

## Computer Beveiliging Waarom en hoe

Onze maatschappij kent vele mensen die het niet zo nauw nemen met zaken die hen niet aangaan en het verschil tussen mijn en dijn niet kennen. Dat betreft niet alleen materiële zaken als een computer, TV en dergelijke maar ook onze pasjes met bijbehorende (PIN-)code en daarnaast natuurlijk onze immateriële zaken zoals foto's en erfstukken. Door dit alles wordt onze privacy behoorlijk geschaad en kan, zoals bij inbraak en molest, zelfs ernstige emotionele schade toebrengen.

Daarom nemen we steeds meer maatregelen om onze eigendommen te beschermen. Vroeger werd de buitendeur nauwelijks op slot gedaan en konden mensen gewoon binnenkomen. Die hadden dan ook geen slechte bedoelingen. Inmiddels is het op slot hebben van de voor- en achterdeur een minimale vereiste. Verder wordt nu extra vergrendeling aangebracht op alle deuren en openslaande ramen. Ook wordt aangeraden om bij afwezigheid vooral licht te laten branden, post niet zichtbaar te laten bij de voordeur, geen tasje aan de deur, geen boodschap op de stoep, et cetera.

Welnu met de beveiliging van onze computer gaan we ook steeds verder. Sinds de meeste computers zijn aangesloten aan het Internet zijn de bedreigingen steeds verder toegenomen. Deze syllabus probeert inzicht te geven in de bedreigen maar vooral hoe we ons daar tegen kunnen of zelfs moeten wapenen.

De bedreigingen en vervelende zaken behandelen we in de volgende onderwerpen:  
bijwerken systeem, inbraak, virus, spyware, spam, cookie, phishing, internetbankieren.

### Bijwerken systeem

Windows is een zeer geavanceerd pakket uitgebreide software met wel een miljard regels aan codering verdeeld over vele, vele modules. Zo bestaat het Windows pakket voor Vista Home Premium uit bijna ACHT GIGABYTE aan software. Ja en daar kan hier en daar een fout(je) in zitten waar misbruik van gemaakt kan worden.

Daarom ziet u regelmatig dat Windows wordt bijgewerkt om (soms) nieuwe zaken ter beschikking te stellen maar vooral om fouten te herstellen en dan met name om de beveiliging te verbeteren. Zeker de updates die door Microsoft zijn aangemerkt als essentieel zijn zeker noodzakelijk.

Het (automatisch laten) bijwerken van Windows is een eerste **vereiste** om uw computer te beveiligen.

Denk niet dat alleen beveiligingslekken in Windows voorkomen. Elke software en driver kan ook lekken bevatten, het bijwerken van deze zaken is minder urgent dan Windows maar kan zeker belangrijk zijn. Niet alleen vanwege lekken maar ook vanwege verbeterde functionaliteit.

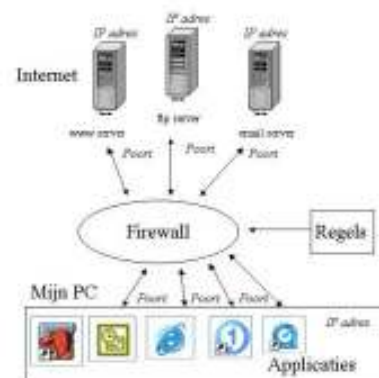
### Inbraak

Een firewall beschermt uw computer door te voorkomen dat onbevoegde gebruikers via internet of een netwerk toegang krijgen tot uw computer. Dat is het inkomende deel. Het uitgaande deel bewaken voorkomt dat toepassingen ongewenst verbinding maken met het netwerk. Hierdoor wordt voorkomen dat Trojaanse paarden, backdoors, keyloggers en andere malware uw computer beschadigen en privégegevens stelen.

De standaard firewall van Windows XP houdt alleen indringers tegen en is daardoor beperkter dan de meeste andere firewalls.

Bekende firewalls van commerciële bedrijven zijn McAfee, Norton (Symantec) en Panda.

Daarnaast kunt u gebruik maken van de gratis versie van ZoneAlarm of de betaalde PRO versie



daarvan zie [www.zonealarm.com](http://www.zonealarm.com).

