Herken phishing e-mails

Phishing e-mails zijn in de meeste gevallen gemakkelijk te herkennen. Neem bijvoorbeeld een nep-mail die van de Rabobank af lijkt te komen waarin staat dat jouw bankpas is geblokkeerd. **Logisch nadenken** is dan al genoeg om jezelf en je bedrijf te beschermen. Phishingmails kunnen echt lijken. Het is daarom slim om altijd een e-mail op onderstaande punten te controleren. Wel zo veilig!

Controleer de afzender

Als de afzender het adres @rabobank.vestiging-205.nl gebruikt, weet je dat de e-mail niet door de Rabobank is verstuurd. Dan zou er mail.rabobank.nl of rabobank.nl staan. Als dat niet het geval is, **informeer** de IT-afdeling en volg de instructies op, **klik niet** op links in de e-mail en tot slot **verwijder** de e-mail.

Inspecteer altijd de links

Dit doe je door met je muiswijzer boven de link te “hangen“ zonder erop te klikken. Zo zie je het adres waar de link je naartoe wil sturen. Meestal weet je of het om phishing gaat of niet. Op je smartphone druk je lang op de link om deze te kopiëren. Vervolgens kun je deze bijvoorbeeld in een nieuwe e-mail plakken om de volledige URL te zien.

Controleer de weergavenaam (CEO-fraude)

Een veel voorkomende phishing-taktiek bij criminelen is om de weergavenaam van een e-mail te vervalsen. Dit is zeer eenvoudig te herkennen door de domeinnaam van de afzender te controleren. Klopt dit niet, **informeer** de IT-afdeling en volg de instructies op, **klik niet** op links in de e-mail en tot slot **verwijder** de e-mail.

Bel voordat je geld overmaakt

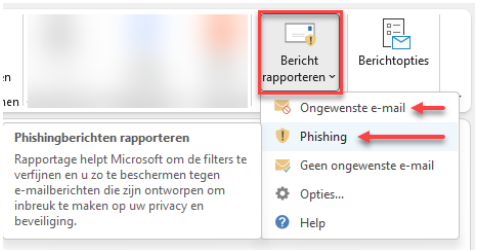
Er wordt helaas nog steeds vaak betaald aan criminelen. Dit is eenvoudig te voorkomen wanneer bijvoorbeeld je baas je een mailtje stuurt, dat er met **spoed** geld overgemaakt moet worden aan een relatie, je toch even de telefoon pakt en dit verifieerd en niet zomaar geld overmaakt. Je kunt dit namelijk niet meer terughalen. Ook banken vergoeden de schade **niet**.

Laat je niet verleiden door urgentie en spelfouten

Echte e-mails van bedrijven of van jouw collega/manager/eigenaar gebruiken **jouw naam** in de aanhef. Phishing e-mails hebben meestal een algemene aanhef, zoals “Beste klant” of “Geachte heer/mevrouw”. Daarnaast bevatten phishing e-mails vaak taalfouten, gebrekkige formuleringen of onlogische zinopbouw. Laat je tot slot **niet** onder druk zetten.

Wat **wel** te doen

1. Klik nooit zomaar op links
2. Informeer de IT-afdeling
3. Rapporteer en verwijder de e-mail
4. Betaal nooit
5. Geeft nooit persoonlijke informatie
6. Gebruik je gezond verstand



M·IT SERVICES