## Hoe veilig is uw computer?

### *Enkele tips.*

Het grootste gevaar voor uw computer, en dus meteen ook voor uw gegevens, zijn cybercriminelen. Deze plunderen uw bankrekening, verhuren uw computer of doen hem crashen om losgeld te eisen.

Hoe loop je die besmettingen op?

- Door oude software te gebruiken. Deze software bevat soms veiligheidslekken die door de malware gebruikt wordt om je computer binnen te dringen. Doe dus steeds alle updates, zeker deze van Windows. Klap dus s'avonds niet gewoon je laptop dicht want op deze manier kunnen de updates niet geïnstalleerd worden. Een update hersteld de net gevonden veiligheidslekken.
- Door spam. Deze oude bekende van je mailbox verspreid zich nog altijd massaal. Klik niet op vreemde linken in mails van onbekenden.
- Malware via sociale media werkt op dezelfde manier. Klik niet op gelijk welke link.
- Klikken op een link is trouwens niet echt nodig om besmet te worden. Wie surft doet niets anders dan downloaden. Alles wat je op een website ziet wordt gedownload. Plug-ins en kleine toepassingen om bvb. Video te bekijken of audio te beluisteren worden doorgaans zonder toestemming geïnstalleerd. Het is dus niet moeilijk dat hiermee ook malware op je toestel binnenkomt. Zodra de malware op je toestel staat kunnen de criminelen ermee aan de slag. E-mailadressen, wachtwoorden, identiteits- en kredietkaartgegevens zijn waardevol. Wanneer je betaling uitvoert kan die door malware onderschept worden om meteen een groter bedrag naar een frauduleuze rekening te storten. Jij geeft daarvoor gewoon de toestemming via je digipass en krijgt de fraude pas te zien als het geld al van je rekening is.
- Zelfs wie geen informatie opslaat en geen bankverrichtingen doet met zijn computer blijft een waardevolle prooi. Een gehackte computer wordt gebruikt om malware te versturen of een cyberaanval uit te voeren.

1. Installeer alle updates voor je programma's, zeker de Windows updates. Let op: de ondersteuning voor Windows XP is stopgezet op 8 april 2014 en voor Windows Vista op 11 april 2017. Vanaf dan zijn er voor XP en Vista geen beveiligingsupdates meer en wordt je toestel dus steeds meer vatbaar voor cyberaanvallen.
2. Klik niet zomaar op een link, foto of video.
3. Let op met spam. Doe deze niet open en klik zeker niet op een aantrekkelijk lijkende link.
4. Ga op sociale media behoedzaam te werk. Ook dit is een broeihaard van frauduleuze berichten.
5. Installeer een degelijke virusscanner met een betrouwbare firewall en hou deze up-to-date! De gratis virusscanners die je kunt downloaden bevatten meestal geen firewall en beschermen ook niet zo goed als de betalende! De gratis virusscanner van Microsoft is puur basis en kan momenteel niet tippen aan de degelijke beveiliging.
6. Laat je computer, minstens jaarlijks, scannen op virussen en verdachte software. Meestal is je toestel daarna ook weer een stuk sneller. Dit is een service die Trax Computers uitvoert voor € 50,-.
7. Maak regelmatig backups !!! Je kunt bij Trax Computers ook een 'image' van je computer laten maken. Dit is een exacte kopie van uw toestel op dat gegeven ogenblik. Deze kan altijd weer worden teruggeplaatst zodat je alle gegevens, mails en programma's terugkrijgt. Zelfs als de harde schijf helemaal stuk is en er een nieuwe geplaatst moet worden. Dit kan al vanaf € 30,-. Deze 'image' wordt dan een jaar bewaard. Hoe vaker je een 'image' laat maken, hoe minder gegevens je kwijt bent.