☐ 1 Installeer een antivirusprogramma

Gebruik een antivirusprogramma om uw apparaat beschermen en schakel automatische updates in. Laat het antivirus-programma daarnaast geregeld uw apparaten scannen op infecties. Schakel een eventueel meegeleverde firewall altijd in, zodat het de verbindingen tussen het apparaat en het internet in de gaten kan houden.

☐ 2 Gebruik sterke wachtwoorden

Het gebruiken van een moeilijk te raden wachtwoord is belangrijk, vooral bij cruciale systemen zoals DigiD of uw wifi netwerk. Gebruik daarnaast voor elke dienst een uniek wachtwoord. Hiervoor kunt u gebruik maken van een wachtwoordmanager, die unieke wachtwoorden kan genereren en opslaan. Gebruik waar mogelijk twee-staps-verificatie om uw account extra te beschermen.

☐ 3 Installeer altijd de software updates

Producenten van besturingssystemen, browsers en andere programma's brengen geregeld updates uit om beveiligingslekken te verhelpen. Maak ook hier waar mogelijk gebruik van automatische updates. Controleer in andere gevallen minimaal maandelijks of updates beschikbaar zijn en installeer deze.

☐ 4 Maak alleen verbinding met vertrouwde wifi-netwerken

Bij openbare en onbeveiligde wifi-netwerken kunnen anderen meekijken. Verstuur dus geen gevoelige gegevens (e-mail, internetbankieren) over netwerken die u niet kent of niet vertrouwt, of gebruik een Virtual Private Network (VPN).

☐ 5 Open geen berichten en onbekende bestanden die u niet verwacht of vertrouwt

Ontvangt u onverwacht een bericht met een bijlage, (ingekorte) hyperlink of verzoek om in te loggen op een systeem? (phishing). Gebruik uw gezond verstand en ga hier niet op in, zelfs niet wanneer u de afzender kent. Accepteer het bericht alleen als u het van deze afzender verwachtte te krijgen. Spam verwijdert u het beste direct.

☐ 6 Installeer alleen apps via de officiële applicatiewinkels

Ook apps voor uw mobiele telefoon of tablet kunnen malware bevatten. Installeer apps daarom alleen via de officiële applicatiewinkels en gebruik geen illegale kopieën. Kijk ook goed naar de toegangsrechten van de app. Bekijk ervaringen van medegebruikers om u een beeld te vormen van de betrouwbaarheid van de app.

ERCRIME CYBERCRIME CYBERCRIME CYBERCRIME CYBERCRIME CYBERCRIME CYBERCRIME

☐ 7 Controleer het adres van websites

Controleer het webadres (URL) en het certificaat (het hangslotje in de adresbalk van de browser) om vast te stellen dat u geen nagemaakte of onveilige website bezoekt. Is er geen hangslotje? Vul dan geen gevoelige gegevens in op deze website. Gebruik bladwijzers voor websites die u vaak bezoekt en let extra op bij het openen van verkorte URLs. Deze worden veel gebruikt op sociale netwerken.

☐ 8 Ongevraagd helpdesk advies: verbreek de verbinding

Oplichters die zich voordoen als medewerkers van IT-bedrijven zoals Microsoft proberen u telefonisch wijs te maken dat u een computerprobleem heeft, maar dat daar (tegen een vergoeding) iets aan te doen is. Vervolgens vraagt de oplichter om hem mee te laten kijken in uw computer, waardoor hij bijvoorbeeld bij uw bankrekening kan komen. Of hij vraagt betaling voor zijn diensten, bijvoorbeeld via Western Union of Moneygram. Krijgt u zo'n telefoontje, ga dan niet met deze mensen in gesprek. (vishing). Gerenommeerde bedrijven als Microsoft bellen nooit met dit soort meldingen.

☐ 9 Bedenk goed met wie u wat deelt op internet

Zo gemakkelijk als het is om iets op internet te plaatsen, zo moeilijk is het om dit er weer af te krijgen. Denk dus goed na over wat u wel of niet op internet wilt delen. Scherm uw sociale netwerksites goed af (social engineering) en wees selectief in wie toegang krijgt tot uw profiel en gegevens. Laat u uw gegevens ergens achter, ga dan na bij welke organisatie u dat doet, hoe lang uw gegevens worden bewaard en aan wie deze nog meer kunnen worden verstrekt. Geef niet meer gegevens dan noodzakelijk is.

☐ 10 Maak regelmatig back-ups

Door regelmatig back-ups te maken van uw computer en van uw bestanden of foto's op uw telefoon of tablet, kunt u schade van bijvoorbeeld gijzelsoftware of virussen beperken. Indien u een back-up heeft liggen, kunt u toch nog bij een kopie van uw gegevens. Back-ups maakt u op externe, losgekoppelde gegevensdragers (zoals een DVD, USB-stick of externe harde schijf) die u op een andere locatie bewaart. Ook kunt gebruik maken van een online-opslagdienst.

☐ 11 Tenslotte.. gebruik uw gezond verstand!

Als iets te mooi lijkt om waar te zijn, dan is het dat meestal ook. Wees alert online en sceptisch als u iets niet vertrouwt of niet kent.

CYBERCRIME CYBERCRIME CYBERCRIME CYBERCRIME CYBERCRIME CYBERCRIME CYBERC