#

**Top 5 stappen om veilig thuis te werken**

We begrijpen dat werken vanuit huis voor sommigen van jullie nieuw is en dat het aanpassen aan de nieuwe situatie misschien zelfs overweldigend kan voelen. Een van onze doelen is ervoor te zorgen dat jullie zo veilig mogelijk kunnen thuiswerken. Hieronder vind je vijf eenvoudige stappen om veilig te werken. Het mooiste van alles is dat deze stappen niet alleen helpen om je werk te beveiligen, maar dat ze ook helpen om je huis cyberveilig te maken voor jou en je familie.



**Jijzelf**: Als allereerste, technologie alleen kan je niet volledig beschermen. Jijzelf bent de beste verdediging. Aanvallers hebben geleerd dat de makkelijkste manier om te krijgen wat ze willen is jou tot hun doelwit te maken, in plaats van de computers of andere apparaten. Als ze je wachtwoord, werkgegevens of controle over je computer willen, dan zullen ze proberen om jou te misleiden zodat je deze informatie geeft, vaak door een gevoel van urgentie te creëren. Zo kunnen ze bijvoorbeeld opbellen en zeggen dat ze de technische dienst van Microsoft zijn en beweren dat je computer besmet is. Of misschien sturen ze je een e-mail waarin ze waarschuwen dat een pakketje niet afgeleverd kon worden, om je zo te verleiden om op een schadelijke link te klikken. De meest voorkomende aanwijzingen van een mogelijke social engineering-aanval:

* **Iemand creëert een enorm gevoel van urgentie, vaak door angst, intimidatie, een crisis of een belangrijke deadline. Cyberaanvallers zijn goed in het maken van overtuigende berichten die lijken te komen van betrouwbare organisaties, zoals banken, de overheid of internationale organisaties.**
* Druk om veiligheidsregels of -procedures te omzeilen of negeren, of een aanbod dat te mooi lijkt om waar te zijn (nee, je hebt de staatsloterij echt niet gewonnen!)
* Het bericht lijkt afkomstig te zijn van een vriend of collega, maar de handtekening, toon van het bericht of het woordgebruik is anders.

Uiteindelijk ben jij de beste bescherming tegen aanvallen.

**Thuisnetwerk**: bijna elk thuisnetwerk begint met een draadloos netwerk (ook wel wifi genoemd). Hiermee maken je apparaten een draadloze verbinding met het internet. De meeste thuisnetwerken worden bestuurd door je internetrouter of een apart, toegewijd draadloos toegangspunt. Beide werken op dezelfde manier: ze zenden draadloze signalen uit waar andere apparaten verbinding mee kunnen maken. Dit betekent dat het beveiligen van je draadloze netwerk een essentieel onderdeel is van het beveiligen van je huis. We raden de volgende stappen aan ter beveiliging:

* Verander het standaard beheerderswachtwoord van het apparaat dat je draadloze netwerk bestuurt. Met het beheerdersaccount kun je de instellingen voor je draadloze netwerk aanpassen.
* Zorg ervoor dat alleen mensen die je vertrouwt verbinding kunnen maken met je draadloze netwerk. Dit bereik je door een sterke beveiliging in te schakelen. Hierdoor moeten mensen een wachtwoord gebruiken om in te loggen op je draadloze netwerk en wanneer ze zijn verbonden, worden hun online-activiteiten versleuteld.
* Zorg ervoor dat het wachtwoord dat mensen gebruiken om verbinding te maken met jouw draadloze netwerk een sterk wachtwoord is, dat anders is dan het beheerderswachtwoord. Onthoud dat je voor ieder apparaat het wachtwoord maar één keer hoeft in te vullen, omdat deze het vervolgens opslaat en onthoudt.

Weet je niet zeker hoe je deze stappen moet uitvoeren? Vraag het je internetprovider, kijk op hun website, sla de documentatie erop na die werd meegeleverd met je draadloze toegangspunt of kijk op de website van de verkoper/fabrikant.



**Wachtwoorden**: wanneer een website je vraagt om een wachtwoord aan te maken, maak dan een sterk wachtwoord aan: hoe meer tekens, hoe sterker het is. Het maken van een wachtwoordzin is een eenvoudige manier om ervoor te zorgen dat uw wachtwoord sterk is. Een wachtwoordzin is niets anders dan een wachtwoord dat bestaat uit meerdere woorden, zoals “bij honing whiskey”. Een unieke wachtwoordzin betekent een ander wachtwoord voor iedere apparaat of online account. Mocht één wachtwoordzin achterhaald worden, dan zijn zo je andere accounts en apparaten nog steeds veilig. Kun je al die wachtwoordzinnen niet onthouden?

Gebruik dan een wachtwoordmanager, een speciaal programma dat al je wachtwoordzinnen veilig op versleutelde wijze opslaat (en vaak nog meer handige functies heeft!). Schakel twee-staps-verificatie in (ook wel twee-factor- of multifactor-authenticatie genoemd) als dit kan. Dit gebruikt je wachtwoord, maar voegt ook een tweede stap toe, zoals een code die naar je smartphone wordt gestuurd of een app die een dergelijke code aanmaakt. Twee-staps-verificatie is waarschijnlijk de belangrijkste stap die je kunt nemen om je online accounts te beschermen en het is veel gemakkelijker dat je denkt.

**Updates**: zorg ervoor dat al je computers, mobiele apparaten, programma's en apps de nieuwste versie van hun software gebruiken. Cyberaanvallers zijn constant op zoek naar nieuwe zwakke plekken in de software die je apparaat gebruikt. Wanneer ze zo'n zwakke plek ontdekken, gebruiken ze speciale programma's om hier misbruik van te maken en zo in te breken in je apparaten. Ondertussen zijn de bedrijven die deze software maken hard bezig om deze zwakke plekken te verhelpen door updates uit te brengen. Door ervoor te zorgen dat jouw computers en apparaten deze updates meteen installeren, maak je het veel lastiger voor iemand om je te hacken. Om up-to-date te blijven, hoef je alleen maar automatisch updaten in te schakelen. Deze regel geldt voor bijna elke technologie die is verbonden met een netwerk, dus niet alleen de apparaten van het werk maar ook met internet verbonden tv's, babyfoons, beveiligingscamera's, routers, spelconsoles en zelfs je auto.



**Kinderen/gasten**: iets waar je je waarschijnlijk op kantoor nooit druk over hoeft te maken, is of kinderen, gasten of andere familieleden gebruik maken van je werklaptop of andere werkapparatuur. Zorg ervoor dat familie en vrienden begrijpen dat ze je werkapparaten niet mogen gebruiken, omdat ze dan mogelijk per ongeluk informatie kunnen wissen of veranderen, of nog erger: misschien per ongeluk het apparaat besmetten.