12 tips om veilig om te gaan met je computer en het internet

Een lijstje om na te kijken: pas jij alle basistips toe om veilig online te gaan?

De basis

1. Zorg voor een virusscanner en scan regelmatig

Besef wel dat antivirusprogramma's altijd even tijd nodig hebben om nieuwe virussen te herkennen. Zo ontsnappen nieuwe virussen soms aan het oog van de virusscanner. Zorg dus dat je steeds de laatste versie van het antivirusprogramma op je computer hebt staan en wees zelf altijd waakzaam.

2. Hou je computer en je programma's automatisch up-to-date

Kijk de instellingen van je computer na. Zorgt je besturingssysteem er automatisch voor dat je steeds de meest recente versie van je programma's hebt? Een aantal programma's (zoals Adobe PDF reader) of verschillende browsers (Internet Explorer, Firefox en Chrome) bieden zelf ook automatische updates aan.

3. Maak regelmatig een reservekopie op een externe harde schijf

Maak een reservekopie op één of verschillende externe harde schijven. Bewaar deze op een veilige plek en koppel de reservekopie steeds systematisch los van je computer of netwerk. Zo vermijd je bij een besmetting met ransomware dat ook je reservekopie gegijzeld wordt. Ook bij technische problemen is het fijn te kunnen terugvallen op een kopie.

Wees waakzaam…

4. Externe bestanden? Even scannen op virussen!

Krijg je een document via e-mail of wil je bestanden vanop een USB-stick op je computer plaatsen? Scan deze altijd even voor je ze opent. Dit kan eenvoudig via je virusscanner.

5. Klik niet zomaar op alle links, afbeeldingen of video's

Een bezoek aan een onbekende of valse website is voldoende om je computer te besmetten. Klik dus enkel op links of afbeeldingen en video's die je vertrouwt.

6. Installeer alleen software van een betrouwbare bron

Download een programma nooit van de eerste de beste website die door zoekmachines (zoals Google) wordt weergegeven, maar download enkel van de officiële website van de maker van het programma.

Bij het gebruiken van accounts zoals e-mail…

7. Gebruik sterke wachtwoorden, hergebruik ze niet en deel ze nooit

De gouden regel: hoe langer het wachtwoord, hoe veiliger. Gebruik een wachtzin in plaats van een woord: een lange zin is simpel te onthouden én veiliger. Je kan ook een beroep doen op programma's, oftewel 'wachtwoordkluizen', om het wachtwoord voor jou te maken én te onthouden.

8. Log in 2 stappen in voor je belangrijke accounts, zoals e-mail

Naast je wachtwoord geef je bijvoorbeeld ook een code in die alleen jij via je gsm toegestuurd krijgt. Deze mogelijkheid kan je vaak zelf activeren binnen het programma of bij de website waarmee je werkt. De antwoorden op geheime vragen die je kan invullen om je wachtwoord extra te beveiligen of te resetten, zijn simpel te raden. Moet je dit toch invullen, dan antwoord je best niet op de vraag, maar geef je een fictief antwoord. Onthoud dit zelf goed of maak gebruik van een wachtwoordkluis.

Als je online betaalt…

9. Surf via https als je online betaalt en vertrouw geen bedrijven die je via mail of telefoon contacteren

Wanneer https:// in je browser staat als begin van je internetadres, dan werk je met een beveiligde verbinding. Vertrouw ook geen bedrijven die je via mail of telefoon contacteren om gegevens vragen. Verwijder de mail of hang op.

Als je draadloos internet gebruikt…

10. Wees waakzaam wanneer je openbare Wi-Fi gebruikt

Online betalen of wachtwoorden ingeven van belangrijke accounts, zoals je e-mail, doe je best nooit wanneer je op een onbeveiligd draadloos netwerk werkt.

11. Beveilig je Wi-Fi-netwerk thuis

Beveilig je netwerk thuis met een wachtwoord. Zo kan niemand, of het nu cybercriminelen of je buren zijn, gebruik maken van je draadloos internet.

En als je je toestel weg doet…

12. Zorg dat het geheugen van je toestel volledig gewist is

Het geheugen van je smartphone of tablet maak je leeg via de optie "wissen" op je toestel. Je computer of laptop wis (formatteer) je best volledig. Je kan dit snel of uitgebreid laten uitvoeren. Een snelle “format” is geen goed idee, dan blijven er altijd gegevens achter.