Computerhulp Direct
Sijmonsweijde 2 - 1704MP HEERHUGOWAARD
Tel.: 072-5316763 - E-mail: info@computerhulpdirect.nl
IBAN-rekeningnummer: NL09 RABO 0162 4739 23 - BTW-nummer: NL001259838B55 - KvK Alkmaar: 53550137

# Een vijftal essentiële computertips

**Tip 1: Wees kritisch op welke websites u bezoekt!**

Het internet is ongekend groot, en onder de miljoenen websites bevinden zich ook grote aantallen schadelijke websites. Wees daarom altijd oplettend, ook al ziet een website er netjes uit. Diverse beveiligingspakketten bieden al waarschuwingsmogelijkheden die u helpen om schadelijke sites te vermijden.
Twijfelt u over de betrouwbaarheid van een site, vul de naam van de website dan eens in op een zoekmachine en kijk rond wat u op andere sites over deze website vindt. Dat kan u helpen in het beoordelen van de veiligheid van deze website.
Wees uiterst voorzichtig met het verstrekken van persoonlijke informatie aan partijen die u niet kent. Doet u aankopen en/of betalingen via internet, let dan op, of de pagina waarop u betalingen doet, beveiligd is: In plaats van 'http' staat er bij beveiligde pagina's 'https' > de s van secure (= extra beveiligd!) is hier dus toegevoegd!

**Tip 2: Wijzig regelmatig wachtwoorden!**

Veel toepassingen zijn te beveiligen met wachtwoorden. Het is verstandig deze wachtwoorden regelmatig te veranderen en daarbij niet al te voor de hand liggende wachtwoorden te kiezen. Bijvoorbeeld de naam van uw partner of uw verjaardag zijn relatief eenvoudig te achterhalen. Kies daarom een wachtwoord dat voor anderen niet zomaar te raden is, en combineer letters en cijfers, kleine letters en hoofdletters.
Wees ook voorzichtig met het gebruiken van één wachtwoord voor meerdere toepassingen: Stel dat uw wachtwoord in verkeerde handen valt, dan is het het beste als men er zo weinig mogelijk schade mee kan aanrichten. Pas op met het opslaan van wachtwoorden op uw pc of het laten 'onthouden' van wachtwoorden door uw pc. Immers: Iedereen heeft zo rechtstreeks toegang tot uw privé-informatie. Laat u bijvoorbeeld uw outlook- of gmail-wachtwoord onthouden door de browser, dan kan iedereen die op uw pc naar de website van outlook of gmail surft, zonder moeite doorklikken naar uw inbox!

**Tip 3: Let op welke e-mails u opent!**

Veel bedreigingen verspreiden zich via e-mail. In veel gevallen zijn dergelijke besmettingen in staat zichzelf door te sturen via e-mail, en daarbij zelfstandig e-mailadressen te gebruiken uit het adresboek (de contactpersonen!) van de besmette pc. Het kan dus zijn dat u mails ontvangt die afkomstig (lijken te) zijn van het e-mailadres van een goede bekende, maar wel degelijk onveilig zijn. Wees daarom bij het openen van e-mails, en zeker bij daarbij meegestuurde bijlagen, altijd heel kritisch. Let bijvoorbeeld goed op de onderwerpregel van de mail. Is die in het Engels, terwijl u en de bekende afzender altijd in het Nederlands communiceren? Of gaat de mail over het winnen van prijzen, terwijl u de afzender goed genoeg kent om te weten dat deze dergelijke mails normaal gesproken niet zou doorsturen? Neem dan het zekere voor het onzekere, en open de mail niet!

**Tip 4: Wees voorzichtig met wat u downloadt!**

Het klinkt als het intrappen van een open deur, maar toch is het iets wat al te vaak mis gaat. U bent naar iets op zoek, vindt het, en in uw enthousiasme hebt u voor u het weet een bestand of programma gedownload, dat zomaar eens schadelijk zou kunnen zijn. Wees daarom kritisch op het feit, van welke sites u downloadt. Installeer downloads niet rechtstreeks, maar scan het gedownloade bestand eerst op virussen, mal- en spyware voordat u het gaat installeren. Als u twijfelt over de betrouwbaarheid van een download of website: Google dan eerst eens om te zien of u ervaringen van andere gebruikers kunt achterhalen. Vaak zeggen die genoeg!

**Tip 5: Maak geregeld back-ups van uw waardevolle bestanden en images van uw systeem!**

Het beschadigd raken van de juiste werking van uw systeem en het verliezen van uw waardevolle bestanden, is dikwijls een ramp! Zorg er daarom voor dat u regelmatig een reservekopie (= back-up!) maakt. Mocht uw systeem dan tóch besmet raken, dan bent u er zeker van dat u alles kunt herstellen met 'schone' kopieën.
Voor back-ups kunt u gebruik maken van verschillende software en opslagbronnen (dvd's, usb-sticks, externe harddisks, maar ook bijvoorbeeld online opslagruimte!). Alles kan, zolang het maar een opslaglocatie is die los staat van uw desk- of laptop. Voor de veeleisende thuisgebruiker, is er tegenwoordig ook nog een andere handige oplossing: Werken met een zgn. 'NAS' (meerdere harde schijven, die via uw thuisnetwerk met uw computer(s) verbonden zijn!
Ook bij dit gegeven kan Computerhulp Direct u qua advies en hulp uitstekend van dienst zijn. Middels een extra investering in wat hard- en software, zijn dergelijke processen geheel te automatiseren!