Zomaar een willekeurig aantal andere gratis firewalls die u kunt vinden op:

1. PC Tools Firewall Plus: [www.pctools.com/nl/firewall](http://www.pctools.com/nl/firewall)
2. Sunbelt Personal Firewall (ook een gratis versie): [www.sunbelt-software.com](http://www.sunbelt-software.com)
3. Outpost Free Firewall: [www.agnitum.com](http://www.agnitum.com) -
4. Comodo Firewall: [www.personalfirewall.comodo.com](http://www.personalfirewall.comodo.com)

U kunt **niet** zonder een **actieve** firewall

## Virus

U heeft natuurlijk allemaal een antivirusprogramma programma, er zijn er veel beschikbaar. De meeste daarvan moet u kopen en dan jaarlijks opnieuw betalen om weer volledig bijgewerkt te zijn. De bekendste leveranciers daar van Norton (Symantec), McAfee, Norman, Kaspersky, Panda, TrendMicro, Nod32 en Gdata.

Opgemerkt moet nog wel worden dat Norton (Symantec) en McAfee het meest aan de weg timmeren. Het zijn zeker goede producten maar hebben als nadeel dat ze de computer veelal traag maken. Hoewel er berichten zijn dat Norton en McAfee hun versie van 2008 verbeterd hebben.

Daarnaast zijn er enkele bijzonder goede gratis antivirusprogramma programma's:

1. [www.avast.nl](http://www.avast.nl) voor het program AVAST! Home Edition. U moet registreren om een download-link te krijgen. Ook registratie, jaarlijks herhalen, is verplicht. Het programma is Nederlandstalig, maar alle email gaat in het Engels.
2. <http://free.grisoft.com>, AVG Anti-Virus Free Edition.
3. [www.free-av.com](http://www.free-av.com) voor het programma Avira AntiVir® PersonalEdition Classic
4. [www.clamwin.com](http://www.clamwin.com) voor het programma ClamWin Free Antivirus (nu nog niet voor Vista)

U kunt **niet** zonder een **actief** antivirusprogramma, dat altijd automatisch wordt bijgewerkt

## Spyware

Spyware kunt u vertalen als 'spionage software' en dan is het direct duidelijk wat er mee wordt bedoeld. Het zal allerlei gegevens over het gebruik van de computer opslaan en doorsturen naar anderen en die gegevens worden dan vaak weer verkocht aan bijvoorbeeld marketingbedrijven. Voorbeelden van die gegevens zijn e-mailadressen, de bezochte Internetpagina's (en hoelang), welke programma's gebruikt worden enzovoort. Het gaat dus om privé-gegevens, en daar heeft dus eigenlijk niemand wat mee te maken.

Vooral gratis software **kan** spyware bevatten, soms staat dat ook in de gebruikersovereenkomst te lezen. Echter in veel gevallen zal de spyware geïnstalleerd worden zonder dat het duidelijk is. Dat kan bijvoorbeeld bij het bezoeken van een webpagina, hierbij wordt dan gebruik gemaakt van fouten in Windows. En dat gebeurt niet alleen op discutabele Internet sites met

Het is vooral uw eigen gedrag wat spyware mogelijk maakt. Gebruik uw gezonde verstand en klik niet achteloos op een pop-up of op 'ja' wat het installeren van spyware in gang kan zetten.

Daarnaast wordt het afgeraden om pagina's te bezoeken die gratis muziekbestanden, gratis porno, gratis cracks en dergelijke beloven omdat die juist vaak spyware op je computer zetten.

Helemaal te voorkomen is het echter niet en soms merkt u daar niets van, maar de computer kan heel traag worden, de startpagina is veranderd of er komt heel veel reclame via pop-ups.

Een deel wordt herkend en verwijderd door uw antivirusprogramma. Er zijn speciale programma's die de computer scannen en spyware verwijderen. Ook hier is weer een keur aan programma's en elk schijnt zijn eigen specifieke aandachtsgebieden te hebben waardoor meerdere nodig zijn om alles te verwijderen.

De bekendste gratis programma's om aanwezige spyware van uw computer te verwijderen zijn AdAware en Spybot Search & Destroy. Beter is dan nog om Hitmanpro ([www.hitmanpro.nl](http://www.hitmanpro.nl)) te gebruiken, dat voert scans uit met die twee en nog anderen. Ook worden enkele probeerversies gedownload en uitgevoerd met als gevolg dat u daarover regelmatig meldingen en aanbieding krijg.

