Personal Data Protection & Cybersecurity

Bridge4Mothers **© 2026 by** *Bridge4Mothers Erasmus+ VET KA210* **is licensed under** *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

PERSONAL DATA PROTECTION & CYBERSECURITY

Every time we use the Internet, shop online, send emails, or use social media, we share information about ourselves. While technology makes everyday tasks easier, it also creates new risks such as identity theft, online fraud, and cyberattacks. Understanding how to protect your personal information is an essential digital skill.

In this module, you will learn how to recognize common online threats, protect your personal data, create strong passwords, and use digital services safely. These practical skills will help you use technology with greater confidence while reducing the risk of becoming a victim of cybercrime.

💡 **Tip:** Cybersecurity is not only for IT professionals. Everyone who uses the Internet plays a role in protecting their personal information.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

UNDERSTANDING PERSONAL INFORMATION

Personal data is any information that can identify you directly or indirectly. Some examples include your name, address, telephone number, email address, date of birth, national identification number, and bank account details. Even photographs, location data, and IP addresses may be considered personal data.

Many websites and applications collect personal information to provide their services. Knowing what information you are sharing helps you make informed decisions about your privacy and reduces the risk of misuse.

💡 **Tip:** Before entering personal information online, ask yourself whether it is really necessary.

Did You Know? Even a combination of small details, such as your birthday and hometown, can help identify you.

Bridge4Mothers © 2026 by *Bridge4Mothers Erasmus+ VET KA210* is licensed under *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

YOUR INFORMATION HAS VALUE

Personal information is valuable not only to you but also to businesses, organisations, and unfortunately, cybercriminals. Criminals may try to steal personal information to commit identity theft, financial fraud, or access your online accounts.

Protecting your data helps safeguard your privacy, finances, and reputation. It also reduces the risk of unauthorized access to your accounts and prevents others from using your identity without permission. Good cybersecurity habits protect both individuals and organisations.

💡 **Tip:** Share only the information that is necessary for the service you are using.

⚠️ **Remember:** Once sensitive information has been exposed online, recovering from the damage can be difficult.

Bridge4Mothers © 2026 by *Bridge4Mothers Erasmus+ VET KA210* is licensed under *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

WHAT IS CYBERSECURITY?

Cybersecurity refers to the practices and technologies used to protect computers, mobile devices, networks, and personal information from unauthorized access, attacks, or damage. It helps ensure that your information remains private and secure.

Cybersecurity is part of everyday digital life. Whether you are checking your email, shopping online, or working remotely, following basic security practices reduces the likelihood of becoming a victim of cybercrime. Everyone who uses digital devices has a responsibility to protect their information.

💡 **Tip:** Good cybersecurity starts with simple habits such as updating your software and using strong passwords.

Bridge4Mothers © 2026 by *Bridge4Mothers Erasmus+ VET KA210* is licensed under *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

COMMON CYBER THREATS

Cybercriminals use different methods to steal information or damage devices. Some of the most common threats include phishing emails, malicious software (malware), ransomware, fake websites, identity theft, and password attacks.

Although these threats may seem complicated, many can be avoided by staying alert and following safe online practices. Learning to recognize suspicious messages, websites, and downloads is one of the best ways to protect yourself.

💡 **Tip:** If something online seems unusual or too good to be true, take a moment to verify it before clicking.

Did You Know? Most cyberattacks succeed because users are tricked into taking an unsafe action rather than because of technical weaknesses.

Bridge4Mothers © 2026 by *Bridge4Mothers Erasmus+ VET KA210* is licensed under *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

YOUR FIRST LINE OF DEFENCE

Passwords protect your online accounts from unauthorized access. A strong password should contain at least 12 characters and include a combination of uppercase and lowercase letters, numbers, and special symbols. Avoid using personal information such as birthdays or names.

Each online account should have its own unique password. If one account is compromised, your other accounts will remain protected. A password manager can help you create and securely store strong passwords without having to remember them all.

💡 **Tip:** Use a memorable phrase instead of a single word to create longer and stronger passwords.

⚠️ **Remember:** Never share your passwords with anyone.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

ADDING EXTRA SECURITY

Two-factor authentication, often called **2FA**, provides an additional layer of protection for your online accounts. After entering your password, you must confirm your identity using a second method, such as a code sent to your phone or generated by an authentication app.

Even if someone learns your password, they will usually be unable to access your account without the second verification step. Many email providers, banks, and social media platforms now offer this feature free of charge.

💡 **Tip:** Enable two-factor authentication for your most important accounts, including email, banking, and social media.

Did You Know? Your email account is often the most important account to protect because it can be used to reset passwords for many other services.

