Tips & adviezen

Volg deze tips en adviezen op voor goede online veiligheid. Dit onderdeel is ontwikkeld in samenwerking met Get Safe Online (VK) en het Department of Homeland Security (departement Binnenlandse veiligheid) van de VS.

- Bescherm uw pc en draagbare apparaten
- Bescherm uw persoonsgegevens en uw identiteit
- Bescherm bedrijfsinformatie buiten uw organisatie
- Wees voorzichtig met internetverbindingen
- Wees webwijs

Bescherm uw pc en draagbare apparaten

pc

- Gebruik een firewall: firewalls beschermen uw netwerk tegen virussen en hackers.
- Installeer antivirussoftware: antivirussoftware voorkomt virusinfecties op uw computer.
- Installeer de meest recente beveiligingsupdates: houd uw toepassingen en besturingssysteem in een goede conditie en up-to-date.
- Geef spyware geen kans: wis verdachte e-mails en aangehechte bestanden, zodat vreemden geen toegang kunnen krijgen tot uw computer.
- Maak geregeld back-ups: bescherm uw gegevens tegen calamiteiten.

Laptops

- Schakel draadloze verbindingen uit wanneer u ze niet meer gebruikt of nodig hebt.
- Zoek vanaf uw laptop verbinding met een vertrouwd netwerk en werk regelmatig uw beveiligingsmechanismen bij.
- Zorg voor regelmatige back-ups van de informatie op uw laptop.
- Laat uw laptop niet onbeheerd achter.

USB-sticks

- Gebruik een versleutelde USB-stick.
- Zet de USB-geheugenstick met de fysieke schakelaar in de read-only-modus om de verspreiding van virussen te voorkomen: sommige USB-sticks zijn voorzien van een fysieke schakelaar om de stick in read-only-modus te zetten, zodat de hostcomputer niet ongewild gegevens op de stick kan schrijven noch ongewild gegevens op de stick kan wijzigen.
- Scan de USB-stick op virussen nadat u bestanden hebt gekopieerd vanaf een niet-vertrouwd en/of niet-geautoriseerd apparaat.

- Verwijder alle bestanden die u op dat moment niet nodig hebt, van uw USB-stick voordat u deze op de computer van iemand anders gebruikt.
- Maak regelmatig back-ups van de informatie op uw USB-stick voor het geval er zich een calamiteit voordoet.
- Doordat USB-sticks zo klein zijn, raakt u ze gemakkelijk kwijt en worden ze eerder gestolen. Hang de stick daarom aan een keycord. Verder heeft de hogere opslagcapaciteit tot gevolg dat meer gegevens blootstaan aan potentiële ongeautoriseerde toegang. USB-sticks worden vaak in tassen, rugzakken, laptopkoffers, jas- en broekzakken gestopt, of worden in onbeheerde werkstations achtergelaten. Het aantal incidenten waarbij USB-sticks zoekraken, zonder toestemming worden geleend of worden gestolen, neemt snel toe.

Mobiele telefoons en smartphones

Smartphones als Windows Mobile, Palm, iPhone, Android en Blackberry zijn voorzien van internettoegang en de mogelijkheid er grote hoeveelheden informatie op te bewaren. Het feit dat ze eenvoudig kunnen worden meegenomen, brengt met zich mee dat er zeer voorzichtig mee moet worden omgesprongen.

- Schakel draadloze verbindingen (zoals Bluetooth en WLAN) uit als u ze niet gebruikt. Bluetooth-technologie houdt in dat elektronische apparaten via radioverbindingen over korte afstanden met elkaar kunnen communiceren.
- Laat uw mobiele telefoon en zakcomputer niet onbeheerd achter. Doet u dat wel, dan kunt u gegevens kwijtraken.
- Gebruik de wachtwoordfunctie om te voorkomen dat iemand op afstand inbreekt in uw smartphone.

Bescherm uw persoonsgegevens en uw identiteit

- **Gebruik een sterk wachtwoord**: uw wachtwoord heeft voor internet dezelfde functie als het slot en de sleutel voor uw huis. Wachtwoorden bieden belangrijke bescherming. Door goede wachtwoordpraktijken te ontwikkelen draagt u ertoe bij dat uw gevoelige persoonsgegevens en identiteit beter beveiligd zijn. Het wachtwoord van uw computer is de sleutel tot alle informatie — zowel bedrijfs- als persoonlijke gegevens — die u op uw computer en in online accounts hebt opgeslagen. Gebruik een sterk wachtwoord om uw gegevens te beschermen; dit is een wachtwoord dat bestaat uit een complexe reeks tekens, waarin letters (in hoofdletters en kleine letters), cijfers en symbolen met elkaar zijn gecombineerd. Hoe gevarieerder de tekens die u gebruikt, hoe moeilijker uw wachtwoord te raden is. Gebruik geen persoonsgegevens — naam, naam van uw kind, geboortedata, enz. — die gemakkelijk te achterhalen zijn en probeer algemene woorden te voorkomen; sommige hackers maken gebruik van programma's die alle woorden uit het woordenboek proberen.

