookies during your session.

Anonymous browsing

Anonymous browsing hides your identity, location, and activity by using advanced tools like the **Tor Browser**. The Tor Browser encrypts your internet traffic and routes it through multiple servers, making it very difficult to track.

Recommended tool:

- **Tor Browser** (torproject.org) – Designed for anonymity and privacy.

When to use it:

- To keep your activity hidden from trackers.
- When accessing restricted or censored content (responsibly).

Important warning

While the Tor Browser provides excellent privacy, it also allows access to the **Dark Web**, which includes unsafe and illegal content. If you use the Tor Browser, stick to known websites and avoid clicking on unfamiliar links.

▼ Secure messaging

Secure messaging is a way to protect your private conversations from being read by others. Many popular messaging apps are not fully secure, meaning hackers, companies, or even governments could potentially access your messages.

Apps with **end-to-end encryption** ensure that only you and the person you're messaging can read your conversation. This is especially important for protecting sensitive information, personal privacy, or work-related communication.

Why use secure messaging?

- **Keeps your conversations private:** Messages are encrypted and cannot be read by anyone else.
- **Prevents hacking:** Protects your messages from being intercepted by hackers.
- **Supports personal and professional safety:** Ensures both personal chats and work discussions stay secure.

Recommended tool

Signal Messenger (signal.org)

- **Why use it?** Signal Messenger is free, secure, and trusted by privacy experts worldwide. It uses strong encryption, does not store your data, and works on phones and desktop devices.

How to stay secure while messaging

1. Use apps with **end-to-end encryption**, like Signal.
2. Avoid sharing sensitive information (e.g., passwords or financial details) in messages.

3. Be cautious of suspicious links sent through messaging apps.

▼ **Cybersecurity awareness and education**

▼ **How hackers trick you**

1. Fake emails or websites (phishing)

Phishing is one of the most common tricks hackers use. They send fake emails or create websites that look like they are from trusted companies, such as banks or online stores. These messages often ask for your personal information, like passwords or credit card details.

What to do:

- Always double-check the sender's email address.
- Avoid clicking on links in emails unless you are sure they are safe.
- Never share sensitive information through email.

2. Public Wi-Fi networks without a VPN

Hackers can use public Wi-Fi networks, like those in cafes or airports, to intercept your data. If you're not using a VPN (Virtual Private Network), your online activity and personal information can be exposed.

What to do:

- Avoid using public Wi-Fi for tasks like banking or online shopping.
- Use a VPN to encrypt your connection and stay secure.

3. Weak passwords

Hackers often guess passwords using tools that can try millions of combinations in seconds. If your passwords are short, simple, or reused across accounts, they are easy targets.

What to do:

- Use a password manager to create and store strong, unique passwords for every account.

- Avoid using obvious passwords like "123456" or "password."

▼ **Example: "How to hack someone's phone in 2 easy steps"**

How it happens:

1. Using a weak password

Hackers can easily guess weak passwords, such as "123456" or "password." With tools that try millions of combinations in seconds, it's only a matter of time before they crack a simple password.

2. Connecting to public Wi-Fi without protection

Public Wi-Fi networks, like those in cafes or airports, are not secure. Hackers can intercept data being sent over these networks, such as login details, messages, or personal files. Without a VPN, this information is exposed and vulnerable to attack.

Lesson learned

- **Always use strong passwords:** Create unique, complex passwords for each account and store them securely in a password manager.
- **Secure your network with a VPN:** A VPN encrypts your internet connection, making it much harder for hackers to intercept your data, even on public Wi-Fi.

▼ **Tips to stay safe online**

1. Do not click on links from people you do not trust

Hackers often send fake links through email, social media, or messaging apps. These links can lead to phishing websites or download harmful software onto your device.

What to do:

- Double-check the sender before clicking any link.
- Hover over the link to see where it leads. If it looks suspicious, don't click.

2. Keep your social media accounts private

Sharing too much personal information on social media can make you a target for scams or cyberbullying.

What to do:

- Adjust your privacy settings so only friends or trusted people can see your posts.
- Avoid sharing sensitive information like your phone number, address, or travel plans.

3. Back up your important files

Losing important files due to a cyberattack or device failure can be devastating. Backups ensure your data is safe and can be recovered if needed.

What to do:

- Use cloud storage services like Google Drive or Dropbox.
- Save copies of your files on an external hard drive.
- Set up automatic backups for your most important documents.

