

Internet, risico's en veiligheid

Verkleinen kans op virussen/ransomware

Hieronder kan je een aantal tips vinden, om de kans op virussen/ransomware zo klein mogelijk te houden.

Standaard voorzorgmaatregelen

1. Zorg te allen tijden dat je een backup hebt op een veilige locatie!
2. Houd je software up-to-date;
3. Zorg voor een goed Antivirus pakket (inclusief webprotectie);
4. Open geen e-mails, links in e-mails en zeker geen bijlage(n) van onbekende afzenders;
5. Open ook geen e-mails, links in e-mails en bijlage(n) die u eigenlijk niet verwacht, ook al is de afzender bekend.

De meeste virussen die in omloop zijn, worden via een e-mail verstuurd.

Denk bijvoorbeeld aan een e-mail van KPN met een factuur.rar als bijlage.

Hieronder vindt je een aantal opties, hoe je makkelijk kunt herkennen of een e-mail veilig is.

1. Als een factuur wordt verstuurd, staat er altijd een aanhef in de mail
Voorbeeld: Geachte heer "Achternaam".
2. Als alleen Geachte heer/mevrouw staat, kan je er bijna vanuit gaan dat de mail niet veilig is.
3. Als er een factuur wordt verstuurd, zal er altijd een pdf bijgevoegd zijn in de bijlage.
Voorbeeld: factuur.pdf
Als er een **.rar, .zip, .docx, .txt enz** is bijgevoegd als bijlage, dan is dit geen veilige e-mail.
4. Regelmatig wordt er in een e-mail ook een link bijgevoegd, waarmee je bijvoorbeeld kan inloggen op uw bank.
Hieronder wordt er vaak doorgeleid naar een andere URL (website) dan dat op het eerste oog zichtbaar is.
Dit is makkelijk te controleren door alleen de muis op de link te houden (**Let op! niet erop klikken.**)
Onderaan het venster komt er een balk tevoorschijn, met de website waar daadwerkelijk naartoe verwezen wordt.
5. Twijfel je of de mail veilig is?
Neem dan altijd contact op met de afzender (bijvoorbeeld KPN, ING etc.).

Unieke FAQ ID: #1724

Auteur: Helpdesk

Laatst bijgewerkt: 2017-07-05 10:22