Bridge4Mothers ***© 2026 by*** *Bridge4Mothers Erasmus+ VET KA210* ***is licensed under*** *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

BROWSE THE WEB SECURELY

Every day we visit websites to shop, read the news, learn, or communicate with others. Before entering personal information, check that the website uses a secure connection. Secure websites begin with **https://**, and most browsers display a padlock icon next to the web address.

Avoid clicking on suspicious advertisements, pop-up windows, or links from unknown sources. Download software only from trusted websites or official app stores, and always keep your browser updated to benefit from the latest security improvements.

💡 **Tip:** Type important website addresses directly into your browser instead of clicking links received in unexpected emails or messages.

⚠️ **Remember:** A secure website protects your connection, but you should still verify that the website itself is trustworthy.

Bridge4Mothers ***© 2026 by*** *Bridge4Mothers Erasmus+ VET KA210* ***is licensed under*** *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

RECOGNISING PHISHING & ONLINE SCAMS

Phishing is one of the most common online scams. Cybercriminals send fake emails, text messages, or social media messages that appear to come from trusted organisations such as banks, delivery companies, or online stores. Their goal is to trick you into revealing personal information, passwords, or payment details.

Be cautious if a message asks you to act immediately, click a suspicious link, or provide confidential information. Always verify the sender and visit the official website directly instead of clicking links in unexpected messages.

💡 **Tip:** Hover your mouse over a link before clicking to see its real destination.

⚠️ **Remember:** Legitimate organisations will never ask for your password or PIN by email or text message.

Bridge4Mothers © 2026 by *Bridge4Mothers Erasmus+ VET KA210* is licensed under *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

IDENTIFYING FAKE WEBSITES

Some fraudulent websites are designed to look almost identical to legitimate ones. Their purpose is to steal personal information, payment details, or login credentials. Small differences in the website address, poor design, or spelling mistakes are often warning signs that something is not genuine.

Before entering personal information, check that the website address begins with **https://** and displays a padlock icon. Also look for contact information, company details, and customer reviews to help confirm that the website is trustworthy.

💡 **Tip:** Type the website address directly into your browser when visiting important websites such as banks or government services.

⚠️ **Remember:** A professional-looking website is not always a legitimate one.

Bridge4Mothers ***© 2026 by*** *Bridge4Mothers Erasmus+ VET KA210* ***is licensed under*** *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

SAFE ONLINE SHOPPING

Online shopping is convenient, but it is important to buy only from trusted retailers. Before making a purchase, compare prices, read customer reviews, and check the seller's contact information and return policy. Extremely low prices may be a sign of a fraudulent website.

Use secure payment methods whenever possible and avoid making purchases while connected to public Wi-Fi. After completing your purchase, save your confirmation email and regularly review your bank statements for any unfamiliar transactions.

💡 **Tip:** Shop from well-known websites or retailers that have positive customer feedback.

Did You Know? Many credit card providers offer additional protection against fraudulent online purchases.

Bridge4Mothers © 2026 by *Bridge4Mothers Erasmus+ VET KA210* is licensed under *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

ONLINE BANKING SAFETY

Online banking allows you to manage your finances quickly and conveniently. However, because financial information is highly valuable, cybercriminals often target banking customers through fake websites, phishing emails, and fraudulent phone calls.

Always access your bank by typing the official website address into your browser or by using the bank's official mobile application. Never share your PIN, passwords, or verification codes with anyone, even if they claim to work for your bank.

💡 **Tip:** Enable transaction notifications so you are immediately informed about activity on your account.

⚠️ **Remember:** If you notice an unfamiliar transaction, contact your bank immediately.

Bridge4Mothers © 2026 by *Bridge4Mothers Erasmus+ VET KA210* is licensed under *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

MALWARE, VIRUSES AND RANSOMWARE

Malware is harmful software designed to damage devices, steal information, or gain unauthorized access to your computer. Common types include viruses, spyware, trojans, and ransomware. Ransomware encrypts your files and demands payment to restore access.

You can reduce the risk of infection by downloading software only from trusted sources, avoiding suspicious email attachments, and keeping your operating system updated. Reliable antivirus software also provides an additional layer of protection.

💡 **Tip:** Scan downloaded files before opening them, especially if they come from unfamiliar sources.

⚠️ **Remember:** Never pay a ransomware demand, as there is no guarantee your files will be recovered.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

KEEP YOUR DEVICES SECURE

Computers, tablets, and smartphones store large amounts of personal information. Protecting these devices is just as important as protecting your online accounts. Use a strong password, PIN, fingerprint, or facial recognition to prevent unauthorized access.

