

PHISHING BINGO

Wie van je collega's heeft het eerst een rij, of de kaart vol?
De spelregels spreek je samen af.

Je baas vraagt je om vertrouwelijke informatie te e-mailen

Controleer bij je baas of deze informatie gevraagd heeft. Gebruik Radboud-middelen om veilig informatie te delen.

Spoed! Urgent!

Tijdsdruk kan een tactiek zijn, zodat je minder alert bent.

Maak geld over

Neem bij een onverwachts verzoek altijd even contact op met de bekende. Dit kan oplichting zijn.

E-mail van bank of overheid, vul gegevens in

Geef nooit een reactie met persoonsgegevens je wachtwoord of pincode. Hier vraagt een bank niet om.

Je account is 'gelocked', ontgrendel met persoonlijke gegevens

Trap er niet in!

Klik hier om in te loggen

Ben alert bij links. Controleer of de link echt verwijst naar de betreffende website.

Taalfouten in e-mail, app of SMS

De berichten worden steeds beter, maar blijf alert op slordigheden.

Bericht vanuit een persoonlijk adres in plaats van een werkaccount

Ziet het e-mailadres er anders uit dan je gewend bent, bel de persoon even.

Een social media verzoek van iemand met wie je al 'bevriend bent'

Gooi deze weg.

Het bericht bevat een 'vreemd' bestand om te downloaden

Vraag na of dit klopt voordat je het bestand download.

Je wint een gratis vakantie!

Nergens aan meegedaan? Dit is phishing.

Offerte of factuur als bijlage

Niks besteld. Open het bestand niet en vraag aan de afzender waar het van is.

Gemaakt door Information & Library Services

Hoe meer van deze kenmerken, des te groter de kans dat het phishing is.
Meld phishing bij de ICT Helpdesk 024-36 22222.

