Beveiligd mailen

Sinds de invoering van de ‘Algemene Verordening Gegevensbescherming’ (AVG) komt tijdens visitaties het onderwerp ‘Beveiligd mailen’ vaak ter sprake.

Wellicht verstuur je, als therapeut of coach, dagelijks gewoon e-mails die betrekking hebben op een behandeling of die een factuur bevatten. Maar is dit wel zo gewoon? Nee, eigenlijk moet dit soort mailverkeer op een beveiligde manier worden verzonden.

Waarom eigenlijk beveiligd mailen? Is dit eigenlijk noodzakelijk? En welke gevaren liggen er op de loer wanneer de e-mailbeveiliging te wensen over laat?

De risico’s hebben vooral te maken met de weg die een e-mailbericht aflegt van het opstellen ervan door de verzender tot het openen ervan door de ontvanger. Een verzonden e-mail komt als eerste aan bij de Internet Service Provider (ISP) van de verzender. De e-mail gaat vervolgens langs diverse e-mailservers, voordat hij terecht komt bij de ISP server van de ontvanger. Doordat de e-mail op vrijwel alle tussenliggende servers (tijdelijk) wordt opgeslagen, blijft er op de weg van zender naar ontvanger informatie achter. Om te voorkomen dat de inhoud met bijlage van een e-mail op de tussengelegen servers te lezen is, kunnen e-mails versleuteld worden.

En nu … wat kun jij hieraan doen? Gewoon de ouderwetse postduif gaan gebruiken?

Nee, gelukkig bieden een aantal e-mail leveranciers, zoals Microsoft en Google, reeds de mogelijkheid om een mail versleuteld te versturen. Ook zijn er andere wel of niet gratis e-mail softwarepakketten beschikbaar, die mails versleuteld kunnen versturen. Enkele voorbeelden zijn: Zivver, Protonmail of Tutanota.

Beveiligd mailen? Ja, maar maak zelf de keuze met welk softwarepakket. Wacht hier niet te lang mee. Immers voorkomen is beter dan genezen.

Met vriendelijke groet,

Piet Offermans