In 10 stappen een veilige Windows-pc

Houd de Windows-computer in tien eenvoudige stappen schoon en veilig!

1. Gezond verstand
Een veilige pc begint en eindigt bij u als bewuste computergebruiker. Hoeveel sloten het systeem ook heeft, door eigen handelen kunt u allerlei narigheid binnenhalen. Houd daarom deze tips in het achterhoofd:

- Reageer niet op mails van onbekende afzenders. Klik niet zomaar op links en bijlagen als u niet honderd procent zeker weet wat het is en van wie het komt.
- Open bij twijfel geen bijlage van een bekende afzender. Het e-mailadres kan overgenomen zijn door kwaadwillende.
- Wees achterdochtig wanneer bedrijven en mensen vragen naar persoonlijke informatie en financiële gegevens.
- Gebruik moeilijke en verschillende wachtwoorden.
- Bekijk webwinkels met een kritische blik. Zijn de prijzen extreem laag? Ziet de website er amateuristisch uit? Komt u veel spelfouten tegen? Is er geen echt bezoek- of postadres vermeld? Staat er een KvK-nummer? Dit zijn allemaal punten die iets zeggen over de betrouwbaarheid van de webwinkel. Meer informatie staat op Consuwijzer.nl.
- Websites waarop u persoonlijke informatie moet invoeren, zoals die voor internetbankieren, moeten beveiligd zijn. U herkent een beveiligde webpagina doordat het adres begint met 'https://' in plaats van met 'http://'.
- Klik nooit op rare meldingen. Boodschappen als 'Spyware gevonden', 'uw computer dient nu te worden gescand', leiden u om de tuin. Klikt u op zo'n boodschap, dan kan de computer worden besmet!
- Vertrouwt u een bezochte website of een melding niet, scan de computer dan op virussen.

2. Windows Update
Een computer bijwerken is belangrijk voor de veiligheid. Windows haalt alle updates zelfstandig binnen via het onderdeel 'Windows Update'. Gebruikers kunnen ze het installeren van updates korte tijd uitstellen. Bekijk de instellingen zo:

- Klik op de Startknop > **Instellingen** (pictogram van het tandwiel).
- Klik in Windows 10 op **Bijwerken en beveiliging**. Klik in Windows 11 linksonder op **Windows Update**.

Het gedeelte 'Windows Update' opent. Hier staat onder meer de mogelijkheid om updates tijdelijk te onderbreken en om de gebruikstijden op te geven (klik in Windows 11 eerst op **Geavanceerde opties**). Dit zijn de uren dat de pc normaal gesproken in gebruik is. In die periode start Windows de pc niet automatisch opnieuw op voor updates. Meestal krijgt u dan bij het afsluiten van Windows te zien of bijwerken en opnieuw starten nodig is.

3. Windows Firewall
Met behulp van een firewall kunt u zich beveiligen tegen kwaadwillende lieden die via internet op de computer willen inbreken, zoals hackers. Windows heeft een firewall die standaard aanstaat.

4. Windows-beveiliging
Windows heeft een virusscanner aan boord. Die beschermt gebruikers prima tegen virussen en ander gespuis. Het mooie is dat Windows-beveiliging standaard aanstaat en u er zelf eigenlijk niks voor hoeft te doen. Open zo de beveiligingsinstellingen van Windows:

- Klik op de Startknop > **Instellingen**. Dat is het pictogram van het tandwiel.
- Klik in Windows 10 op **Bijwerken en beveiliging**. Klik in Windows 11 op **Privacy & beveiliging**.
- Klik op **Windows-beveiliging**.
- U ziet een overzicht van onderdelen met een rode, gele of groene markering erbij. Groen betekent dat alles in orde is, bij rood moet u zelf iets ondernemen en bij geel wordt dit aangeraden.
- Klik op **Windows-beveiliging openen**.
- Nu ziet u dezelfde onderdelen als hiervoor, maar dan met een eventuele melding als u iets moet doen, zoals een onderdeel inschakelen. Volg de instructies.

