Uw digitale veiligheid





Dreiging vanuit statelijke actoren

Statelijke actoren (buitenlandse inlichtingendiensten) hebben de tijd, middelen en capaciteiten om geavanceerde cyberaanvallen uit te voeren. Zij gaan veelal heimelijk te werk waardoor een cyberaanval lastig te detecteren is. Als de basismaatregelen worden nageleefd, kunnen zij nog steeds succesvol zijn. Wees u hiervan bewust. Statelijke actoren hebben het doel om geopolitiek voordeel te halen uit de door hen (heimelijk) verkregen informatie.



Dreiging vanuit criminelen en criminele organisaties

Cybercriminelen beschikken over de kennis en hebben de financiële middelen om (geavanceerde) cyberaanvallen uit te voeren. Als de basismaatregelen worden nageleefd, zullen zij minder snel succesvol zijn. Hun acties kunnen maatschappelijk ontwrichtend zijn en hebben het doel geld te verdienen. Hoe belangrijker de verkregen informatie of de getroffen instantie, des te meer zij kunnen verdienen.



Dreiging vanuit overige kwaadwillenden (zonder statelijke steun)

Kwaadwillenden kunnen toevallig of gericht aan informatie komen die niet voor hen bedoeld is. Doordat hackmiddelen toegankelijk zijn, is specialistische kennis niet noodzakelijk. Als de basismaatregelen worden nageleefd, zullen zij niet snel succesvol zijn. Ook met laagdrempelige middelen kunnen kwaadwillenden grote impact hebben.

De steeds verdere digitalisering van onze samenleving brengt naast vele gebruiksgemakken en talloze mogelijkheden ook risico's met zich mee. Als gebruiker wilt u maximaal gebruik maken van alle functionaliteiten van uw mobiele apparatuur. Helaas gaan (sommige) van deze functionaliteiten soms ten koste van uw digitale veiligheid.

Deze brochure beschrijft de maatregelen die u kunt nemen om uw persoonlijke apparaten en informatie beter te beveiligen. Zo kunt u de kans verkleinen om slachtoffer te worden van een digitale aanval.

Deze brochure is opgesteld door de AIVD, BVA-Rijk, CIO-Rijk, de MIVD, het NCSC en de NCTV.

Algemeen



1. Gebruik voor elk account een uniek wachtwoord. Gebruik een sterk wachtwoord van minimaal 16 karakters. Een gerenommeerde passwordmanager is een handige manier om wachtwoorden te genereren en veilig op te slaan.



2. Schakel waar mogelijk *Multifactor Authenticatie* (MFA) in. Gebruik bij voorkeur geen MFA via sms. Kies liever voor een authenticatie-app of e-mail.



3. Controleer of contactgegevens van uw contacten nog correct en nog in gebruik zijn als u langere tijd geen contact heeft gehad. Verifieer dat het liefst via een ander communicatiemiddel.



4. Wees bedacht op risico's als *social engineering* en *phishing*.



5. Open niet zomaar vreemde bestanden of bestanden van onbekenden. Klik niet zomaar op toegezonden links.

6. Vraag bij twijfel of als u vermoedt slachtoffer te zijn van een digitale aanval om advies bij uw Beveiligingsautoriteit (BVA) en/ of uw Chief Information Security Officer (CISO).

Software en apps



7. Wees terughoudend met het installeren van apps. Installeer alleen apps uit vertrouwde bronnen (App stores).



8. Kies een chat-app die standaard *end-to-end* versleuteling toepast en activeer de optie (her)registratie via PIN of MFA.



9. (Her)overweeg of de app-machtigingen, zoals toegang tot locatiegegevens, daadwerkelijk nodig zijn voor het gebruik van de app.



10. Zorg dat uw software (apps en besturingssysteem) altijd up-to-date is en schakel automatisch updaten in.



11. Klik veiligheidswaarschuwingen en meldingen niet zonder meer weg, maar doe er iets mee.



12. Verstuur geen foutrapporten, gebruiksstatistieken en dergelijke aan de fabrikant. Schakel waar mogelijk deze opties uit.

Mobiele apparatuur



13. Voer geen staatsgeheime gesprekken via uw mobiele apparatuur.



14. Voer geen gesprekken over staatsgeheime of bedrijfsvertrouwelijke informatie met mobiele apparaten in dezelfde ruimte. Apparaten uitschakelen is niet genoeg. Het biedt geen garantie dat via het apparaat niet wordt meegeluisterd.



15. Schakel Bluetooth, wifi en locatie-voorziening standaard uit als u deze niet gebruikt.



16. Verwijder (niet relevante) wifi-netwerken die op uw mobiele apparaten zijn opgeslagen.



17. Stel een vergrendeling in op uw mobiele apparaten. Ontgrendel uw apparaat met een wachtwoord of biometrie (vingerafdruk of gezichtsherkenning).



18. Herstart uw mobiele apparatuur dagelijks en gebruik alleen een door de fabrikant verstrekte oplader en oplaadkabel.

Onderweg en op reis



19. Neem uw mobiele apparaten niet mee naar reisbestemmingen met een verhoogd risico op digitale spionage.



20. Brengt u een bezoek aan een land met een verhoogd risico op digitale spionage en is het nodig dat u bereikbaar bent? Kies voor tijdelijke mobiele apparatuur die u alleen op deze bestemming gebruikt en daarna vernietigt.



21. Geef uw apparatuur nooit uit handen en laat deze nooit onbeheerd achter.



22. Maak nooit gebruik van open wifi-verbindingen. Maak altijd gebruik van uw mobiele (data-) abonnement.



23. Maak in het buitenland altijd gebruik van een *Virtual Private Network* (VPN). Kies hierbij uitsluitend voor gerenommeerde VPN-aanbieders.

Privé en thuisomgeving



24. Geef uw draadloos netwerk een niet-herleidbare naam en gebruik geen identificerende termen in de naamgeving van uw mobiele apparatuur (telefoon, laptop, iPad, enzovoort).



25. Verander het standaardwachtwoord van uw router en modem in een sterk wachtwoord.



26. Indien u gasten toegang wilt geven tot uw thuisnetwerk, stelt u hiervoor een gastennetwerk in. Scherm uw gastennetwerk af van uw eigen apparaten.



27. Verwerk geen zakelijke gegevens op uw privéapparaten en vice versa.



28. Verbind uw zakelijke mobiele apparatuur niet met uw thuisnetwerk en gebruik uw privémail niet voor zakelijke doeleinden.

Contactgegevens



29. Wees terughoudend met het verstrekken van uw contactgegevens. Verstrek bij voorkeur algemene contactgegevens.



30. Gebruik online zo min mogelijk uw volledige naam.



31. Overweeg het gebruik van een prepaid telefoonnummer en een alternatief, niet herleidbaar e-mailadres voor registratie op social media accounts en websites.



32. Houd uw privé en zakelijke contactgegevens gescheiden.

Uw omgeving



33. Besef dat personen in uw omgeving ook (onbedoeld) uw gegevens prijs kunnen geven.



34. Slimme apparaten (zoals speakers, camera's, deurbellen, rookmelders) zijn uitgerust met microfoons en andere sensoren die gebruikt kunnen worden om onbedoeld mee te luisteren. Plaats deze apparaten niet in uw werkomgeving.

Deze publicatie is een gezamenlijke uitgave van:

AIVD
BVA-Rijk
CIO-Rijk
MIVD
NCSC
NCTV

maart 2022