Cyber hygiene checklist for employees

Thirteen simple habits that protect your organisation every day. Print it, share it, hang it up.

NIS2 Aware · nis2aware.eu · November 2026

Accounts and passwords

- [ ] **Use multi-factor authentication everywhere it is offered**
  Especially for email, remote access and cloud services.
- [ ] **Use a password manager**
  One long, unique password per service.
- [ ] **Never share your password, even with IT**
  IT will never ask for it.

Devices

- [ ] **Install updates promptly**
  On computers, phones, browsers and apps.
- [ ] **Lock your screen when you leave your desk**
  Windows: Windows key + L. Mac: Ctrl + Cmd + Q.
- [ ] **Keep laptops and phones encrypted and protected**
  With a PIN or password and anti-malware.
- [ ] **Don't plug in unknown USB sticks**
  And don't install software yourself without approval.

Email and messages

- [ ] **Check the sender, the links and the urgency**
  When in doubt, don't click.
- [ ] **Confirm payment or bank detail changes by phone**
  Using a number you already know, not the one in the message.
- [ ] **Report suspicious messages to IT**
  Quickly: it protects your colleagues too.

Data and work

- [ ] **Save work files in the company's approved storage**
  So they are backed up.
- [ ] **Be careful on public Wi-Fi**
  Use the company VPN or your phone's connection.
- [ ] **Report a lost device or a mistake immediately**
  Fast reporting limits the damage.

> Test your team with our phishing quiz.

General information on the Belgian NIS2 framework as of November 2026, not legal advice. Always check the latest guidance from the CCB (ccb.belgium.be and atwork.safeonweb.be).