- **Wijzig uw wachtwoord regelmatig**: als u vermoedt dat uw systeem is gehackt, dient u direct uw wachtwoord te wijzigen.
- **Houd uw wachtwoord geheim**: uw wachtwoord is uniek en mag aan niemand worden toevertrouwd. Probeer als het even kan uw wachtwoorden te memoriseren volgens een bepaalde strategie. Wilt u uw wachtwoorden toch opschrijven, bewaar ze dan op een veilige plek. Bewaar de wachtwoorden niet op een plek waar u ook niet de informatie die ze beschermen, zou bewaren.
- **Uniek account, uniek wachtwoord**: gebruik verschillende wachtwoorden voor elk online account waar u toegang toe hebt (of werk in elk geval met een aantal verschillende wachtwoorden). Als u hetzelfde wachtwoord gebruikt voor meerdere accounts, zal een hacker die toegang heeft verkregen tot één account ook toegang kunnen krijgen tot al uw andere accounts.
- **Beveilig uw accounts**: veel verstrekkers van accounts bieden extra mogelijkheden om te controleren wie u bent, voordat u zaken gaat doen op de desbetreffende site.
- **Houd de regie over uw online aanwezigheid**: stel indien mogelijk de privacy- en beveiligingsinstellingen op websites in op het niveau van gegevensuitwisseling dat u prettig vindt. Het verdient de voorkeur het aantal mensen met wie u informatie uitwisselt, beperkt te houden.
- **Wees voorzichtig met het gebruik van sociale-netwerksites**: wees u ervan bewust dat sociale-netwerksites veel van de risico's van online aanwezigheid in zich verenigen: online pesten, openbaarmaking van privégegevens, cyberstalking, toegang tot content die niet geschikt is voor de leeftijd en in extreme gevallen zelfs online grooming en kindermisbruik.

Bescherm bedrijfsinformatie buiten uw organisatie

- **Zorg ervoor dat u gevoelige informatie veilig bewaart**: als u zich buiten uw organisatie bevindt, dient u gevoelige informatie en apparatuur te allen tijde veilig te bewaren ter voorkoming van verlies of diefstal. Met name als u zich in openbare ruimten bevindt, moet u zorgvuldig met informatie omspringen.
- **Behandel bedrijfsinformatie vertrouwelijk:** wees u ervan bewust dat iemand uw gesprek kan horen. Stel vertrouwelijke informatie van uw bedrijf niet aan iedereen ter beschikking.
- **Wees alert op 'shoulder surfing'**: let op dat mensen niet over uw schouder meekijken wanneer u reist of op afstand werkt.
- **Ga verstandig om met webmail**: met het gebruik van een internetbrowser voor het lezen van uw mail moet u net zo voorzichtig omspringen als met een desktopmailsysteem en u moet attent zijn op nog een aantal extra veiligheidsrisico's.

Wees voorzichtig met internetverbindingen

- **Schakel draadloze verbindingen uit wanneer u ze niet meer gebruikt of nodig hebt.**

- **Ga verstandig om met wifi-hotspots**: wanneer u wifi-hotspots gebruikt, beperk dan de soorten werk die u verricht en pas de beveiligingsinstellingen op uw apparaat aan om de toegang tot uw computer in te perken.
- **Bescherm uw geld**: wanneer u online bankiert en winkelt, controleer dan eerst of de desbetreffende site beveiligd is. Dit kunt u zien aan het internetadres: wordt dit voorafgegaan door https:// of shttp://, dan betekent dat dat de site extra maatregelen neemt om uw gegevens te beveiligen. Bij http:// is dat niet het geval.
- **Stop ongewenste e-mail**: spam vormt een bedreiging voor de beveiliging. Open geen onbekende e-mails en aanhangsels.
- **Bij twijfel: weg ermee!**: als links in e-mails, tweets, posts en online advertenties er verdacht uitzien, is het het beste om ze, zelfs als u weet waar ze vandaan komen, te wissen, of ze, indien van toepassing, als junkmail te markeren.
- **Stuur e-mail alleen door voor zover dat passend is**: overweeg om de voorafgaande e-mailwisseling te wissen voordat u het bericht doorstuurt.
- **Wees voorzichtig met surfen op internet.**
- **Download geen documenten en materiaal van niet-vertrouwde partijen.**
- **Ga voorzichtig om met het gebruik van publiek toegankelijke computers:** maak alleen gebruik van internettoegang op publiek toegankelijke computers als u een versleutelde verbinding hebt (aangegeven met een hangslot in de rechterbenedenhoek van uw browservenster en met de letters 'https://' aan het begin van het internetadres).
- **Gebruik webmaildiensten van goed bekendstaande en vertrouwde bedrijven.**

Wees webwijs

- **Blijf op de hoogte:** houd bij welke nieuwe manieren er zijn om veilig online te zijn. Kijk op vertrouwde websites voor de meest recente informatie, deel deze met familie, vrienden en collega's en moedig hen ook aan om webwijs te worden. Zorg ervoor dat uw browser veilig is.
- **Denk na alvorens te handelen**: wees voorzichtig met berichten die u ertoe aanzetten direct te handelen, die iets aanbieden dat te mooi is om waar te zijn of die om persoonsgegevens vragen.
- **Maak back-ups**: bescherm uw werk, muziek, foto's en andere digitale informatie door een elektronische kopie te maken en deze veilig op te slaan.