Cyber
Weerbaarheidscentrum
Greenport

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. Hieronder vind je een aantal adviezen om mogelijke valse e-mails te herkennen.

Afzender

- Controleer het adres van de afzender. De naam van de afzender mag dan precies hetzelfde zijn als die van je bank of webwinkel, maar vaak is het gebruikte e-mailadres vaag of een afgeleide versie van een echte bedrijfsnaam of de naam van een instantie.
- Kijk goed naar de domeinnaam waarvan je de e-mail hebt ontvangen. De domeinnaam is te herkennen aan alles wat achter het @-teken in het e-mailadres staat.
- Controleer of het e-mailadres ook echt overeenkomt met het websiteadres. Een veel gebruikte manier om valse e-mails te verspreiden is namelijk het vervangen van bepaalde letters uit de domeinnaam door cijfers.
- Het verschil tussen een legitiem en vals e-mailadres kan soms moeilijk te onderscheiden zijn. In het volgende voorbeeld is 1 (cijfer) vervangen door een I (letter). Vergelijk mail@31008mailers.nl en mail@3I008mailers.nl.

Aanhef

Bedrijven en instanties waar je klant bent of zaken mee doet gebruiken in ieder geval je achternaam in een e-mail, of weten of je een man of een vrouw bent. Word je met heel algemene termen, zoals 'Geachte heer/mevrouw' of 'Beste klant', aangesproken, let dan op.

Vragen naar persoonsgegevens

In veel nepmails staat het verzoek om je persoonsgegevens 'te controleren', 'bij te werken' of 'aan te vullen'. Je moet dan op een link klikken om dit te doen. Doe dit nooit zomaar. Je bank, verzekeringsmaatschappij en overheidsinstanties vragen nooit op deze manier naar persoonsgegevens.

Bel het bedrijf of de instantie eerst op om te controleren of ze de e-mail wel zelf hebben verstuurd. Gebruik hiervoor nooit de contactgegevens in de e-mail, maar zoek deze zelf op.

Taalgebruik en vormgeving

De huidige generatie nepmails staan allang niet meer bol van de taal- en spelfouten. Ook de gebruikte logo's en foto's worden steeds professioneler. Lees en bekijk de e-mail goed om te zien of je toch geen onregelmatigheden tegenkomt. Je kunt ook een eerdere mail van een bedrijf of instantie ernaast leggen ter vergelijking.

Spoed of laatste waarschuwingen

Veel valse mailtje proberen je onder druk te zetten door gebruik te maken van laatste waarschuwingen of spoedmeldingen. Een voorbeeld van een dergelijk bericht is bijvoorbeeld "Uw hostingpakket verloopt, als u vandaag bedrag x niet overmaakt zal uw website worden geblokkeerd". Ga hier niet via de e-mail op in maar neem bij twijfel telefonisch contact op met de hostingpartij.

Links

Links in nepmails kunnen ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd of leiden je naar een valse website. Klik dus nooit zomaar op de links in een e-mail die je niet vertrouwt.

Controleer het adres van de link door, zonder erop te klikken, de cursor van je muis op de link te zetten en te kijken welk adres er verschijnt.

Link-verkorters

Vaak worden lange links verkort met diensten als bijvoorbeeld T.co, bit.ly en Goo.gl. Erg handig, maar voor jou als ontvanger erg belangrijk om hier waakzaam op te zijn aangezien het lastig is om te achterhalen waar je nu precies op klikt en naar toe wordt geleid.

Bijlagen

Een bijlage in een nepmail kan ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd. Open dus nooit zomaar een bijlage van een e-mail die je niet vertrouwt.

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.

Gebruik hiervoor nooit de contactgegevens in de e-mail, maar zoek deze zelf (bijvoorbeeld via de website) op.

Hoe weet je of een e-mail te vertrouwen is? Let op bepaalde kenmerken! Zie de Phishing Bingo kaart hieronder!

Dit document is gebaseerd op het document ‘Hoe herken ik een phishing e-mail?’ van het Digital Trust Center. De originele bron is te vinden via https://www.digitaltrustcenter.nl/informatie-advies/phishing/hoe-herken-ik-een-phishing-e-mail


PHISHING BINGO
Hoe weet je of een e-mail te vertrouwen is? Let op onderstaande kenmerken. Hoe meer van deze kenmerken van toepassing zijn, hoe groter de kans dat het een phishingaanval is.
E-mail van bank of overheid
Veel phishingaanvallen gebeuren in naam van een bank of overheid, zoals de Belastingdienst of DigiD.
"Klik hier om in te loggen"
Wees altijd alert bij e-mails met links. Vermijd links door zelf naar de betreffende website te gaan.
"Er gaat iets verlopen"
Let goed op als dit in de e-mail staat. Het kan een tactiek zijn om je op te haasten zodat je minder alert bent.
"Let op! belangrijk"
Met deze tekst kunnen kwaadwillenden je op het verkeerde been proberen te zetten. Wees dus waakzaam.
"Spoed" of "urgent"
Wees bij deze woorden altijd waakzaam en laat je niet opjagen, waardoor je fouten gaat maken.
Uitroepteken bij e-mail
Een collega kan urgentie aan een e-mail geven door een (rood) uitroepteken aan de e-mail te geven. Phishingoplichters maken hier ook gebruik van.
Geen persoonlijke aanhef
Een belangrijke e-mail bevat vaak een persoonlijke aanhef. Zo niet dan kan dit duiden op een phishingaanval.
Afzender e-mailadres ziet er vreemd uit
Check altijd het e-mailadres van de afzender. Ziet dit er anders uit dan je gewend bent, bel diegene dan even.
Onverwacht verzoek van een bekende
Krijg je een apart of onverwacht verzoek van een bekende? Check dit dan even na. Dit kan oplichting zijn (spoofing).
Offerte of factuur als bijlage
Bijlagen (bijvoorbeeld PDF's of Word-documenten) worden vaak gebruikt om malware te installeren. Wees dus kritisch bij het openen hiervan.
Taalfouten
Hoewel dit steeds minder wordt, bevatten veel phishingberichten nog taalfouten en slordigheden.
Actueel wereldnieuws
Vaak worden actualiteiten gebruikt in phishingcampagnes, zoals nep-coronaberichten die van de overheid lijken te komen.
Meer weten over phishing? Kijk op www.digitaltrustcenter.nl
digital trust center.