Daarom is het beter om Webroot SpySweeper en NOD32 uit te schakelen. Ook AVG Anti-Spyware (<http://free.grisoft.com>) is een gratis programma. Windows Defender is ook gratis en beschermt uw computer tegen pop-ups, vertragingen en bedreigingen als gevolg van spyware en andere ongewenste software. Het programma biedt realtimebescherming, een bewakingssysteem dat u aanraadt actie te ondernemen tegen gevonden spyware, dat lange onderbrekingen voorkomt en dat u helpt productief te blijven. Zie: <http://www.microsoft.com/athome/security/spyware/software/default.mspx> Onder Windows Vista is de AntiSpyware “Windows Defender”, deze is gratis en ook onder Windows XP te gebruiken en te verkrijgen via de website van Microsoft: <http://www.microsoft.com/netherlands/ondernemers/veiligheid/defender.aspx>.

U moet **regelmatig** uw computer scannen om spyware te verwijderen

## Spam

Steeds meer mensen krijgen te maken met steeds meer spam, dat zijn ongevraagde e-mails die naar massa's e-mailadressen worden verzonden. Volgens spamexperts groeit het aantal gestaag, er worden percentages genoemd variërend van 70 tot ruim 90 van de totale email, dus heel veel. Waarschijnlijk komen de meeste spam berichten al niet bij u aan omdat veel Internet Service Providers maatregelen hebben genomen om al heel veel tegen te houden. Helaas kunnen ze spam nooit voor 100% uitfilteren en komt dus ook spam bij u terecht.

Spammers beschikken over enorm grote zombienetwerken en worden steeds inventiever. Hackers zijn verantwoordelijk voor het opzetten van een netwerk met geïnfecteerde computers. In oktober 2005 werd een zombienetwerk door GOVCERT.NL afgebroken, het bestond uit 1,5 miljoen computers waarvan 30.000 in Nederland. Door het opbouwen van nieuwe zombienetwerken verkrijgen spammers steeds weer andere unieke verzendadressen, en is het lastig om te bepalen of een bericht van een spammer afkomstig is.

Allereerst moeten we zelf voorzichtig omgaan met ons e-mailadres, hierna volgens een aantal aandachtspunten om spam tegen te gaan.

## Goed e-mailadres

Spammers gokken naar een e-mailadres door alle combinaties van letters, voor het @ teken, te proberen. Het is daarom van belang het adres niet te kort te houden en liefst wat bijzondere tekens daarin op te nemen. Voor verantwoord e-mail beheer zijn een aantal adressen nodig.

- Adres voor vrienden en bekenden (het hoofd e-mailadres)
- Adres voor bedrijven en mailinglijsten (een eenvoudig te wijzigen alias op het hoofdadres)
- Adres voor incidenteel internetgebruik (tijdelijke e-mailadres providers)

## E-mailadres vermommen

Gewoon lukraak uw e-mailadres op een website of een nieuwsgroep publiceren is vragen om spam. De oplossing is het adres te vermommen onder andere de volgende opties zijn:

- naam(a)domein.nl
- naam(at)domein.nl
- naam@domein DOT nl
- naam(at)domein DOT nl

## Website contactformulieren

De hierbij ingevoerde gegevens wordt vaak onbeschermd doorgeleid naar het e-mailadres. Spammers kunnen hieraan hun eigen informatie hangen. De webserver wordt hierdoor enorm belast en fungeert als zombienetwerk. Nu zijn er met behulp van ASP speciale mailcontactformulieren ontwikkeld die beveiligd zijn tegen misbruik door derden.

## Gebruikersgedrag

Welke en hoeveel maatregelen u ook treft, de zwakste schakel blijft uzelf. U moet zich bewust zijn van spam en de negatieve gevolgen daarvan. Neem het volgende in acht:

