Voorkomen van nieuwe infectie na een besmetting.

Spyware- en virusinfectie's kunnen nooit uitgesloten worden. Men kan wel het risico beperken om besmettingen te voorkomen met onderstaande tips.
Meestal treed een nieuwe infectie op , omdat de beveiligigingsinstellingen te laag ingesteld staan.

Windows Updates.

De meeste besmettingen gebeuren via Windows beveiligingslekken . Zorg daarom dat je windows altijd is bijgewerkt met de recentste updates. Stel de Windows en Microsoft Updates zo in dat ze altijd automatisch gebeuren. Laat daarom de updates automatisch downloaden en installeren.
Controleer ook regelmatig of er nieuwe updates beschikbaar zijn op de site van Microsoft.
Wanneer er nieuwe updates beschikbaar zijn download ze en installeer alle essentiële updates en eventuele servicepack's als deze nog niet geïnstalleerd zijn. Herstart de computer en voer nog eens een controle uit of alle nodige essentiële updates geïnstalleerd zijn. Voer deze bewerking uit tot er geen essentiële updates meer beschikbaar zijn. Op deze wijze ben je zeker dat je altijd over de laatste updates beschikt.

Veilig surfen.

Vermijd het bezoeken van verdachte en dubieuze sites. Een bezoek aan een verdachte of dubieuze site kan al voldoende zijn om je computer te infecteren.
Maak altijd gebruik van sterke wachtwoorden wanneer je jou ergens registreert. Een combinatie van hoofd- en kleine letters, vreemde tekens en cijfers. De kans bestaat nog altijd dat je wachtwoord(en) kan gekraakt worden, maar zal hierdoor veel kleiner zijn.
Verzin ook antwoorden op beveiligingsvragen. Niet de beveiligingsvraag is belangrijk, maar het antwoord op de beveiligingsvraag is belangrijk. Geef daarom een sterk antwoord op de beveiligingsvraag dat niets met de beveiliginsvraag te maken heeft.
Voorbeeldje van beveiligingsvraag : Wat is mijn lievelingshuisdier.
Antwoord op de beveiligingsvraag : rode kool met worst.
Wees ook zeer voorzichtig wanneer je iets gaat downloaden. Vooral via P2P- en freesoftware sites word het meest spyware verspreid. Zorg ervoor dat de linkscanner van je antirussoftware ingesteld staat.
Ga nooit op plots verschijnende popups klikken van onbekende antivirussoftware of systeemsoftware die waarschuwingen geven dat het systeem besmet is of systeemfouten bevat. Raak vooral niet in paniek , maar voer onmiddelijk taakbeheer uit , als dit mogelijk is.

Dit doe je door tegelijkertijd de CTRL + ALT + DELETE toets in te drukken en kiezen voor taakbeheer.
Of door tegelijkertijd de CTRL + SHIFT + ESC toets in te drukken.
Of door met met rechtermuisklik in een leeg gebied van de taakbalk te klikken en kiezen voor taakbeheer.
Selecteer in taakbeheer "Toepassingen" en beëindig alle taken.

Instellingen Internet Explorer.

Belangrijk is om de ActiveX beveiligingsinstellingen in je Internet Explorer te verhogen. Dit omdat wanneer Internet Explorer een ActiveX element uitvoert er een programma gestart word.
Breng in Internet Explorer onderstaande aanwijzingen aan.
Ga naar het menu Extra > Internet opties > Beveiliging > Internet en klik bij Aangepast niveau.
Bij ActiveX - besturingselementen- en invoegtoepassingen breng de volgende onderstaande instellingen aan.

- ActiveX-besturingselementen met handtekening downloaden: Vragen
- ActiveX-besturingselementen zonder handtekening downloaden: Vragen
- ActiveX elementen die niet zijn gemarkeerd als veilig initialiseren en uitvoeren in scripts: Uitschakelen

Vanaf nu zal eerst gevraagd worden of ActiveX elementen mogen uitgevoerd worden.
Sites die je helemaal vertrouwd kunnen aan de beveiligde zones toevertrouwd worden op deze wijze : Extra > Internetopties > Beveiliging > Vertrouwde Websites.
Controleer ook of je van de laatste Internet Explorer gebruik maakt. Hier vind je meer informatie.

Vooraleer op een link te klikken in een webpagina , controleer eerst naar welke pagina of site je doorgelinkt word. Ga niet onmiddelijk op de link klikken, maar ga met de muisaanwijzer op de verborgen link staan.
Links onderaan in je scherm kun je dan de volledige link lezen en controleren , naar welke site en pagina je doorgelinkt zal worden. In besmette sites kun je bij verborgen linken, doorverwezen naar malafide of dubieuze sites, met de gevolgen vandien, wanneer zomaar op de verborgen link geklikt word.

Veilig e-mailen.

Open nooit bijlagen in een e-mail bericht , als de afzender je onbekend is.
Beantwoord ook nooit e-mails waarin je gebruikersnaam en wachtwoord word gevraagd.
Ook bijlagen van bekende personnen zoals vrienden, familie enz.... kunnen soms besmet zijn, zonder deze mensen er iets van afweten. Voor de bijlage te openen, sla ze eerst op en controleer ze op mogelijk aanwezige malware. Dit doe je door rechts op het opgeslagen bestand te klikken , en dan kiezen voor "scannen met" , en scan de bijlage met je antivirussoftware en antispyware software.

Verouderde software.

Niet alleen je Windows besturingssysteem moet Up to date ziijn, maar ook je andere geïnstalleerde software. Malwareverspreiders zoeken niet enkel naar computers waarvan het besturingssysteem niet Up to date is, maar ook naar computers waarvan de andere geïnstalleerde software niet Up to date is.
Voorbeelden hiervan zijn Apple Quicktime Player, Adobe Flash Player, Adobe Reader , Java enz.....
Het is daarom dan ook zeer belangrijk dat altijd de laatste versies van deze software geïnstalleerd staan.
Een nuttig programmaatje hiervoor is Secunia Online Software Inspection. (OSI).
Secunia Online Software Inspection scant de computer op software die niet Up to date is , die hierdoor beveiliginslekken kunnen hebben , en door allerhande soorten malware kunnen misbruikt worden.
Voor de scan te beginnen, plaats een vinkje bij "Enable thorough system inspection". Hiermee kan Secunia ook programma's vinden die op de standaardlocatie niet geïnstalleerd zijn.
Als er een programma gevonden word dat niet Up to date is , word dit in het rood gemarkeerd onder "Insecure" en krijg je de mogelijkheid via de "download link" de recentste versie van het programma te downloaden.

Scan regelmatig je computer naar mogelijke malware.

Voer wekelijks een snelle scan uit met je antivirus- en antispyware software.
Voer maandelijks een volledige scan uit met je antivirus- en antispyware software.
Stel je antivirus zo in dat deze taken automatisch uitgevoerd worden, wanneer je

computer aanstaat.
Zorg er ook voor dat je beveiligingssoftware altijd is bijgewerkt met de laatste definities. Stel je beveiligingssoftware in, dat de updates automatisch gebeuren.
Stel je antivirus in dat eerst de bootsector word gescant , voor het besturingssysteem word opgestart. Liever een minuutje langer wachten , dan dat de computer niet meer zou opstarten.

Handleiding gemaakt voor pctuts.be