Cybersecurity hygiene - 5 step checklist

1. Passwords and Logins

Use strong passwords!

• Create a password that is at least 12 characters long and includes a mix of upper- and lowercase letters, numbers, and special characters. For example: StrongPass!2025.

• Use different passwords for different services.

• Enable multi-factor authentication. This makes it much harder for unauthorized individuals to access your account.

• Do not save login information in your web browser, it can be stolen from there.

2. Devices and Software

Good Practices!

• Make sure your devices require a password or code to unlock the screen.

• Update your devices regularly.

• Install and use antivirus software.

• Back up your devices.

3. Social Media

Be cautious on social media:

• Don't share too much personal information and be careful who you accept as friends or followers.

• Got a message from an old friend on Facebook? It might be a scammer who has hijacked their account.

4. Browsing and Networks

Wi-Fi at hotels, in the city, or your favorite café?

• Avoid using public Wi-Fi if possible, but if you must, make sure you have a good VPN installed.

• Beware: scammers can set up fake Wi-Fi networks with names that are almost identical to the real ones.

5. Email and Messages

Be alert, scammers exist!

• Don't click links or images in emails or messages unless you are sure they are safe.

• Don't open attachments from unknown senders.

Cyber security in your everyday life

Cybersecurity is important in our daily lives, especially when using digital devices and services. By following a few simple security measures, we can reduce the risk of someone stealing our information, locking our systems, or scamming us.

Use strong and unique passwords for every account. A strong password includes a mix of lowercase and uppercase letters, numbers, and special characters. Enable multi-factor authentication to increase your security, this means using more than one way to verify your identity, like a password and a code sent to your phone. Avoid saving passwords in your browser. Use a digital password manager or write down your passwords in a notebook stored in a safe place.

Make sure your devices are updated with the latest software and have antivirus programs installed. Change the passwords for your Wi-Fi and router—default passwords should be replaced. If possible, enable a firewall in your router; some providers offer this as an add-on for a monthly fee. This reduces the risk of attacks on connected devices in your home.

Tip: Some municipalities offer IT support for seniors.

Always be cautious with links and attachments in emails and messages. Emails can look real but come from a scammer. This is called phishing—a common trick where scammers pretend to be a trusted source to get your personal information. Always double-check the sender by, for example, hovering your cursor over the address to see if it looks right. Scammers trick people by changing or switching characters in the address.

When using public Wi-Fi networks, use a VPN (Virtual Private Network). A VPN encrypts your internet connection and protects your data from being intercepted by unauthorized individuals—especially important on insecure networks. Often, your antivirus provider offers this type of service.

Cybersecurity is everyone's responsibility, and the more we know, the better we can protect ourselves and each other.

If you suspect that you are a victim of fraud involving, for example, BankID, contact your bank to block the affected bank card. Report it to the police by calling 114 14 or visiting www.polisen.se.

Find more information on earhart.se

Browse safely!

About Hanna Linderstål and Earhart

Security Profile of the Year 2024 & Business Protection Agency

Earhart Business Protection Agency is a Swedish firm specializing in business protection services such as threat and risk assessments, security consultations, crisis exercises, and advisory services for management and boards. They also offer expertise in protection against digital espionage. The agency supports authorities, organizations, and the private sector both in Sweden and internationally. They help organizations comply with EU regulations and emerging market standards.