1. Negeer spam: verwijder deze meteen zonder te openen. Zelfs in het openen van spam-mail zit een risico.
2. Beantwoord nooit spam. Klik ook niet op knoppen waarmee u zich kunt afmelden voor de mail. Dit moet u alleen doen als u zich bewust heeft aangemeld.
3. Update voortdurend alle software die u gebruikt om te e-mailen. Update ook de bijbehorende mailfilters. Spammers zullen voortdurend de laatste nieuwe trucs toepassen om antispam maatregelen te omzeilen.
4. Geef nooit persoonlijke informatie zoals pincodes af via e-mail, als daar om verzocht wordt. Het verzoek kan een truc zijn. Goedwillende bedrijven doen dit niet.
5. Gebeurt dit wel neem dan contact op met de klantenservice van het desbetreffende bedrijf.
6. Open geen e-mailbijlagen als u de afzender niet vertrouwt.
7. Koop nooit via een spam-e-mailbericht. Dit maakt het spammen alleen maar lucratiever. Als u geïnteresseerd bent in het aangeboden product, surf dan rechtstreeks naar de website van het bedrijf en laat de link in de e-mail ongebruikt.
8. Stuur nooit **ketting-e-mailberichten** door. Ongeacht de waarschuwingen of onheilsvoorspellingen die daarin staan. U wordt er echt niet slechter door.
9. Maak altijd melding van spam bij uw Internet Service Provider (ISP).
10. Meld phishing en spam bij de bedrijven die genoemd worden. Sommige bedrijven hebben hiervoor een speciaal e-mailadres ingesteld. Zo kunt u spammail over MSN melden bij [abuse@msn.com](mailto:abuse@msn.com). Met de speciale Junkmail-knop in Hotmail kunt u direct een melding maken van spam voordat u de mail heeft verwijderd.

**Spamgourmet** - gratis wegwerp-e-mail adressen, sterke spamblokkering, korte aanleertijd.

2,551 dagen, 161,637 gebruikeraccounts  
2,953,986 wegwerpdressen  
26,872,149 afgeleverde berichten, 11,107 vandaag  
228,476,126 opgegeven berichten, 203,858 vandaag

"Kom maar opt!!!"

<b>Hersenloze modus</b> goede afscherming geen onderhoud	<b>Modus voor gevorderden</b> betere bescherming weinig onderhoud nodig
--	---

Log in

gebruiker  Log in

wachtwoord

afgeschermd adres  sla op

Je bent niet ingelogd!

## Tijdelijke e-mailadressen

E-mail adressen worden verkocht, hiervoor wordt zelfs, in de vorm van spam, reclame gemaakt. Hoewel de meeste mensen het privacy statement of de licentie niet lezen, is het verstandig dit wel te doen. Staat dat u niet aan, geef dan uw e-mailadres niet. Als dat toch nodig is voor die site "ter bevestiging" dan is een tijdelijk e-mailadres de oplossing.

Het is natuurlijk ook mogelijk om gewoon het e-mailadres te plaatsen, maar dit regelmatig te vervangen. Op de achtergrond kunt u dan toch de mail doorlinken naar een door u gewenst adres.

Een aardige site die u hierbij kan helpen is Spamgourmet (Engelstalig):

<http://www.spamgourmet.com/>. Na registratie kunt u een e-mailadres aanmaken dat een aantal malen gebruikt kan worden. Daarna wordt het adres uitgeschakeld en wordt een nieuw adres aangemaakt. Spam krijgt op deze manier geen enkele kans.

Email programma actief tegen spam

Een goede ISP zal zorgen dat u zo min mogelijk spam ontvangt in uw Inbox, zij hebben zelf belang om dit goed te doen. De spam die de ISP doorlaat zal ook door een goed e-mailprogramma gefilterd worden. Zij kunnen strikter zijn omdat ze de e-mails allen verplaatsen en het aan uzelf is om het definitieve oordeel te vellen (verwijderen of niet).

## Berichtregels en Spamfilter

Als u nog veel spam ontvangt dan kunnen daar berichtregels voor aangemaakt worden in het e-mailprogramma. Dat is best een klus omdat regelmatig nieuwe regels moeten worden ingevoerd. Gelukkig bestaan er gratis programma's die dat voor u kunnen doen, dat zijn ondermeer de gratis

spamfilter programma's Spamihilator en Spamfighter. In alle gevallen is de SPAM al ontvangen, het enige wat gedaan wordt is berichten uit de Inbox verplaatsen naar een special SPAM-map, dan kunt u zelf een laatste controle op de berichten uitvoeren en ze verwijderen.

Spammers zijn zeer inventief en verzinnen steeds meer en nieuwe technieken, daarom zal nooit een 100% spam herkenning kunnen worden gerealiseerd.

SPAM is vooral lastig en vervelend maar kan op zich weinig kwaad. Mits ...

