

...

Checklist

...

1

Wijzig je wifi-wachtwoord regelmatig

Voorkom dat oud-medewerkers of onbevoegden toegang houden. Gebruik aparte netwerken voor gasten en apparaten.

2

Gebruik een wachtwoordmanager (niet die van je browser!)

Browsers slaan wachtwoorden onveilig op. Gebruik een wachtwoordmanager zoals Bitwarden of 1Password voor sterke, unieke wachtwoorden.

3

Beperk admin-rechten

Te veel admins = te veel risico. Geef alleen noodzakelijke accounts beheerders-rechten en gebruik aparte accounts voor dagelijks werk.

4

Maak en test back-ups

Back-ups beschermen tegen dataverlies. Zorg voor automatische en externe back-ups en test regelmatig of je alles kunt terugzetten.

5

Check of je wachtwoorden zijn gelekt

Voer je e-mailadres in op [Have I Been Pwned](#). Gelekt? Wijzig je wachtwoorden en zet MFA aan.

6

Verwijder oude gebruikersaccounts

Voormalige medewerkers en externe partijen mogen geen toegang behouden. Controleer en verwijder onnodige accounts.

7

Update al je software

Beveiligingslekken worden continu misbruikt. Houd besturingssystemen, software, websites en apparaten altijd up-to-date. Denk ook aan je router en printer!

8

Zet Multi-Factor Authenticatie (MFA) aan

Voorkom hacks met MFA. Gebruik een authenticator-app en voorkom sms-verificatie waar mogelijk.

9

Gebruik een zakelijke VPN

Een VPN versleutelt je verbinding, voorkomt dataverlies en beschermt tegen afluisteren. Gebruik alleen betrouwbare zakelijke VPN-oplossingen.

...

Checklist

...

10**Beperk toegangsrechten op bestanden en mailboxen**

Niet iedereen hoeft overal bij te kunnen. Geef alleen toegang waar nodig en controleer dit periodiek.

11**Train medewerkers met nep-phishingmails**

Phishing is de grootste dreiging. Test en train medewerkers regelmatig om verdachte e-mails te herkennen.

12**Monitor je ICT-omgeving**

Wees proactief. Houd verdachte inlogpogingen, netwerkactiviteit en ongebruikelijke opdrachten in de gaten.

13**Scan e-mailbijlagen op virussen**

Voorkom malware via bijlagen. Gebruik e-mailfilters en antivirussoftware die verdachte bestanden direct blokkeert.

14**Versleutel apparaten en opslagmedia**

Laptops, telefoons en usb-sticks bevatten gevoelige data. Zet encryptie aan en voorkom dat gegevens uitlekken.

15**Gebruik Mobile Device Management (MDM)**

Beheer en beveilig zakelijke apparaten op afstand. Met MDM kun je apparaten updaten, toegang beheren en wissen bij verlies of diefstal.