

SAFER INTERNET



CHECKLIST

FIBER CREW

SAFER INTERNET CHECKLIST

-  Gebruik wachtwoorden waar **geen logica** in zit. Een combinatie van hoofdletters, kleine letters, cijfers en leestekens is het beste.
-  Nog beter is om een '**password manager**' te gebruiken. Hierin kan je al je wachtwoorden opslaan én goede wachtwoorden automatisch genereren.
-  Gebruik **geen openbare WiFi-netwerken**. Hackers kunnen dan namelijk heel eenvoudig in jouw apparaat en bij jouw gegevens komen. Dit geldt ook voor WiFi-netwerken waarvan het wachtwoord bekend is, zoals in hotels en restaurants.
-  Moet je toch vaak openbare WiFi-netwerken gebruiken? Overweeg dan een **VPN-verbinding**. Dit kan je al voor een paar euro per maand afnemen. Met een VPN ga je als het ware als een afgesloten tunnel door de openbare WiFi met jouw gegevens. Zo blijft jouw surfgedrag anoniem en veilig.
-  Houd je **thuisnetwerk veilig**! Kies een lastig wachtwoord voor je eigen WiFi-netwerk en verander het af en toe.
-  Check bij websites of de URL begint met '**https**'. De 's' is heel belangrijk, want die staat voor *secure*. Er staat dan ook altijd een slotje voor een website met 'https' Doe nooit een online betaling via een website zonder zo'n slotje en HTTPS.
-  Zorg dat de software op je computer en het besturingssysteem altijd **up to date** zijn, dan is de beveiliging dat ook!

Leestip:

Je hebt wél iets te verbergen door Maurits Martijn (2018)

FIBER CREW

De Fiber Crew © 2020

SAFER INTERNET CHECKLIST

-  Doe je een online betaling? **Check** ook **de url**. Criminelen worden steeds beter in het misleiden van internetgebruikers en maken de websites van banken soms tot in de details na. Lees daarom altijd wat er achter 'www' staat en check nauwkeurig of de spelling van de url klopt. Zo deden criminelen zich voor als Rabobank met de url www.rab0bank.nl. Neem bij twijfel altijd contact op met je bank.
-  Kijk verder dan de **eerste zoekresultaten**, de bovenste resultaten zijn niet per se het meest betrouwbaar, goedkoop of interessant.
-  *Worst case scenario*: al je bestanden kwijt, foto's weg en digitale agenda gewist. Maak daarom regelmatig een **back-up** op een harde schijf of in de cloud.
-  Download apps voor je smartphone en tablet **alleen** in de **officiële appstores**: Google Play Store, App Store en Windows Store. Zo verklein je het risico op virussen en malware.
-  Installeer een **adblocker**. Adblock Plus is gratis te downloaden voor bijna alle internetbrowsers en blokkeert de meeste advertenties, inclusief tracking, malwaredomeinen, banners en pop-ups.
-  **Accepteer niet alle cookies**. Wees je ervan bewust dat bij het accepteren van bijvoorbeeld marketingcookies, sommige websites jouw gegevens aan tientallen bedrijven doorgeven. Accepteer daarom alleen de noodzakelijke cookies.

Leestip:

Het is oorlog maar niemand die het ziet door Huib Modderkolk (2019)

FIBER CREW

De Fiber Crew © 2020

SAFER INTERNET CHECKLIST

-  **Duik eens in de privacy- en advertentie-instellingen** van jouw social media en geef aan wat je wel en níet wilt. Op LinkedIn kan je bijvoorbeeld instellen dat iemand geen melding krijgt dat jij zijn/haar profiel hebt bekeken.
-  **Zet locatievoorzieningen uit.** Bekijk eens in je telefoon of browser welke apps of websites jouw toestemming hebben om je locatie te bepalen en vraag je af of jij wel wil dat deze partijen continu weten waar jij je bevindt. Wellicht verhandelen ze deze gegevens zelfs door! Wees hier dus kieskeurig in.
-  **Verwijder cookies.** Door bijvoorbeeld eens per maand je browsegegevens te wissen voorkom je dat je online stiekem achtervolgd wordt. Let op: niet alle cookies zijn slecht!
-  **Pas op met gratis templates.** Met digitale templates kan je goedkoop een website (laten) maken. Helaas zijn criminelen er heel bedreven in om de populairste templates te hacken. Doe daarom altijd research naar het template dat je kiest en zorg dat alle plugins en templates continu up to date zijn!
-  **Vergrendel je scherm** als je niet op je werkplek zit.
-  Phishing-criminelen blijven nieuwe wegen naar Rome zoeken. **Wantrouw** daarom alle **e-mails, smsjes en andere berichten** via informele kanalen waarin gevraagd wordt om een wachtwoord, pincode of het overmaken van een bedrag. Jouw bank, verzekeraar of creditcardmaatschappij zal je nooit via de telefoon, e-mail of sms om zulke belangrijke informatie vragen. Bovendien is een e-mailadres heel eenvoudig te vervalsen. Bij twijfel: niks geven en melding maken bij de politie!

FIBER CREW

De Fiber Crew © 2020