### **NEGEER SPAM**

Niet beantwoorden, niet doorsturen, niets kopen en de afbeeldingen niet downloaden

#### **Phishing**

Phishing komt steeds vaker voor, de term komt van het Engelse fishing, dat "vissen" betekent, dus het 'hengelen' naar gegevens. U krijgt dan bijvoorbeeld een e-mail uit naam van een bedrijf waarin wordt gevraagd naar persoonlijke gegevens. Maar dat komt van oplichters die uw gegevens willen stelen. Meestal leiden zij u in die e-mail via een klik naar een website waar dan uw gegevens ingevoerd moeten worden. Die NEP-website kan best het juiste bedrijfslogo en kleuren worden gebruikt en ook de teksten zullen professioneel overkomen. Bedrijven zoals banken zullen u echter nooit op deze wijze benaderen voor uw gegevens. Het hoeft trouwens niet alleen via e-mail gevraagd te worden maar het kan ook een instant message of een popupvenster op Internet zijn. Als u een dergelijke phishing ontdekt is het verstandig om het ECHTE bedrijf daarvan op de hoogte te stellen.

#### **Hoe herkent u een phishingmail**

- Financiële gegevens  
Dit zijn de meest voorkomende zogenaamd uit naam van een financiële instelling, zoals een bank, online betaaldienst of handelsplaats op internet. Deze bedrijven zullen nooit op deze wijze om uw gegevens vragen.
- Persoonlijke gegevens  
Ook kan een zeer dringend verzoek gedaan worden om persoonlijke financiële informatie door te geven, zoals een pincode, sofinummer, creditcardgegevens of wachtwoord. Deze bedrijven zullen nooit op deze wijze om uw gegevens vragen.
- Haast geboden  
De oplichters willen een snelle reactie anders wordt uw account of toegang opgeheven of dat u een zeer aantrekkelijke aanbieding misloopt, als u niet snel reageert.
- Slordig taalgebruik  
In Nederlandstalige phishing zitten vaak spelfouten of stijlfouten, het resultaat van een slechte vertaling uit het Engels ("lieve klant"). Een dergelijke commerciële e-mail met dergelijk taalgebruik zal (bijna) zeker phishing zijn
- Onpersoonlijk  
Als u niet persoonlijk wordt aangesproken zullen de berichten in grote hoeveelheden zijn verzonden en dus niet van een betrouwbare instantie afkomstig. Die zullen u op zijn minst aanspreken met mevrouw/mijnheer, uw achternaam en eventueel ook uw voorletters.
- Andere links  
Oplichters vragen u in de e-mail op een, al dan niet gecamoufleerde, link te klikken en u komt ergens anders uit dan verwacht. Meestal een ontzettend goed gelijkende website zodat u niet direct argwaan krijgt. Zelfs de aanduiding "https://" in het internetadres (met de "s" van secure) en het gele hangslotje kunnen oplichters tegenwoordig namaken. Dus niet zomaar op een link klikken, liefst zelf het internetadres in uw adresbalk intypen.
- Bijlagen  
Deze nooit openen, het kunnen meegestuurde programma's of documenten zijn die een virus of spyware bevatten. Of zelfs automatisch naar een online formulier gaan.
- Twijfel

Bij twijfel kijkt u op de website van het bedrijf onder wiens naam de e-mail is verstuurd: vaak zal het bedrijf al heel snel bekend maken dat het is getroffen door phishing. Als u op de website (nog) niets kunt vinden, bel dan gewoon naar het betreffende bedrijf.

- Toch de dupe  
Bent u toch in een phishing email getrap, neem dan direct contact op met de betrokken instantie.

**De enig juiste remedie: Wees attent en hap niet!**

### **Veilig Internetbankieren**

Ter voorkoming van Phishing moet u voor Internetbankieren letten op een aantal aspecten, zie hiervoor de website [www.3xkloppen.nl](http://www.3xkloppen.nl). De vragen die daar gesteld worden moet u kunnen beantwoorden, samengevat kunt u veilig op Internet werken als u:

- De Windows updates zijn doorgevoerd (automatische updates aan);
- De Firewall actief is; Voert u de betalingen volgens bankvoorschrift uit?
- Een Antivirusprogramma programma actief is;
- Het Antivirusprogramma automatische van updates (en upgrades) wordt voorzien;
- Uw Browser de nieuwste versie is en nieuwste updates doorgevoerd;
- De Browser beveiliging aan staat; - Is het hangslotje in browser aanwezig
- Anti-spyware, het nieuwste programma regelmatig uitvoeren
- Wees attent welke bestanden u download - Staat de naam juist in het certificaat
- Let op dat het Internetadres (URL) een S van https bevat
- Controleer de spelling van de URL - Controleer regelmatig uw bij- en afschrijvingen
- Verloopt het inloggen wel zoals altijd, geen extra tussenvragen

**Wees zorgvuldig, het zijn uw centen!**

### **Belangrijke gegevens - Cookies**

Een cookie is een klein tekstbestandje dat op de computer staat als hulp voor een website. Echt gevaarlijk zijn ze niet, ze verwijderen geen gegevens van de computer en beschadigen geen bestanden of programma's. Ze sturen ook geen geheime informatie door op de achtergrond. Het zijn immers geen programma's.

