Hoe werk je veilig online thuis?

Op dit moment werken er bijzonder veel mensen thuis. In veel gevallen is dit noodgedwongen door Corona. We ervaren dat het voordelen met zich meebrengt. Toch merken we ook hoe makkelijk en snel het werk op kantoor was. Het is een situatie die voor zowel werknemer als werkgever nieuw is en brengt allerlei zaken met zich mee om rekening te houden. Zeker als het gaat om de veiligheid van het versturen van documenten, de privacy van data en het verwerken van informatie op afstand. Hoe werk je veilig online thuis? In deze blog geven we je hiervoor tips en handvatten voor zowel werkgever als werknemer.

Dreigingen tijdens het online thuiswerken

Criminelen gebruiken deze tijd om rond het nieuws van COVID-19 hun activiteiten te plannen. Mensen worden al overspoeld met informatie en nieuws en dat is waar de crimineel toeslaat. Denk aan phishingmails en SMS berichten met foute links. Nu er massaal thuisgewerkt wordt op eigen apparatuur (die niet altijd up-to-date blijkt te zijn) is een crimineel zo binnen via een phishingmail.

Dus:

- Ga voorzichtig om met vreemde, rare of onbekende mailtjes. Is de verzender onbekend? Denk dan zeker goed na of deze mail echt is. Is het een bekende verzender maar wordt er getwijfeld aan de echtheid van het bericht? Neem dan contact op met de verzender. Doe dat het liefst via een kanaal dat je kent. Bijvoorbeeld het mobiele nummer of zoek het op via de website van de verzender.
- Een vreemd bericht ontvangen met een bijlage? Bedenk dan of je deze bijlage had verwacht. Twijfel? Ook nu contact opnemen. Wil je de bijlage toch openen maar eerst controleren? Via https://checkjelinkje.nl kun je veilig een bijlage laten scannen op malware. Handig!
- Het versturen van vertrouwelijk data (denk aan persoonsgegevens, gevoelige bedrijfsinformatie, etc.) zou eigenlijk niet via mail moeten. Veel organisaties bieden een veilige “verzend-ontvang oplossing” in plaats van mail. Informeer of deze er is binnen jou organisatie. Dit kan bijvoorbeeld cryptoshare zijn, een Microsoft Sharepoint omgeving of een ander manier van delen. Moet het toch via de mail? Zorg dat je het bestand dat je wilt versturen versleutelt met een wachtwoord en stuur dit wachtwoord bij voorkeur via een SMS naar de ontvanger.

Apparatuur en programma’s

Ik noemde net al even het veilig versturen van bestanden dat misschien lastiger is geworden nu we thuis werken. Maar ook het thuiswerken zelf heeft veel uitdagingen met zich meegebracht. De ene organisatie biedt wel een laptop aan om thuis te kunnen werken, de andere niet. In het ene geval mag je wel online toepassingen gebruiken om snel data te versturen in het andere niet. En hoe zit het nu met al die videochat programma’s.

Ook hier een paar tips:

- De belangrijkste denk ik: zorg dat je alleen programma's gebruikt die je van je organisatie mag gebruiken. Vraag er naar als je het niet precies weet. Een fout is zo gemaakt en voor je het weet is er een datalek.
- Voor de werkgever: beschrijf wat je mag gebruiken. Het liefst in voorbeelden. Dus: je wilt videobellen. Hiervoor gebruiken we ….. Leg kort uit hoe het geïnstalleerd moet worden of waar het bestand gevonden kan worden. Dat maakt thuiswerken echt een stuk makkelijker.
- Werknemers: lees het stuk dat je werkgever gemaakt heeft. Zo weet je precies wat je wel en niet kunt gebruiken.
- Gebruik nooit privé-accounts om gegevens te delen. Daarvoor is het niet bedoeld en kan leiden tot een datalek of veiligheidslek.
- Videobellen: er zijn enorm veel applicaties. Welke je gebruikt is afhankelijk van je wensen: hoeveel mensen in de chat, wel of niet scherm delen, bestandoverdracht, etc. Wat je in je achterhoofd moet houden: bespreek nooit persoonsgegevens in een openbare chat. Meeluisteren is zo gedaan en ook nu kan dat voor vervelende situaties zorgen. Weet ook wie er in de chat mogen zitten. Vreemde gebruiker? Dan niet verder en meldt dit. Maak ook niet zomaar opnames. Vraag dit van te voren. Het is echt heel eenvoudig en je kunt het nazien maar niet iedereen vindt het fijn als ze opeens op Youtube staan of iets dergelijk. Als het mogelijk is: maak een pincode aan en stuur deze in een apart mailtje aan de deelnemers.

Een samenvatting van tips om veilig online thuis te werken:

- Update je software. Dit geldt voor alle apparatuur waar je op werkt. Je laptop, pc, je telefoon én tablet. Software die up-to-date is, is veiliger en minder interessant voor een crimineel.
- Zorg dat je je virusscanner (of malware scannner, zo worden ze ook genoemd) up-to-date houdt. Zo blijven vervelende virussen buiten je thuiswerkplek.
- Je wifi-netwerk (en dit geldt ook voor niet thuiswerkers): zorg dat je een goed wachtwoord op je netwerk hebt. Deel je wifi niet zomaar met iedereen en zeker nu niet tijdens het thuiswerken. Iemand op je netwerk kan zomaar meekijken met wat je stuurt en doet. En dat is niet handig.
- Deel je bedrijfsapparatuur niet met je vrienden of familie. Laat je kinderen bijvoorbeeld geen spelletjes spelen terwijl je persoonsgegevens van een klant verwerkt op de laptop van je werk.
- Vergrendel ook thuis je werkplek. Ga je even koffie halen? Prima. Zet nu ook je scherm op slot. Dit zorgt ervoor dat er niemand meekijkt of dat opeens de kat je Word-document verwoest (die je net niet bleek te hebben opgeslagen).
- Let ook op hoe je thuis werkt. Wanneer je gevoelig informatie verwerkt bijvoorbeeld, zou je niet met je scherm naar het raam moeten zitten waar iedereen die langsloopt mee kan kijken.
- Verder: bespreek niet alle bedrijfsgevoelig of persoonsgevoelig informatie thuis. Denk aan wie er mee kan luisteren. Met het mooie weer de deur open is heel fijn maar een telefoongesprek voeren over een collega of klant terwijl je buurman meeluistert is niet veilig.

- Zet ook geen foto’s online van je werkplek. Mensen vinden het leuk om te laten zien hoe ze thuiswerken en dat is begrijpelijk. Echter, een foto van een scherm met een bedrijfsdata kan weer leiden tot een datalek. Hetzelfde geldt voor papieren documenten of een geeltje met een wachtwoord. Niet doen dus.

Kortom

Werk veilig, denk goed na wat je deelt en met wie en bij vragen neem je contact op met degene die over het werkplekbeheer gaat. Liever een keer te veel dan te weinig. Daarnaast geeft onze partner Den Ouden Informatiebeveiliging trainingen en webinars over hoe je veilig thuis kunt werken. Neem gerust contact met ons op: info@thuiswerkengoedgeregeld.nl