U hoeft zelf geen andere virusscanner aan te schaffen of te installeren. Mocht u een lopend abonnement hebben op betaalde antivirussoftware en bijvoorbeeld een nieuwe pc hebben, dan kunt dat programma uiteraard gebruiken. Windows-beveiliging schakelt dan uit.

5 Spyware ontdekken en verwijderen
Spyware is een verzamelnaam voor programma's en bestanden (zoals tracking cookies) die gegevens over uw computer- en internetgebruik door kunnen sturen naar derden. Soms installeert u dit zonder dat u het in de gaten hebt. Het zit nogal eens in gratis software van minder betrouwbare makers. Spyware is niet altijd gevaarlijk, maar u wilt natuurlijk nooit software op de computer waar u niet om hebt gevraagd. U kunt het programma Malwarebytes Anti-Malware gebruiken tegen spyware. Het doorzoekt de pc en kan de betreffende bestanden verwijderen.

6. Omgaan met spam
Het grootste deel van al het e-mailverkeer bestaat uit spam (ongewenste reclamemail). De kans is dan ook groot dat u met spam te maken hebt. En een handige Nee/Nee-sticker voor op uw digitale brievenbus bestaat helaas niet.
Veel providers hebben een gratis of betaalde spamfilter. Die houdt foute mails tegen en laat alleen echte berichten door. Veel e-maildiensten zoals Gmail en Outlook.com hebben een eigen spamfilter. U hoeft dit niet in te stellen: het is standaard actief.

7. Nepmails en phishing
Nepmails en phishingmails kunnen erg gevaarlijk zijn. De phishingmail hengelt naar persoonlijke informatie zoals uw creditcard- of bankgegevens, en de nepmail verzamelt e-mailadressen. Verwijder deze mails meteen.
Nepmails blijven lastig te herkennen. SeniorWeb-leden kunnen verdachte mails naar onze phishingchecker doorsturen. U hoort uiterlijk de volgende werkdag of het een phishingmail is.

8. Software bijwerken
Programma's en apps op de pc krijgen periodiek een update. Oude versies van software zijn soms een gevaar voor de pc, omdat ze niet genoeg beveiligd zijn. Verwijder daarom programma's die u ooit hebt geïnstalleerd, maar nooit gebruikt.

- Klik op de Startknop **> Instellingen**. Dat is het pictogram van het tandwiel.
- Klik in Windows 10 op **Apps**. Klik in Windows 11 op **Apps > Apps en onderdelen**.
- Een lijst met alle aanwezige programma's opent. Verwijder het programma:
    - Windows 10: klik op de naam van het programma **> Verwijderen > Verwijderen > Ja**.
    - Windows 11: klik achter de naam van het programma op het pictogram met de drie puntjes **> Verwijderen > Verwijderen**.

Zorg dat u programma's die u wel gebruikt bijwerkt naar de nieuwste versies. Dit werkt vaak op verschillende manieren. Soms hebben ze een automatische updatefunctie die u kunt inschakelen. Of er wordt automatisch om de zoveel tijd gevraagd of u de nieuwste versie wilt installeren. Kies dan voor **Ja**. Tenslotte kunt u kijken op de website van de maker en daar de laatste versie van het programma downloaden.

9. Back-up instellen
Maak regelmatig back-ups van zaken die belangrijk voor u zijn. U denkt er niet graag aan, maar de computer kan crashen of onbruikbaar worden door een virus. Daardoor kunt u alle e-mails, foto's en belangrijke documenten kwijtraken. Lees op SeniorWeb hoe u een back-up in Windows 10 of Windows 11 instelt.

10. Draadloos netwerk beveiligen
Beveilig het wifi-netwerk met een eigen wachtwoord, zodat derden geen toegang hebben. Bent u niet handig met routers en dergelijke? Volg nauwkeurig de instructies in de handleiding. Of laat een expert het netwerk installeren en beveiligen. Uw provider kan u daarbij helpen.

Bron: SeniorWeb nieuwsbrief van 26 mei 2022