

9 Tips om phishing e-mails te herkennen

Phishing is al lang een veel gebruikte methode bij hackers om gegevens van personen of bedrijven te stelen. Waar je vroeger de e-mails makkelijk herkende aan alle spelfouten of vreemde beloftes zoals erfenissen, zijn hackers steeds beter en creatiever geworden om de e-mails zo echt mogelijk te laten lijken. Hoe onderscheid je nu toch de echte e-mails van phishing e-mails?

9 Tips waar je op kunt letten!

1 Let op de bijlages

Open niet zomaar bijlages. Hackers versturen graag nepbestanden als bijlage. Een bijlage kan een Word-icoon bevatten, maar hoeft geen Word bestand te zijn.



2 Klik niet zomaar op links

Ga met je muis over links heen om te zien waar de link heen verwijst. Is dit een gekke omschrijving of website, klik er niet op.



3 Lay-out & handtekening

Betrouwbare mailings bevatten vaak een volledig handtekeningblok in de e-mail, inclusief bedrijfslogo.



4 Taalgebruik

Naast het letten op spelfouten, kijk ook naar schrijfstijl. Vraag jezelf af, past dit bij de afzender.



5 Dwingende toon

Hoe meer een afzender dwingt om iets te doen, hoe eerder het een nepbericht kan zijn. Ook tijdsdruk kan een indicatie zijn.



6 Betrouwbare site

Als je toch op een link klikt in de e-mail, kijk dan of je op een beveiligde website uit komt.



7 E-mailadres checken

Kijk niet alleen naar de displaynaam van iemand, maar ook naar het volledige e-mailadres.



8 Verwacht je e-mail?

Ontvang je e-mail van de ING terwijl je eigen bank ABN is, dan is dit hoogst waarschijnlijk phishing. Hetzelfde geldt voor postpakketten of andere leveranciers.



9 Vertrouw je intuïtie

Is iets te mooi om waar te zijn of krijg je een apart gevoel bij de e-mail, verwijder de e-mail of neem (op een andere manier dan e-mail) contact op met de afzender.

Bij twijfel, vraag een collega op je scherm mee te kijken, bel de afzender op of vraag om raad bij de IT beheerder. Stuur de e-mail niet verder door!

