Veilig thuiswerken; zo doe je dat

1. Gebruik van WiFi

Op kantoor is WiFi beveiligd. We gaan er vanuit dat dit bij jou thuis ook het geval is. Hoe check je dat? Lees hier de tips op de website van de Consumentenbond.

Digitale werkomgeving: VMWare Horizon Client

Onze IT-omgeving is ook vanuit huis (of elders) te benaderen via de Horizon Client van VMWare. In eerdere berichten is al aangegeven dat een niet up-to-date versie tot inlogproblemen kan leiden. Zorg dus voor een actuele versie.

Deze digitale werkomgeving is goed beveiligd, dus sla hierbinnen de (persoons)gegevens op waarmee jij werkt. Vanaf elke willekeurige pc, tablet of laptop kun je toegang verkrijgen tot de digitale desktop en is het op je device opslaan van (persoons)gegevens niet nodig. Het is goed mogelijk dat je mensen om je heen hebt die niet bij de provincie Overijssel werken en voor wie de informatie waarmee jij werkt niet is bedoeld. Wees daarom thuis nóg zorgvuldiger met het locken van je scherm als je erachter vandaan gaat.

2. Werken met papier

Zorg ook dat eventuele papieren (aantekeningen, dossiers) niet door anderen kunnen worden ingezien.

Op kantoor hebben we speciale containers voor het verwijderen van papier met vertrouwelijke gegevens. Werk je thuis met uitgeprinte stukken? Bewaar ze dan zorgvuldig. Staan er gevoelige (persoons)gegevens op papieren die je weg wilt gooien? Stop ze dan in een apart tasje, dat je na de periode van thuiswerken kunt legen in de papiercontainers op kantoor.

3. Uitwisselen van gegevens

We wisselen veel gegevens uit, vaak via belletjes, appjes of e-mails. Een datalek voorkomen doe je thuis niet anders dan op kantoor. Voor gegevensuitwisseling met collega's gebruik je e-mail, voor chatten kun je whatsapp gebruiken.

Maak alleen gebruik van video-/beeldbellen wanneer dit noodzakelijk is. Is dat het geval, gebruik daarvoor dan alleen een van de reguliere beeldbelapps: Skype (Microsoft),FaceTime (Apple), Hangouts (Google) , Zoom of Whatsapp (Facebook). Realiseer je bij het gebruik hiervan, dat er nooit vertrouwelijke gegevens, persoonsgegevens, politiek gevoelige of bedrijfskritische informatie gedeeld mag worden via deze apps. Je weet namelijk niet hoe en waar de data van het gesprek wordt opgeslagen (waarschijnlijk buiten Europa) en wie daar mogelijk toegang toe heeft. Voor het juist gebruiken van deze apps ben je uiteindelijk zelf verantwoordelijk.

Aandachtspunten bij het gebruik van zakelijke e-mail

Ga je zakelijke mail sturen die persoonsgegevens of andere vertrouwelijke informatie bevat? Gebruik dan CryptShare. Je kan de e-mail alleen versturen vanuit de Outlook-omgeving die draait op het netwerk van de provincie (CryptShare werkt niet via mailapps of webmail).

Je kunt ook mailen zónder gebruik te maken van de digitale werkomgeving via een app op jouw tablet of smartphone. Zorg er dan voor dat je de gegevens goed beschermt.

- Dat begint met ervoor te zorgen dat de software van het apparaat altijd ‘up-to-date’ is en dat de bescherming tegen virussen is ingesteld (de meeste nieuwe virussen zijn gericht op mobiele apparaten).
- En ben je ook verplicht om een schermvergrendeling in te stellen met een pincode of wachtwoord. Eventueel kun je gebruik maken van biometrie, zoals een vingerafdruk. Gebruik je een pincode, dan is de code 0000 niet toegestaan, evenmin een opeenvolgende op- of aflopende reeks cijfers, zoals bijvoorbeeld 1234 of 7654.
- Beveilig eveneens de SIM-kaart met een zelfgekozen pincode, hiervoor gelden dezelfde regels.

Het is belangrijk je zakelijke e-mailadres te gebruiken voor werkgerelateerde zaken. Dit heeft te maken met beveiliging en privacy. Veel apparaten voegen contactenlijsten van privé en zakelijke e-mailaccounts samen. Let dus goed op of je een e-mailtje wel naar de juiste contactpersoon verstuurt.

4. Corona en phishing

Het coronavirus krijgt wereldwijd veel aandacht en cybercriminelen liften hierop mee. Cyberexperts waarschuwen dan ook voor een toename van phishing aanvallen rond het coronavirus. De e-mails lijken van ziekenhuizen of overheidsinstanties afkomstig en zouden naar eigen zeggen extra informatie of nieuwe richtlijnen over het coronavirus bevatten. De oplichters trekken de aandacht met onderwerpregels als ‘Is het coronavirus in uw stad?’ of ‘Nieuwe veiligheidsmaatregelen tegen coronavirus’. De bedoeling hiervan is nietsvermoedende ontvangers achteloos op links te laten klikken. Bijvoorbeeld door ziektesymptomen op te sommen en door te linken naar een bestand met veiligheidsmaatregelen die de verspreiding van het coronavirus zouden tegengaan. De cybercriminelen verstoppen malware (schadelijke software) achter onschuldige ogende .pdf-, .mp4- of .doc- bestanden. Zo is een vergissing snel gemaakt. Laat je dus niet verleiden door echt lijkende e-mailtjes met ogenschijnlijk originele nep-afbeeldingen of logo’s van bedrijven of organisaties.

Vermoed je een phishingmail te hebben ontvangen? Klik niet op een link, laat nooit je gebruikersnaam en wachtwoord achter op een website (mocht dit gevraagd worden in de e-mail) en open geen bijlages. Heb je toch inloggegevens achtergelaten? Verander dan onmiddellijk je wachtwoord. Meld daarnaast phishing e-mail altijd bij de ICT Servicedesk.