Enable automatic screen locking and avoid leaving your devices unattended in public places. If your device is lost or stolen, features such as "Find My Device" or remote wipe can help you locate it or erase sensitive information.

💡 **Tip:** Lock your device every time you leave it, even if only for a few minutes.

Did You Know? Modern smartphones automatically encrypt stored data when a secure screen lock is enabled.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

Co-funded by the European Union

KEEP EVERYTHING UP TO DATE

Software developers regularly release updates to improve performance, add new features, and fix security vulnerabilities. Cybercriminals often target outdated software because known weaknesses can be exploited to gain access to devices.

Enable automatic updates for your operating system, web browser, antivirus software, and mobile applications whenever possible. Updating your devices regularly is one of the easiest and most effective ways to improve your cybersecurity.

💡 **Tip:** Restart your device after major updates to ensure all security improvements are installed correctly.

⚠️ **Remember:** Delaying updates may leave your device vulnerable to known security threats.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

STAYING SAFE ON PUBLIC WI-FI

Public Wi-Fi networks are available in cafés, hotels, airports, and shopping centres, but they are generally less secure than private networks. Cybercriminals may monitor unsecured networks or even create fake Wi-Fi hotspots to collect users' personal information.

Avoid logging into online banking, shopping websites, or other sensitive accounts while connected to public Wi-Fi. If you need to access confidential information, consider using your mobile data connection or a Virtual Private Network (VPN).

💡 **Tip:** Disable automatic Wi-Fi connections so your device does not connect to unknown networks without your knowledge.

⚠️ **Remember:** Never assume that free public Wi-Fi is completely secure.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

SECURING YOUR MOBILE DEVICES

Smartphones and tablets contain emails, contacts, photos, banking applications, and personal documents. Because they store so much valuable information, they should be protected just like computers.

Install applications only from official app stores, review app permissions before installation, and remove applications you no longer use. Regularly updating your mobile operating system helps protect your device against newly discovered security risks.

💡 **Tip:** Enable the "Find My Device" feature so you can locate your phone if it is lost.

Did You Know? Many mobile banking applications automatically block access if they detect that a device has been compromised.

Bridge4Mothers ***© 2026 by*** *Bridge4Mothers Erasmus+ VET KA210* ***is licensed under*** *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

MANAGING APP PERMISSIONS

Many applications request permission to access your camera, microphone, contacts, location, or files. While some permissions are necessary for an app to function, others may collect more information than required.

Before installing a new application, review the permissions it requests and consider whether they are appropriate for its purpose. You can also manage permissions later through your device's settings and remove access that is no longer needed.

💡 **Tip:** Periodically review your installed applications and delete those you no longer use.

⚠️ **Remember:** Giving unnecessary permissions may expose more personal information than you intend to share.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

EMAIL SECURITY

Email is one of the most common ways people communicate online, but it is also one of the most common targets for cybercriminals. Suspicious emails may contain harmful attachments, fake links, or requests for personal information. Learning how to recognise these threats helps protect both your personal data and your devices.

Before opening an attachment or clicking a link, make sure you know who sent the email and verify that the message is genuine. If an email seems unusual or unexpected, contact the sender using another method before responding.

💡 **Tip:** Check the sender's full email address, not just the display name.

⚠️ **Remember:** Never open unexpected attachments from unknown senders.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

DOWNLOADING FILES SAFELY

Downloading documents, images, or software is a normal part of using the Internet, but not every file is safe. Files downloaded from untrusted websites or received through suspicious emails may contain malware that can damage your device or steal personal information.

Always download software from official websites or trusted app stores. Before opening downloaded files, scan them with antivirus software if available. If a file or download request seems unexpected, verify that it is legitimate before opening it.

💡 **Tip:** Be cautious of free software offered on unfamiliar websites, especially if it promises premium features at no cost.

⚠️ **Remember:** If you are unsure whether a file is safe, do not open it.

Bridge4Mothers ***© 2026 by*** *Bridge4Mothers Erasmus+ VET KA210* ***is licensed under*** *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

PROTECT YOUR IMPORTANT FILES

Computers and mobile devices can be damaged, lost, or infected with malware. Regular backups ensure that your important files, such as photographs, documents, and personal records, can be recovered if something goes wrong.

You can back up your files to an external hard drive, USB drive, or secure cloud storage service. The best approach is to keep more than one backup and update it regularly so that your latest files are always protected.

💡 **Tip:** Schedule automatic backups whenever possible so you don't have to remember to do them manually.

Did You Know? Many cloud storage services automatically save previous versions of your files, making recovery easier after accidental changes or deletion.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

COOKIES AND WEBSITE TRACKING

When you visit a website, it may store small files called **cookies** on your device. Cookies help websites remember your preferences, keep you logged in, and improve your browsing experience. However, some cookies are also used to collect information about your browsing habits for advertising or analytics.

