security checklist

Je medewerkers werken veilig vanuit huis. Denk je ook aan de veiligheid van je documenten en data? Zeker nu apparaten vanaf thuisnetwerken toegang hebben tot je bedrijfsnetwerk.

Met deze checklist controleer je zelf al eenvoudig of je al zo veilig mogelijk werkt.

Vind je deze termen lastig en wil je liever samen met ons deze lijst doorlopen?
Bel ons op 085 - 0435 900 of mail naar sales@nm2d.nl.

Bedrijfsnetwerk

- ☐ Je geeft toegang op basis van persoonlijke authenticatie en bijhorende rechten
- ☐ Je hebt de laatste updates geïnstalleerd (bijv. Windows Server)
- ☐ Je geeft medewerkers via een VPN veilig toegang tot je bedrijfsnetwerk
- ☐ Je hebt indien mogelijk multifactor authenticatie geactiveerd voor toegang tot systemen, apps en portals (via SMS of app)
- ☐ Je controleert op openstaande poorten in je firewall
- ☐ Je maakt frequent back-ups van je data, bij voorkeur buiten je eigen netwerk

  Tip: Maak ook back-ups van je bestanden in Office 365! Dit gebeurt niet automatisch.

Laptop, PC en andere mobiele devices

- ☐ Je maakt gebruikt van een anti-virus programma
- ☐ Je maakt indien mogelijk gebruik van multifactor authenticatie (via SMS of app)
- ☐ Je Microsoft Windows, Apple MacOS, Android of iOS is up-to-date
- ☐ Je gebruikt verschillende wachtwoorden voor je apps
- ☐ Je slaat wachtwoorden niet lokaal op (in bijvoorbeeld een Excel-bestand). Gebruik een beveiligde wachtwoord-app zoals 1Password of LastPass
- ☐ Je gebruikt niet automatisch wachtwoorden opslaan
- ☐ Je hebt een wachtwoord ingesteld voor je devices en vergrendelt deze wanneer je wegloopt, ook thuis

Surfen op het internet

- ☐ Je maakt alleen gebruik van bekende en vertrouwde websites
- ☐ Bij gevoelige informatie of inloggen controleer je het internetcertificaat (https linksboven)

hallo, | New Media 2Day

security checklist

Thuisnetwerk en WiFi

- ☐ Je WiFi is afgeschermd met een wachtwoord
- ☐ Je maakt gebruik van je eigen WiFi netwerk
- ☐ Je gebruikt de hotspot van je mobiele telefoon in plaats van een openbaar WiFi
- ☐ Je maakt gebruik van een VPN naar kantoor voor een beveiligde verbinding
- ☐ Je controleert op openstaande poorten in je modem of firewall

E-mail

- ☐ Je controleert URL's die je doorgestuurd krijgt voor je klikt
- ☐ Je gebruikt versleuteling of beveiligde cloud-opslag om gevoelige bestanden te verzenden
- ☐ Je bent op de hoogte van de term 'phishing e-mail'

  Tip: Phishing e-mail speelt vaak in op je angst om iets kwijt te raken of opgelicht te worden. De afzender vraagt je snel te reageren, om je impulsief te laten handelen. De e-mails lijken afkomstig van grote bedrijven, hebben veelal een vreemd afzendadres en bevatten vaak spel- of grammaticafouten. Let op deze kenmerken.

Social Media

- ☐ Denk na voordat je iets plaats of reageert op social media
- ☐ Bedenk goed wie je berichten kunnen en mogen zien
- ☐ Zorg dat foto's geen verborgen informatie bevatten (bijv. gegevens op je beeldscherm)
- ☐ Controleer regelmatig je privacy-instellingen
- ☐ Houd zakelijk en privé gescheiden

Alles gecheckt? We helpen je graag

Ook wij zitten noodgedwongen thuis net als jij. En ook bij ons gaat het werk gewoon door. Onze 80 ICT experts staan klaar voor al je vragen, om te zorgen dat je zo snel en soepel mogelijk veilig door kunt werken én verbonden bent met je hele team.

Laat ons weten hoe wij je kunnen helpen. Bijvoorbeeld met anti-virus voor de laptops van je medewerkers. Back-ups van je Office 365 documenten. Of veilige VPN verbindingen voor je collega's. En natuurlijk voor oplossingen om makkelijk met elkaar te communiceren en samen te werken.

Bel ons op 085 - 0435 900 of mail naar sales@nm2d.nl.