Cookies kunnen echter een gevaar vormen voor de privacy. Ze kunnen persoonlijke informatie bevatten over het surfgedrag, en mogelijk zelfs vertrouwelijke informatie zoals wachtwoorden en creditcardnummers. Daarom moeten ze toch met de nodige omzichtigheid behandeld worden. Blokkeer cookies niet helemaal omdat ze soms goed en handig zijn. Directe cookies van betrouwbare websites zullen normaal geen probleem vormen. Indirecte cookies, en cookies van dubieuze websites (die bv. wachtwoorden en creditcardnummers opslaan in cookies) kunnen wel een probleem vormen.

In Internet Explorer kunt u een standaardniveau van cookie-bescherming accepteren of het zelf bepalen door zelf de instellingen te doen. Ga in het menu *Extra* naar *Internet opties* en dan naar het tabblad *Privacy*, waarvan het bovenste deel voor cookie-instellingen is.

Met de schuifregelaar kunt u één van de voorkeurniveaus kiezen. Is de schuifregelaar niet zichtbaar, druk dan op de knop *Standaard*. Bij elke keuze wordt kort aangegeven wat dat niveau inhoudt. Dit gaat van laag (alles is toegelaten) naar hoog (alles geblokkeerd). In de stand hoog zullen een aantal zaken, zoals Webmail, niet meer werken omdat ze gebruik maken van (onschuldige) sessie-cookies. Klikt u daarna op *Websites* dan kunnen websites worden opgegeven waarvoor een uitzondering kan worden gemaakt op het, met de schuifregelaar, gekozen algemene beleid. Vul een adres in en kies *Blokkeren* of *Toestaan* voor cookies van die website. Klik *OK* om naar het hoofdscherm terug te gaan.

Kiest u (op tabblad *Privacy*) voor *Geavanceerd* dan kunt u een eigen niveau van cookie blokkering instellen. Klik dan het bovenste vinkje aan waarna een eigen instelling kan worden gemaakt voor permanente directe cookies (First-party Cookies), permanente indirecte cookies (Third-party

Cookies, bv. van adverteerders) en tijdelijke cookies (session cookies). Zorg in ieder geval dat sessie-cookies toegelaten zijn, voor toepassingen als webmail.

Cookies kunt u altijd verwijderen op het tabblad *Algemeen* van de *Internet Opties* in het menu *Extra*.

### **Gegevens (incl. wachtwoorden)**

Als men uw computer eenmaal weet te benaderen zijn uw opgeslagen gegevens ook niet zeker meer. Geen idee hoe ver men daarin kan gaan. Uw wachtwoorden zijn niet alleen die van uw e-mailaccount maar ook allerlei andere gegevens, inclusief wachtwoorden, die u laat opslaan door Internet Explorer. In IE7 stelt u dat in via het menu *Extra* de *Internetopties* en dan het tabblad *Inhoud* onderaan het deel *Automatisch aanvullen* de knop *Instellingen*. Om de gegevens te verwijderen gaat u naar het tabblad *Algemeen* en klikt op *Verwijderen* (onder *Browsegeschiedenis*) en kunt u uw keuze maken welke gegevens u wilt verwijderen.

### **Overige zaken - Rechten gebruiker**

Om te voorkomen dat ongewenst malware wordt geïnstalleerd of instellingen in uw register worden gemaakt is het aan te bevelen om zelf ook te werken als gebruiker met beperkte rechten. Dan namelijk kan dat niet ongewenst gebeuren.

Het nadeel is dat u wel een aparte gebruiker moet aanmaken met volledige rechten en alleen onder die gebruiker programma's kan installeren. Doe echt verder alleen systeemgerichte dingen en geen gebruikszaken omdat deze dan weer niet beschikbaar zijn voor de normale gebruiker met beperkte rechten.

### **SLOTEN**

Alle sloten en beveiligingen falen als u zelf toegang verschaft. U bepaalt namelijk zelf wat u download, installeert, laat installeren of op reageert. Net als in het dagelijkse leven is ook waakzaamheid noodzakelijk bij computergebruik.