Veilig digitaal werken

Tips voor het voorkomen van cyberincidenten

Een veilige omgeving begint bij jezelf. Met deze goede gewoonten verklein je de kans op datalekken, malware-infecties en andere security- of privacyproblemen.

E-MAIL

- Open geen verdachte bijlagen en klik niet op verdachte links
- Reageer niet op verdachte e-mails
- Verstuur geen zakelijke mails met je privé-account
- Ga nooit in op verzoeken voor bank- en/of creditcardgegevens
- Verstuur nooit persoonsgegevens zonder encryptie en wachtwoordbeveiliging

MOBIEL WERKEN

- Maak enkel gebruik van openbare hotspots met een VPN-verbinding
- Beveilig je smartphone en tablet met een toegangscode
- Heb je een vingerafdrukscanner? Maak er gebruik van!
- Installeer alleen goedgekeurde apps uit de App Store (iOS) of Play Store (Android)

WERKPLEK

- Maak gebruik van schermvergrendeling als je je plek verlaat
- Laat geen persoonsgegevens en wachtwoorden slingeren
- Vreemden op de werkvloer? Vraag naar hun doel en een legitimatiebewijs
- Scherm je webcam af met een sticker, tape of schuifje

SOCIAL MEDIA

- Deel geen bedrijfsgeheimen op social media
- Scherm je openbare profiel zoveel mogelijk af
- Deel nooit persoonsgegevens van anderen zonder toestemming
- Accepteer geen uitnodigingen van vreemden

CLOUD EN APPS

- Gebruik alleen goedgekeurde apps voor bestandsuitwisseling
- Vermijd het gebruik van privé-apps voor werk en vice versa
- Geen centraal updatebeleid? Installeer updates tijdig, ook voor je mobiele device
- Grote bestanden versturen? Vraag de IT-verantwoordelijke naar de procedure

WACHTWOORDEN

- Vermijd makkelijke woorden. Wachtzinnen verdienen de voorkeur
- Veel lastige wachtwoorden? Gebruik een wachtwoordmanager
- Hanteer nooit hetzelfde wachtwoord voor meerdere accounts
- Verander je wachtwoord regelmatig

WEBSITES

- Laat nooit persoonsgegevens achter bij websites zonder groen slotje! (HTTPS)
- Klik nooit op verdachte pop-ups
- Bezoek geen websites met torrents, gokspellen of porno
- Vermijd websites met een beveiligingswaarschuwing

PRINTERS

- Laat afgedankte printers, computers en datadragers altijd opschonen door de IT-verantwoordelijke
- Laat geen uitgeprinte documenten slingeren bij de printer
- Maak indien mogelijk gebruik van een ‘ophaalcode’

MOBIELE DATADRAGERS

- Maak zoveel mogelijk gebruik van versleuteling
- Weet welke data wel en niet mee ‘naar buiten’ mag
- Laat geen usb-sticks, laptops of mobiele schijven slingeren
- Mobiele datadrager gevonden? Lever deze in bij de IT-verantwoordelijke