VSA
Specialisten in IT

Phishing e-mail herkennen
10 dingen om op te letten

Ruim 80% van alle ransomware-aanvallen beginnen met een phishing e-mail. Het is daarom van belang om kritisch te kunnen kijken naar binnenkomende e-mail en phishing e-mails te herkennen.

1 Vertrouw niet de weergavenaam

Dat de weergegeven naam een persoon is die je kent of vertrouwt wil niet zeggen dat dat ook echt zo is. Controleer ook het e-mailadres om de echte afzender te achterhalen.

2 Wees voorzichtig met linkjes

Houd de muis erboven (zonder te klikken) en controleer of de url ook daadwerkelijk is wat je verwacht.

3 Controleer op spelling

Hackers maken zich vaak niet zo druk om de spelling of grammatica. En dit kan opzettelijk zijn om spamfilters te omzeilen.

4 Bekijk de aanhef

Is de aanhef vaag of algemeen? Bijv. "Beste [voeg naam hier]" of "Beste klant".

5 Vragen ze om persoonlijke informatie

Het is onwaarschijnlijk dat normale bedrijven of personen in een e-mail om persoonlijke informatie vragen.

6 Let op urgentie

Hackers hebben niet veel tijd, ze willen cashen voordat duidelijk is dat het mailtje phishing is. En zullen dus de nadruk leggen op urgentie.

7 Let op de e-mailhandtekening

De meeste normale afzenders hebben een normale en volledige handtekeningen blok onder aan hun e-mail.

8 Wees voorzichtig met bijlagen

Bijlagen met virussen hebben vaak een intrigerende naam die je moet aanmoedigen hem te openen, bijv.: “Hier is het overzicht, als beloofd”.

9 Geloof niet alles wat je ziet en/of leest

Als iets al enigszins afwijkend lijkt, kun je beter het zekere voor onzekere nemen.

10 Neem bij twijfel contact op met VSA

We kijken liever een keer extra met je mee om te voorkomen dat de organisatie in gevaar wordt gebracht. Bel +31 88 872 0 510.

www.vsa.nl