

Viruspreventie

Bent u zich bewust van

→ **Basis**

U gebruikt uw PC/Macintosh professioneel. Uw werkt eveneens met professionele legale software. Deze combinatie is voor u een dagdagelijks werkinstrument. Indien zo belangrijk bezit u een backupsysteem en neemt u rigoureuus veiligheidskopie van uw gegevens. U heeft een software én hardware servicecontract wanneer u zich bewust bent van het belang ononderbroken te kunnen blijven werken, ook bij panne van uw toestellen! Daarom willen wij nogmaals benadrukken dat het installeren van NIET legale software door eender wie (vrienden, familie, leveranciers) een groot risico kan inhouden.

Wij als leverancier van uw systeem raden u ten zeerste af - en nemen dan ook geen enkele verantwoordelijkheid - wanneer u zomaar toelaat/beslist dat er niet professionele software geïnstalleerd wordt op uw toestel.

Spelletjes, illegale kopies, "gratis" programma's, etc zijn een onuitputtelijke bron van ergernis en problemen en prima leveranciers van virussen. Het herstellen van uw configuratie in originele staat kan u een pak geld kosten.

Wij willen u bij deze enkel bewust maken van dit risico en de bijhorende verantwoordelijkheden die daarbij samengaan.

→ **Enkele gouden regels**

- Gebruik geen opgemaakte mail of onnodige attachments.
In 97% van de gevallen volstaat een niet opgemaakte e-mail.
- wantrouw elk attachment waar je zelf niet om gevraagd hebt - ook al komt het van een afzender die je kent.
Stuur desnoods eerst een mailtje terug met de vraag of het bepaald attachment wel bewust door de afzender is opgestuurd!
- Laat Windows steeds ook de bestands-**extensies** weergeven zodat je kan zien of een attachment bijvoorbeeld een Visual Basic Script is (.vbs) i.p.v. een foto op het internet (.jpg)
- Open geen attachments zonder ze **vooraf** op virussen te scannen.
- Laat je niet verleiden door ego-strelende onderwerpen zoals "I love you" of schijnbaar gratis aanbiedingen of enorme opportuniteiten zoals "Free sex", "Great Nudes" e.d.m.
- Zorg er voor dat je een recent anti-virusprogramma op je pc hebt en gebruik het consequent - dus tot vervelens toe telkens weer die diskette scannen.

Viruspreventie

Bent u zich bewust van

→ Enkele gouden regels (deel 2)

- Zorg er voor dat de virusdefinities die je antivirusprogramma gebruikt geregeld (minstens om de maand) upgedated worden. Kijk wekelijks eens op onderstaande link om na te gaan of er ondertussen geen dringender actie te ondernemen is.
- Zorg er voor dat je anti-virus programma **alle** files scant (en niet slechts een deelverzameling!)
- Schakel in je Internetbrowser het automatisch uitvoeren van Java en Active-X applets uit. Als het voor het raadplegen van een bepaalde site niet anders kan, heb je nog steeds de mogelijkheid om dit tijdelijk aan te zetten. Wees er u echter van bewust dat Active-X subroutines desnoods uw hele harde schijf kunnen wissen!
- Zorg dat je een "RESCUE ANTI-VIRUS BOOT DISKETTE" ter beschikking hebt. Elk goed anti-virus programma moet u toelaten een dergelijke diskette aan te maken voor in het geval de bootsector van uw harde schijf door een virus is aangetast. Je moet deze diskette uiteraard aanmaken **vooraleer** je harde schijf aangetast is.
- Laat ook elk bestand dat je van het Internet download eerst scannen op virussen vooraleer je deze bestanden opent of installeert. Ook al heb je dit van een "gerespecteerde" site gedownload (er zijn ondertussen voldoende gevallen bekend van goed-gekende sites die toch (weliswaar tijdelijk) virussen bevatten)
- Maak geregeld back-up's (veiligheidskopieën) van je belangrijkste bestanden.
- Maak uw eigen diskettes "write protected" als je ze doorgeeft aan iemand anders, en scan ze toch nog als je ze terug krijgt.
- Schakel de automatische uitvoering van macro's van Microsoft documenten uit als je deze bestanden niet zelf aanmaakte.
- Als je een permanente on-line verbinding met het Internet hebt, of je hebt een vast IP-adres, installeer dan ook een **FIREWALL**. Dit is beveiligingssoftware/hardware waarmee je verhindert dat men via het Internet ongevraagd je pc komt binnendringen om bijvoorbeeld, achter de schermen, je eigen pc als server van porno-plaatjes of illegale mp3-bestanden te laten gebruiken.