Phishing

Wat is Phishing?

Phishing is het vissen naar uw persoonlijke gegevens. Oplichters proberen gegevens zoals bankrekening- of creditcardnummers, wachtwoorden, pincodes, enzovoorts van u te bemachtigen. Daarmee proberen ze geld van uw rekening te halen. Dit heet ook wel identiteitsfraude.

Meestal krijgt u een e-mail waarin staat dat u uw account van bijvoorbeeld een bank moet checken en bevestigen. Dit met de alarmerende reden dat er iets mis is met hun of uw beveiliging. Ook wordt wel gebruikgemaakt van instant messaging, soms wordt zelfs telefonisch contact opgenomen. Fraudeurs gebruiken vaak nepsites van financiële instellingen, eBay en PayPal.

SecureOnline doet er alles aan om phishing te voorkomen. Zo sporen we phishingmails en nepsites op. Nog voordat internetcriminelen hun slag slaan, halen we nepsites uit de lucht. Helaas kunnen we niet alles voor zijn. Blijf daarom zelf ook altijd alert.

Wat kunt u zelf doen?
Controleer het adres (URL) van de website
Bij phishing wordt vaak gebruik gemaakt van URL-spoofing, dit is het nabootsen van de URL van bijvoorbeeld een bank. U denkt dan de echte site te bezoeken, terwijl het de URL van de bedrieger is. De crimineel bootst de echte domeinnaam na met, op het origineel lijkende, buitenlandse tekens. Zo merkt u niet dat het adres niet klopt. Controleer daarom altijd nauwkeurig de URL van de website.

Controleer het inlogproces
Verloopt het inlogproces van bijvoorbeeld uw bank anders dan u gewend bent? Log dan niet in en verbreek direct de verbinding.

Controleer de beveiligde verbinding
Logt u in op de website van bijvoorbeeld uw bank of gemeente? Dan gaat dat via een beveiligde verbinding. Uw browser geeft met bijvoorbeeld een hangslotje aan dat u een beveiligde verbinding heeft.

Handige links:
Waarschuwingsdienst
Veiligbankieren

Unieke FAQ ID: #1035
Auteur: n/a
Laatst bijgewerkt:2014-02-03 16:20