



Phishing bingo



Hoeveel bingovakjes kun jij afstrepen met de phishingmail die je ontvangen hebt? Heb je meer vakjes aangekruist dan je collega? Speel Phishing Bingo en trap er niet meer in.



Meer weten?
Bekijk de variatie in [phishingtechnieken](#).

Uitroepteken

Een collega kan een e-mail urgent maken door een uitroepteken aan de e-mail te geven. Cybercriminelen maken hier ook gebruik van.

“Er gaat iets verlopen”

Let goed op als dit in de e-mail staat. Het kan een tactiek zijn die ervoor zorgt dat je snel handelt en minder alert bent.

E-mailbijlage

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

Taalfouten

Hoewel dit door Generatieve AI steeds minder wordt, bevatten sommige phishingberichten nog taalfouten en slordigheden.

“Spoed” of “urgent”

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

Onverwacht of apart verzoek van een bekende of collega

Controleer dit dan even. Dit kan oplichting zijn (spoofing).

Geen persoonlijke aanhef

Als de persoonlijke aanhef ontbreekt, kan dit wijzen op phishing. Maar let op: ook een e-mail mét persoonlijke aanhef kan phishing zijn.

Let op: belangrijk!

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

Afzender e-mailadres ziet er vreemd uit

Controleer altijd het e-mailadres van de afzender. Ziet dit er anders uit dan je gewend bent? Bel diegene dan even.

Actueel nieuws

Vaak worden actualiteiten gebruikt in phishing-campagnes die van de overheid lijken te komen.

E-mail van bank of overheid

Veel phishingaanvallen gebeuren in naam van een bank of overheid, zoals de KVK of de Belastingdienst.

“Klik hier om in te loggen”

Wees alert bij e-mails met links. Vermijd links door zelf naar de website te gaan. Of zweef met je muis over de link om te zien waar deze naartoe leidt.