Becs Phishing Bingo

Hoe weet je of een e-mail te vertrouwen is?

Let op onderstaande 12 kenmerken die zijn vormgegeven in een bingokaart. 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 banken 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 om je op te jagen zodat je minder alert bent.

"Let op! Belangrijk"

Met deze tekst kunnen kwaadwillenden je op het verkeerde been proberen te zetten. Wees dus waakzaam.

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.

"Spoed" of "urgent"

Wees bij deze woorden altijd op je hoede en laat je niet opjagen, waardoor je fouten gaat maken.

Geen persoonlijke aanhef

Een belangrijke e-mail bevat vaak een persoonlijke aanhef. Ontbreekt dit dan kan dat 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 de afzender dan even op.

Onverwacht verzoek van bekende

Krijg je een vreemd of onverwacht verzoek van een bekende? Controleer dit dan even via een ander kanaal bij deze bekende. Het kan oplichting zijn (Spoofing).

Offerte/factuur als bijlage

Bijlagen (bijvoorbeeld PDF's of Word-documenten) worden vaak gebruikt om malware te installeren. Wees dus kritisch bij het openen van bijlagen.

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.