▼ Teaching others about digital safety

As a youth worker, educator or NGO leader, you play a key role in teaching others how to stay safe online. Many young people and community members may not be aware of the risks they face or the tools they can use to protect themselves. By sharing knowledge and practical skills, you can empower them to navigate the digital world securely.

How to teach digital safety

1. Host workshops about online safety

Organize interactive workshops where young people can learn about digital risks, such as phishing, cyberbullying, or weak passwords. Use real-life examples to make the sessions relatable and engaging.

Ideas for workshops:

- Understanding common online threats.
- Creating strong passwords and using password managers.
- Setting up VPNs and enabling automatic updates.

2. Share simple tools and examples

Use the tools and strategies in this toolkit to demonstrate how easy it can be to stay safe online. Share practical examples, such as installing a VPN or activating two-factor authentication, to show how these tools work in real life.

Example activities:

- Step-by-step demonstrations of secure apps like Signal Messenger or BitWarden.
- Group discussions on identifying fake emails and phishing scams.

3. Help others set up safe practices

Many people don't take steps to secure their online activity because they don't know where to start. Offering one-on-one support or group training sessions can help them set up important protections like:

- Strong, unique passwords for all accounts.
- VPNs to secure public Wi-Fi connections.
- Automatic updates to keep devices safe and up to date.



▼ Extra resources

Staying informed about digital security and youth work practices is essential for creating a safer online environment. Below are some valuable resources that provide additional tools, guidelines, and information to help you grow your knowledge and skills.

1. Digital Education Action Plan 2021-2027

The European Union's **Digital Education Action Plan** outlines important guidelines for improving digital skills and promoting safe practices in youth work. It offers strategies to support educators and youth workers in adapting to the challenges of a digital world.

Learn more about the plan and its objectives:

[EU Digital Education Action Plan](#)

2. General tools for youth work, productivity, and life

This resource provides practical tools and apps that youth workers can use to improve their productivity and better support young people. From organization apps to creative digital tools, it's a helpful starting point for anyone working with youth.

3. European Youth Portal

The **European Youth Portal** offers opportunities and information for young people across Europe. It includes resources on volunteering, education, and training, as well as information about programs like Erasmus+.

Visit the portal: europa.eu/youth

4. Cyber Aware (UK)

Cyber Aware is a UK-based initiative that shares easy-to-understand tips and advice for staying secure online. It covers everything from password safety to protecting yourself from online scams.

Explore the website: cyberaware.gov.uk

▼ Conclusion

▼ Checklist for staying safe online

Use strong, unique passwords

- Create passwords that are at least 12 characters long, with a mix of letters, numbers, and symbols.
- Use a password manager, like BitWarden, to store and generate secure passwords.

✓ **Enable two-factor authentication (2FA)**

- Turn on 2FA for all important accounts, such as email, social media, and banking.
- Use an app like Twilio Authy to securely manage your 2FA codes.

✓ **Avoid clicking on suspicious links**

- Don't open links or download attachments from unknown emails or messages.
- Double-check the sender's address and hover over links to see where they lead.

✓ **Always use a VPN on public Wi-Fi**

- Public networks, like those in cafes or airports, are not secure.
- Protect your connection with a VPN like ProtonVPN or Mullvad VPN.

✓ **Back up important files regularly**

- Use cloud storage or an external drive to keep a copy of your essential files.
- Set up automatic backups for added convenience and safety.

How to use this checklist

- Review this list regularly to maintain good digital security habits.
- Share it with friends, family, or colleagues to help them stay safe online too.

▼ **Closing remarks**

Digital security is an essential part of our lives in an increasingly connected world. By adopting the tools, strategies, and practices outlined in this toolkit, you can protect your personal information, empower others, and contribute to a safer online environment.

The steps may seem small, but their impact is significant. From creating strong passwords to teaching others about cybersecurity, every effort you

make helps reduce risks and build a culture of digital safety. As you apply what you've learned, remember that staying informed and proactive is the best way to stay ahead of evolving threats.

We hope this toolkit serves as a valuable resource for your journey toward safer online engagement. Share it with your community, and together, let's make the digital world a safer place for everyone.

▼ **Contacts**

 [Website](#)

 [Facebook](#)

 [Instagram](#)

 [LinkedIn](#)

 youthline.gr@gmail.com





**Co-funded by
the European Union**

Youth Line
FAMILY