Most websites allow you to manage your cookie preferences. Reading privacy notices and adjusting cookie settings gives you greater control over how your information is collected and used.

💡 **Tip:** Review cookie settings when visiting new websites instead of accepting all cookies automatically.

Did You Know? Not all cookies are harmful - many are necessary for websites to function correctly.

Bridge4Mothers © 2026 by *Bridge4Mothers Erasmus+ VET KA210* is licensed under *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

ARTIFICIAL INTELLIGENCE (AI) SCAMS AND DEEPFAKES

Artificial intelligence has created many useful tools, but it has also introduced new types of online scams. Criminals can use AI to generate realistic emails, fake voice recordings, or videos that appear to show real people saying or doing things that never happened. These manipulated videos and recordings are known as **deepfakes**.

Be cautious if you receive unexpected phone calls, videos, or messages requesting money or sensitive information. If something seems unusual, verify the request by contacting the person or organisation through an official communication channel.

💡 **Tip:** Trust verified sources rather than relying on videos or recordings shared through social media.

⚠️ **Remember:** Seeing or hearing something online does not always mean it is genuine.

Bridge4Mothers © 2026 by *Bridge4Mothers Erasmus+ VET KA210* is licensed under *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

WHAT TO DO IF YOUR ACCOUNT IS HACKED

If you believe that someone has gained access to one of your online accounts, act immediately. Change your password, enable two-factor authentication if it is not already active, and review your account settings for any unauthorized changes. Inform the service provider if necessary and monitor your account for unusual activity.

If the compromised account is connected to other online services, change those passwords as well, especially if you have reused the same password elsewhere. Acting quickly can reduce the impact of a security breach.

💡 **Tip:** Store recovery information, such as backup email addresses or phone numbers, so you can regain access to your accounts if needed.

⚠️ **Remember:** Using a different password for every account helps prevent one breach from affecting multiple services.

Bridge4Mothers **© 2026 by** *Bridge4Mothers Erasmus+ VET KA210* **is licensed under** *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

UNDERSTANDING IDENTITY THEFT

Identity theft occurs when someone uses your personal information without your permission, often to commit fraud, open financial accounts, or impersonate you online. Stolen information may include your name, identification number, banking details, or login credentials.

Protecting your identity begins with limiting the personal information you share online, using strong passwords, and monitoring your financial accounts regularly. If you suspect identity theft, report it immediately to the relevant authorities and your financial institutions.

💡 **Tip:** Shred documents containing personal information before throwing them away.

Did You Know? Identity theft can occur both online and offline, making careful handling of personal documents equally important.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

SMALL ACTIONS MAKE A BIG DIFFERENCE

Cybersecurity is not achieved through a single action but through consistent daily habits. Lock your devices when you are away, update your software regularly, use strong passwords, verify information before clicking links, and think carefully before sharing personal details online.

Developing these habits helps reduce the risk of cyberattacks and protects both your personal information and the information of others. Over time, these simple actions become routine and make using digital technologies much safer.

💡 **Tip:** Create a monthly checklist to review passwords, updates, backups, and privacy settings.

Bridge4Mothers © 2026 by *Bridge4Mothers Erasmus+ VET KA210* is licensed under *Creative Commons Attribution 4.0 International*

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

CYBERSECURITY AT HOME AND AT WORK

Good cybersecurity practices are important both at home and in the workplace. Whether you are using a personal computer or a company device, you should follow the same principles: protect confidential information, use secure passwords, keep software updated, and report suspicious activity promptly.

If you work remotely, use only trusted devices and secure Internet connections. Respect your organisation's security policies and avoid storing sensitive work information on personal devices unless authorised to do so.

💡 **Tip:** Separate your personal and work accounts whenever possible to reduce security risks.

⚠️ **Remember:** A single careless action can affect not only you but also your family, colleagues, or organisation.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

KEY TAKEAWAYS

Every Internet user plays an important role in protecting personal information and maintaining a safe digital environment. Strong passwords, secure devices, regular updates, careful browsing, and critical thinking are some of the most effective ways to reduce cybersecurity risks.

Make cybersecurity part of your everyday routine by verifying information before acting, protecting your accounts with two-factor authentication, backing up important files, and staying informed about new online threats. Good digital habits not only protect you but also help create a safer online community for everyone.

💡 **Final Tip:** The best defence against cybercrime is a combination of awareness, good habits, and continuous learning.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *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 (EACEA). Neither the European Union nor EACEA can be held responsible for them.*