Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

10 vuistregels voor veilig internetten

Factsheet FS-2013-06
versie 1.0 | 12 december 2013

Via het internet proberen kwaadwillenden op allerlei manieren uw computer, tablet of mobiele telefoon binnen te komen en persoonlijke gegevens te onderscheppen. Malware, phishing, oplichting en spam zijn dreigingen die veel voorkomen. Deze 10 vuistregels vormen een goede basis om u hier tegen te beschermen.

1) Installeer een antivirusprogramma

Gebruik een antivirusprogramma om uw computer, tablet en mobiele telefoon te beschermen en schakel automatische updates in. Laat het antivirusprogramma daarnaast geregeld uw apparaten scannen op infecties, bijvoorbeeld iedere maand. Schakel een eventueel meegeleverde firewall altijd in, zodat het de verbindingen tussen het apparaat en het internet in de gaten kan houden.

2) Installeer steeds de software-updates

Producenten van besturingssystemen, browsers en andere programma's, zoals Microsoft Office, Adobe Reader en Oracle Java, 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.

3) Gebruik sterke wachtwoorden

Het gebruiken van een moeilijk te raden wachtwoord is belangrijk, vooral bij cruciale systemen zoals DigiD of uw wifinetwerk. Gebruik niet overal hetzelfde wachtwoord, wijzig uw wachtwoorden geregeld (bijvoorbeeld ieder jaar) en sla ze niet op in de internetbrowser. Gebruik waar mogelijk two-factor-authentication.

4) Maak alleen verbinding met vertrouwde wifinetwerken

Bij openbare en onbeveiligde wifinetwerken kunnen anderen mogelijk zien wat u op het internet doet en welke gegevens u verstuurt. Verstuur dus geen gevoelige gegevens (e-mail, internetbankieren) over netwerken die u niet kent of niet vertrouwt. Versleutel thuis uw draadloze netwerk met WPA2 met AES-encryptie om te voorkomen dat kwaadwillenden uw internetverkeer kunnen onderscheppen.

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

Ontvangt u onverwacht een bericht met een bijlage, (ingekorte) hyperlink of verzoek om in te loggen op een systeem? 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.

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) Sluit pop-ups in uw browser af met Alt+F4

Klik nooit op akkoord, ok, de 'X' of nee om een pop-up af te sluiten: u kunt hiermee per ongeluk malware installeren. Een pop-up sluit u het beste af via de toetsencombinatie 'Alt+F4'. Installeer eventueel een pop-up-filter om pop-ups te blokkeren.

9) Bedenk goed wat u met wie 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 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) Gebruik uw gezond verstand

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

Het belang van back-ups

Soms gaat er wel eens iets mis met uw computer, ook wanneer u deze vuistregels goed opvolgt. Een virus kan uw gegevens bijvoorbeeld wissen, of de harde schijf kan beschadigd raken. 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, externe harde schijf), die u op een andere locatie bewaart.

Uitgave van **Nationaal Cyber Security Centrum**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl
T 070-888 75 55 | F 070-888 75 50c.m
Publicatienr: FS-2013-06 v1.0