Top 10 tips voor zorgeloos 2020

Tip 1	**Zorg voor actuele versies van uw software**
Tip 2	**Zorg voor een bijgewerkt antivirus programma**
Tip 3	**Maak gebruik van een betrouwbaar en beveiligd netwerk**
Tip 4	**Maak goede en makkelijk te onthouden wachtwoorden**
Tip 5	**Denk logisch na**
Tip 6	**Maak regelmatig een Back-up**
Tip 7	**Wees alert op Phishing**
Tip 8	**Pincode instellen op al uw apparaten**
Tip 9	**Gebruik tweestaps verificatie**
Tip10	**Schakel expertise in.**

Tip 1

Zorg voor actuele versies van uw software

Windows 10 = Versie 1909

Een perfect stuk software bestaat niet. Fabrikanten doen er alles aan om hun software veilig te maken/houden. Middels updates worden veiligheidslekken gedicht.

Zien welke Windows 10-versies je hebt

Je controleert als volgt welke versie van Windows 10 op je pc is geïnstalleerd:

1. Selecteer de **Startknop** en daarna **Instellingen** .
2. In Instellingen selecteer je **Systeem** > **Info**.

Tip 2

Zorg voor een bijgewerkt antivirus programma.

Microsoft levert Windows 10 standaard met het antivirusprogramma **Windows Defender**. Na een wat moeizame aanloop scoort het programma heel goed als bescherming tegen de gebruikelijke dreigingen zoals virussen en malware.

Virussen willen zo snel mogelijk en zo veel mogelijk schade aanrichten. Documenten en programma's worden beschadigd en in het ergste geval kun je ze niet meer gebruiken (dus: herinstallatie PC).

Windows Defender Antivirus komt als Microsoft’s alternatief voor een antivirus applicatie. Daarbij doet Windows Defender het vrij goed. Windows Defender beschermt uw Windows 10 PC tegen virussen, ongewenste software en adware. Windows Defender is eigenlijk altijd up to date omdat Windows 10 zelf de updates download en installeert terwijl de gebruiker de computer gebruikt voor alle daagse dingen zoals b.v. werken en gamen. Dit is allemaal geen probleem voor Windows Defender.

Tip 3

Maak gebruik van een betrouwbaar en beveiligd (draadloos) netwerk

Zorg voor een goed beveiligd WIFI netwerk. WIFI is namelijk vrij éénvoudig te hacken, en nog éénvoudiger te misbruiken. Geef je netwerk een eigen naam en verander het standaard wachtwoord. Kijk hiervoor in de handleiding van je router.

Tip 4

Maak goede en makkelijk te onthouden wachtwoorden

Gebruik wachtwoorden met minimale lengte van 8 tekens:
het liefst een combinatie van hoofdletters, kleine letters, cijfers en tekens.

Voor de hand liggende wachtwoorden zijn makkelijk te kraken. Een cijferreeks (123456), een woord (Geheim) of een combinatie van uw voornaam en geboortedatum (Rita1957) is door een computerprogramma dat hackers inzetten snel geraden.

Een **sterk wachtwoord** bestaat uit een reeks van zes tot acht willekeurige letters en cijfers, en wat leestekens. Hoe beter het wachtwoord, hoe lastiger het is om te onthouden. Er zijn wel trucjes om sterke wachtwoorden te maken die toch redelijk eenvoudig te onthouden zijn.

Tip 5

Denk logisch na

Als iets te mooi is om waar te zijn, is het dat waarschijnlijk ook

Mensen geven graag informatie als ze te lezen krijgen dat ze iets gewonnen hebben, of de zoveelste 1.000ste bezoeker zijn. Maar bijvoorbeeld ook de creditcardmaatschappij laat je niets online verifiëren.

Tip 6

Maak regelmatig een Back-up

Je foto's, bestanden, scans en wellicht een stuk administratie. Velen hebben deze informatie op de harddisk staan, wanneer de harddisk kapot gaat, of je krijgt een akelig Windows virus, dan heb je kans deze gegevens kwijt te raken. Maak een back-up op een USB stick, externe harddisk of maak gebruik van een Online dienst (zoals Dropbox, OneDrive of GoogleDrive)

Tijdens het maken een back-up wordt enkel de actuele data meegenomen, met slimmere back-up methodes kun je ook wijzigingen back-uppen zodat je naar eerdere versies terug kan grijpen indien nodig.

Tip 7

Wees alert op Phishing

Het lokken van de bezoekers naar nep-sites om daar persoonlijke (betaal) informatie te ontfutselen. Zo is bijvoorbeeld de ING site geheel nagebouwd geweest.

Hyper-links, of teksten waarachter een URL zit verwijzen niet altijd naar de URL die je verwacht. Door met de muis eroverheen te zweven verschijnt vaak de achterliggende URL.

Tip 8

Pincode instellen op al uw apparaten

Het grootste lek wat er is: geen pincodes, maar wel verbonden zijn met het internet. Dit grootste lek is wel het simpelste op de lossen: gewoon instellen :-) !

Tip 9

Gebruik tweestaps verificatie

Het is belangrijk dat je voor alle online diensten een sterk wachtwoord kiest. Gebruik dit wachtwoord niet opnieuw bij andere online diensten en wijzig het regelmatig. Toch kan het nóg veiliger met tweestapsverificatie. Dit kun je bij steeds meer online diensten zelf instellen. Een cybercrimineel heeft dan niet meer genoeg aan je gebruikersnaam en wachtwoord, bijvoorbeeld verkregen uit een datalek bij een leverancier van een online dienst. Met tweestapsverificatie is bij het inloggen een extra toegangscode vereist die je ontvangt via een vertrouwd apparaat zoals je smartphone.

Tip 10

Schakel expertise in

Het installeren, beheren en onderhouden van je pc, laptop, tablet, I-pad, smartphone, I-phone is vakwerk. Wanneer je zelf niet over de benodigde kennis beschikt, schakel dan altijd een professionele partij in die je apparaten en de beveiliging daarvan voor zijn rekening neemt. Wees kritisch want niet elke ICT-leverancier heeft specifieke kennis van digitale veiligheid of ervaring

Frits van der Meer
De Koperwiek 31, 7609 GT Almelo
M: 06 – 37614063 / T:0546 823953

E: *vandermeer.frits@gmail.com*

Voor leren aan huis, voor vragen over - , Voor storingen aan - , Voor advies bij aankoop
Computer, Laptop, I-pad, Tablet, Smartphone of randapparatuur