BINFLASH

Politie PZ Grens Essen Kalmthout Wuustwezel

Buurt-Informatie-Netwerk – Samen zorgen we voor veiligheid

Geachte Binleden,

Spijtig genoeg blijft **phishing** een actueel probleem. Een inwoner van Essen heeft gereageerd op zo'n frauduleuze mail en werd nadien telefonisch gecontacteerd door de oplichters. Hij heeft telefonisch zijn bankgegevens doorgegeven waardoor de oplichters enkele duizenden euro's konden afhalen van zijn rekening.

We kunnen niet genoeg benadrukken dat men nooit bankgegevens mag doorgeven via telefoon of e-mail.

Voor uw veiligheid: let op voor phishing

Wat is phishing?

Phishing, afgeleid van het Engelse fishing, staat voor het 'vissen of hengelen achter persoonlijke gegevens'. Phishing is een vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze te lokken naar een valse (bank)website, die een kopie is van de echte website en ze daar — nietsvermoedend — te laten inloggen met hun inlognaam en wachtwoord of hun creditcard-nummer. Hierdoor krijgt de fraudeur de beschikking over deze gegevens met alle gevolgen van dien. De slachtoffers worden vaak via e-mail naar deze valse website gelokt met daarin een link naar de (valse) website met het verzoek om zogenaamd "de inloggegevens te controleren".

TIPS

- Beschouw elke e-mail waarin men u vraagt naar uw persoonlijke gegevens of betalingen als frauduleus. Een bank zal nooit een e-mail over uw rekeningen, uw betaalmiddelen of uw beleggingen naar uw privé e-mailadres sturen.
- Controleer altijd of het website-adres van uw bank in de adresbalk bovenaan uw browser het beveiligde adres is: U herkent beveiligde adressen aan de 's' in https.
- Ga nooit in op telefoontjes waarbij de bank u zogezegd vraagt naar uw persoonlijke gegevens en/of uw elektronische handtekening (Response-code). Banken zullen dit nooit vragen!
- Zorg voor een zeer goede beveiliging van uw computer: installeer altijd de laatste updates van uw besturingssysteem en antivirusprogramma, alsook de laatste versie van uw firewall.
- Controleer geregeld uw rekeningafschriften.

Als je zo'n mail krijgt kan je o.a. contact opnemen met je eigen bank. Zij hebben procedures om dergelijke nep-websites zo spoedig mogelijk te blokkeren. Kijk ook eens op de website van Belfius-bank over phishing

Mvg

Politiezone Grens
03/620.29.29
email: info@pzgrens.be
website: www.pzgrens.be