Hoe herken je phishingmails?

Het is vaak lastig om het verschil te zien tussen een valse en echte e-mail. Je herkent een phishingmail aan de volgende kenmerken:

Afzender

Let goed op het e-mailadres van de afzender. De gebruikte naam van de afzender onderaan de mail kan sterk lijken op die van bijvoorbeeld je bank of webwinkel, maar toch nep zijn. Criminelen gebruiken een vreemd e-mailadres of een afgeleide versie van een echte bedrijfsnaam. Check daarom de domeinnaam in het e-mailadres. De domeinnaam herken je aan alles wat achter het @-teken staat. Kijk of de domeinnaam overeenkomt met het websiteadres. Een andere

veel voorkomende manier om valse e-mails te verspreiden is het vervangen van letters uit de domeinnaam door cijfers.

Onpersoonlijk

Vervalste e-mails zijn meestal niet persoonlijk aan jou gericht. Let goed op e-mails die beginnen met een algemene aanhef zoals ‘geachte klant’ of ‘geachte heer, mevrouw’.

Taalfouten

Phishingmails bevatten vaak stijl- en taalfouten. Check het bericht daarom goed op slordig taalgebruik.

Spoed

In phishingmails probeert de oplichter je onder druk te zetten. Bijvoorbeeld door gebruik te maken van urgentie, in de vorm van tekst zoals ‘laatste waarschuwing’ of ‘laatste kans’. De fraudeur zegt dat je account verloopt of dat je een speciale aanbieding misloopt als je niet direct reageert.

Persoonlijke gegevens

In nep e-mails wordt vaak gevraagd naar je persoonsgegevens. Bijvoorbeeld om deze ‘te controleren’ of ‘te actualiseren’. Je moet dan op een link klikken om dit te doen. Wees alert en doe dit niet zomaar. Banken, creditcardmaatschappijen en overheidsinstanties vragen nooit via een bericht naar persoonlijke gegevens. Neem telefonisch contact op met de organisatie die de e-mail heeft verstuurd. Gebruik hiervoor niet de contactgegevens in de e-mail, maar zoek deze zelf op.

Schadelijke link of bijlage

Klik nooit zomaar op links of bijlagen in een e-mail die je niet vertrouwt. Links of bijlagen in valse e-mails kunnen ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd. Of ze leiden je naar een nepwebsite waar je persoonlijke gegevens moet achterhalen. Wil je zien naar welke webpagina een link leidt? Zweef met het muispijltje boven een link. Vlak boven de muiscursor verschijnt het webadres waarnaar de link verwijst.

Phishing via social media

Fraudeurs sturen phishingberichten niet alleen per e-mail. Ze gebruiken ook andere kanalen waar ondernemers actief zijn. Via sms-berichten en social media zoals WhatsApp en LinkedIn verspreiden criminelen nepberichten.

Phishing WhatsApp

WhatsApp-fraude is in 2020 sterk toegenomen, vooral door nepberichtjes in de persoonlijke sfeer, ook wel 'vriend-in-noodfraude' genoemd. Reageer nooit op een WhatsApp-bericht van je 'dochter' met de vraag om bijvoorbeeld een code door te sturen of om snel geld over te maken. Neem altijd telefonisch contact op en vraag wat er aan de hand is. Ondernemers gebruiken WhatsApp ook zakelijk. Twijfel je of een appje echt is? Controleer dan via een ander kanaal bij de afzender of het bericht klopt.

Phishing SMS

Bekend zijn ook de phishing sms-berichten die oplichters versturen om achter gegevens te komen. Antwoord nooit zomaar op een sms van je 'bank' of 'creditcardmaatschappij' om je gegevens te controleren of een nieuwe code aan te vragen. Waarschijnlijk is het een nepbericht. Zodra je buiten de sms om inlogt op de webpagina van je eigen bank, zie je de werkelijke berichten van je bank. Neem bij twijfel telefonisch contact op.

Phishing met QR-code

Een nieuwe oplichterstruc is phishing met QR-codes waarmee criminelen proberen je bankrekening te plunderen. Dit werkt zo: je ontvangt een valse e-mail of brief uit naam van je bank. In het nepbericht staat dat je een nieuwe bankpas moet aanvragen of akkoord moet gaan met een nieuwe bank-app. Om dit te doen, moet je de QR-code in het bericht scannen. Deze QR-code leidt naar een phishingwebsite waar de oplichters je inloggegevens stelen. Hiermee hebben ze vervolgens toegang tot je bankrekening.

Een QR-code bestaat uit een vierkantje dat is opgebouwd uit zwarte en witte blokjes. In die blokjes zit informatie zoals een internetadres, telefoonnummer of een betaalverzoek. Het risico is dat je voordat je scant niet weet welke informatie er in zo'n QR-code staat. Wees daarom terughoudend met het scannen van QR-codes. Zorg dat je zeker weet met wie je te maken hebt voordat je scant.

Misdadigers zoeken steeds nieuwe manieren om geld of informatie van slachtoffers te krijgen. Blijf alert op berichten die je niet verwacht, en waar 'tijdsdruk' op zit en waarin de afzender jou vraagt om informatie te geven of ergens op te klikken.