

Zo herkent u een valse e-mail van een deurwaarder

19-4-2019

Het televisieprogramma Radar berichtte onlangs over valse e-mails van deurwaarderskantoren. Meerdere mensen hadden een valse e-mail van gerechtsdeurwaarders ontvangen. Zij werden gedagvaard en werden gesommeerd te betalen, anders zou er beslag op de bankrekening worden gelegd. Hoe herkent u valse e-mails en hoe voorkomt u dat u het slachtoffer wordt van phishing?

Valse berichten

Bij Radar ging het om e-mails waarin werd gesteld dat de ontvanger een app zou hebben gekocht in Google Play Store, maar dat er nog steeds niet was betaald. Het bedrag was al opgelopen tot ruim 500 euro. Deze e-mails zijn afkomstig van onder meer de e-mailadressen:

- swiercs-gerechtsdeurwaarders@gmx.net
- gerechtsdeurwaarders-urgentie@advalvas.be

De Fraudehelpdesk heeft inmiddels bevestigd dat deze e-mails nep zijn. Dat is bijvoorbeeld te zien aan de buitenlandse rekeningnummers die erin staan vermeld. Ook zijn de e-mailadressen niet erg zakelijk.

Valse e-mails herkennen: vijf tips

Phishing is een verzamelnaam voor manieren waarop internetcriminelen proberen uw persoonsgegevens in handen te krijgen. Daarbij gaan ze steeds slimmer te werk. Soms zijn ze bijna niet van echt te onderscheiden. Wij zetten vijf tips voor u op een rijtje om alert op te zijn:

1. Let op het e-mailadres

Hoe echt een e-mail er ook uitziet (huisstijl en de bedrijfsnaam als afzender), het e-mailadres zelf is vaak een onduidelijk e-mailadres, bijvoorbeeld een afgeleide versie van de eigenlijke bedrijfsnaam. Controleer dus altijd het e-mailadres bij verdachte e-mails. Controleer de echte domeinnaam en kijk of die overeenkomt met die in de e-mail. Zo niet, dan is het vaak een valse e-mail. De letters i en l worden vaak gebruikt om een naam aan te passen. Als beide in hoofletter zijn geschreven, dan is het verschil slecht zichtbaar.

2. Let op de aanhef

Een bedrijf waar u klant bent, zal u altijd aanspreken met uw volledige naam. Wordt u aangesproken met algemene termen als 'Beste klant' of 'Geachte heer/mevrouw', let dan extra op.

3. Kijk uit met links

Veel nepmails bevatten een link met het verzoek om uw gegevens te controleren of bij te werken. Ook wordt er vaak gevraagd om via deze link in te loggen bij internetbankieren. Doe dit nooit, want zo krijgen internetcriminelen uw persoonlijke gegevens in handen, of toegang tot uw bankrekening. Banken, verzekeringsmaatschappijen en overheidsinstanties vragen nooit in een e-mail naar persoonsgegevens.

4. Pas op voor bijlagen

Ook het openen van een bijlage kan schadelijk zijn. Internetcriminelen kunnen in een bijlage schadelijke software meesturen die op uw computer wordt geïnstalleerd zonder dat u het merkt. Dat kan hen toegang geven tot uw inloggegevens, of zij kunnen uw computer 'gijzelen' met ransomware en losgeld eisen.

5. Twijfel? Altijd bellen!

Twijfelt u of het e-mailbericht echt is? Bel dan altijd met de instantie die deze zou hebben verzonden. Zoek hiervoor wel de contactgegevens op op de website van het bedrijf zelf en ga niet af op de informatie in de e-mail.

Gerechtsdeurwaarder nodig?

Heeft u een debiteur die niet wil betalen en wilt u een gerechtsdeurwaarder inschakelen? Onze medewerkers nemen deze zaak graag voor u uit handen. Neem contact met ons op om de mogelijkheden te bespreken.

Onze incasso en gerechtsdeurwaardersdiensten bieden wij ook aan in onder meer Soest, Veenendaal en Maarsse.