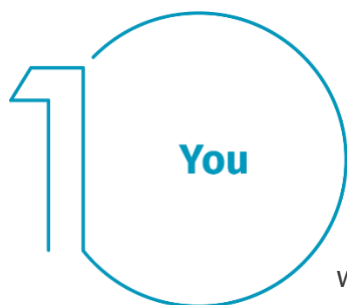


5 belangrijke stappen om veilig van thuis uit te werken

We begrijpen dat van thuis uit werken voor sommigen onder jullie nieuw is en dat je aanpassen aan de nieuwe situatie misschien 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 is dat deze stappen niet alleen helpen om je werk te beveiligen, maar ook om je woning 'cyberveilig' te maken voor jou en je gezin.



Jijzelf: technologie alleen kan je om te beginnen niet volledig beschermen. Jijzelf bent de beste verdediging. Aanvallers hebben geleerd dat de makkelijkste manier om te krijgen wat ze willen, jou tot hun doelwit maken is, in plaats van je computer of andere apparaten. Als ze je wachtwoord, werkgegevens of controle over je computer

willen, dan zullen ze proberen je te misleiden zodat je deze informatie geeft, vaak door een gevoel van urgentie te creëren. Ze kunnen zich bijvoorbeeld voordoen als de technische dienst van Microsoft, je opbellen en beweren dat je computer besmet is. Of ze kunnen je een mail sturen met de melding dat een pakketje niet afgeleverd kon worden, zodat je op een schadelijke link zou klikken. Dit zijn de courantste aanwijzingen van een mogelijke social-engineeringaanval:

- Iemand creëert een gevoel van hoogdringendheid, vaak door middel van angst, intimidatie, een crisis of een belangrijke deadline. Cyberaanvallers zijn goed in het maken van overtuigende berichten die van betrouwbare organisaties lijken te komen, zoals banken, de overheid of internationale organisaties.
- Druk om veiligheidsregels of -procedures te omzeilen of te negeren, of een aanbod dat te mooi lijkt om waar te zijn (nee, je hebt de loterij echt niet gewonnen!)

- Een bericht van een vriend of collega, waarbij de handtekening, de gebruikte woorden of de toon vreemd aanvoelen.

Uiteindelijk ben je zelf de beste bescherming tegen deze aanvallen.

2 Home Network

Thuisnetwerk: bijna elk thuisnetwerk begint met een draadloos netwerk (ook wel wifi genoemd). Hierdoor kunnen je apparaten verbinding maken met het internet. De meeste thuisnetwerken worden bestuurd door je internetrouter of een specifiek draadloos toegangspunt. Beide werken op dezelfde manier: ze zenden draadloze signalen uit waarmee andere apparaten verbinding kunnen maken. Dat betekent dat je draadloze netwerk beveiligen een essentieel onderdeel is van het beveiligen van je woning. We raden de volgende stappen aan:

- Verander het standaardwachtwoord van het apparaat dat je draadloze netwerk bestuurt. Via de beheerdersaccount kun je de instellingen van 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 verbonden zijn, worden hun onlineactiviteiten versleuteld.
- Zorg voor een sterk wachtwoord om verbinding te maken met je draadloze netwerk. Het moet bovendien verschillen van het beheerderswachtwoord. Onthoud dat je voor ieder apparaat het wachtwoord maar één keer hoeft in te geven, omdat het vervolgens wordt opgeslagen en onthouden.

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



3 Passwords

Wachtwoorden: wanneer een website je vraagt om een wachtwoord aan te maken, creëer dan een sterk wachtwoord: hoe meer tekens, hoe sterker. Een wachtzin gebruiken is een eenvoudige manier om ervoor te zorgen dat je wachtwoord sterk is. Een wachtwoordzin is niets anders dan een wachtwoord dat bestaat uit meerdere woorden, zoals '*bij honing whisky.*' Een unieke wachtwoordzin betekent een ander wachtwoord voor ieder apparaat en elke onlineaccount. Zo blijven je andere accounts veilig als een van je accounts wordt gehackt. Kun je al die wachtwoorden niet onthouden?

Gebruik dan een wachtwoordmanager, een speciaal programma dat al je wachtwoordzinnen veilig en versleuteld opslaat (en vaak nog meer handige functies heeft!). Schakel tweestapsverificatie in (ook wel tweefactor- of multifactor-authenticatie genoemd) als dat 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.

Tweestapsverificatie is waarschijnlijk de belangrijkste stap die je kunt nemen om je onlineaccounts te beschermen. Het is bovendien veel makkelijker dan je denkt.



4 Updates

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 er misbruik van te maken en in te breken in je apparaten. Ondertussen zijn de bedrijven die deze software maken, hard bezig om de zwakke plekken weg te werken door updates uit te brengen. Door ervoor te zorgen dat je 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 de functie 'automatisch updaten' in te schakelen. Die regel geldt voor bijna elke technologie die is verbonden met een netwerk: niet alleen apparaten van het werk, maar ook met het internet verbonden tv's, babyfoons, beveiligingscamera's, routers, spelconsoles en zelfs je auto.



Kinderen/gasten: waar je je op kantoor waarschijnlijk nooit druk over hoeft te maken, is of er kinderen, gasten of andere familieleden gebruikmaken van je werklaptop of andere werkapparatuur. Zorg dat familie en vrienden begrijpen dat ze je werkapparaten niet mogen gebruiken. Ze kunnen immers per ongeluk informatie wissen, veranderen of erger nog: het apparaat besmetten.