Hoe herken ik een **phishing e-mail?**

Het goed kunnen afwegen of je een e-mail veilig kunt openen is makkelijker gezegd dan gedaan. Het is vaak erg moeilijk om valse e-mails te herkennen, vooral als het gaat om gerichte aanvallen. Hier vind je een aantal adviezen om mogelijke valse e-mails te herkennen.

Een phishing e-mail ontvangen?

Vermoed je een dergelijke mail te hebben ontvangen? Meld dat altijd bij de IT-helpdesk van jouw school.

Deze infographic (tekst & concept) werd mede mogelijk gemaakt door het Vista College.

Afzender

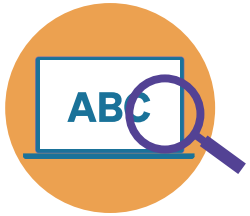
Controleer het adres van de afzender. De domeinnaam is te herkennen aan alles wat achter het @-teken in het e-mailadres staat en check of deze overeenkomt met het websiteadres.

Aanhef

Word je met heel algemene termen, zoals 'Geachte heer/mevrouw' of 'Beste klant', aangesproken, let dan op.

Persoonsgegevens

Klik NOOIT op een link om je persoonsgegevens te controleren of in te voeren.



Taalgebruik & vormgeving

Let op Engelstalige mails of mails in gebrekkig Nederlands. Maar wees je er ook van bewust dat de kwaliteit van de e-mails steeds beter wordt. Ook de gebruikte logo's en foto's worden steeds professioneler. Ben dus extra alert.

Bijlagen

Open nooit zomaar een bijlage van een e-mail die je niet vertrouwt. Vaak gaat het over de attached invoice en pakketten die bezorgd gaan worden. Een zip of rar-bestand is altijd verdacht, omdat bijvoorbeeld facturen en aanmaningen nooit op deze manier worden verstuurd. Verwacht je toch een bestand? Neem dan contact op met de afzender om te vragen wat en hoe ze iets precies verstuurd hebben.

Spoed of laatste waarschuwingen

Valse mailtjes proberen je onder druk te zetten door gebruik te maken van laatste waarschuwingen of spoedmeldingen.

mbo digitaal