Checklist cyberhygiëne voor medewerkers

Dertien eenvoudige gewoontes die uw organisatie elke dag beschermen. Druk ze af, deel ze, hang ze op.

NIS2 Aware · nis2aware.eu · november 2026

Accounts en wachtwoorden

- [ ] **Gebruik multifactorauthenticatie overal waar het kan**
  Zeker voor e-mail, toegang op afstand en clouddiensten.
- [ ] **Gebruik een wachtwoordbeheerder**
  Een lang, uniek wachtwoord per dienst.
- [ ] **Geef uw wachtwoord nooit door, ook niet aan IT**
  IT zal er nooit om vragen.

Toestellen

- [ ] **Installeer updates snel**
  Op computers, telefoons, browsers en apps.
- [ ] **Vergrendel uw scherm als u uw werkplek verlaat**
  Windows: Windows-toets + L. Mac: Ctrl + Cmd + Q.
- [ ] **Houd laptops en telefoons versleuteld en beveiligd**
  Met een pincode of wachtwoord en antimalware.
- [ ] **Steek geen onbekende usb-sticks in uw computer**
  En installeer zelf geen software zonder toestemming.

E-mails en berichten

- [ ] **Controleer de afzender, de links en de tijdsdruk**
  Bij twijfel: niet klikken.
- [ ] **Bevestig wijzigingen van betalingen of bankgegevens telefonisch**
  Op een nummer dat u al kent, niet op dat uit het bericht.
- [ ] **Meld verdachte berichten aan IT**
  Snel: zo beschermt u ook uw collega's.

Gegevens en werk

- [ ] **Bewaar werkbestanden in de opslag die het bedrijf goedkeurt**
  Zodat er een back-up van wordt gemaakt.
- [ ] **Wees voorzichtig op openbare wifi**
  Gebruik de VPN van het bedrijf of de verbinding van uw telefoon.
- [ ] **Meld een verloren toestel of een fout meteen**
  Snel melden beperkt de schade.

> Test uw team met onze phishingquiz.

Algemene informatie over het Belgische NIS2-kader op datum van november 2026, geen juridisch advies. Raadpleeg altijd de meest recente informatie van het CCB (ccb.belgium.be en atwork.safeonweb.be).