

WAT kunt U tegen PHISHING doen?

U kunt een aantal maatregelen nemen om te voorkomen dat u slachtoffer wordt van phishing.

DOEN!

- Controleer of het uitwisselen van persoonlijke gegevens via een beveiligde verbinding plaatsvindt en uw gegevens worden beschermd: begint de adresregel met https? Is er rechts onder in het scherm een gesloten slotje of sleuteltje zichtbaar? Zo niet: wissel dan geen gegevens uit.
- Controleer de naam van het websiteadres waar in de e-mail naar verwezen wordt: staan er spelfouten in? Open anders zélf uw internetbrowser en typ zélf het adres van de website in.
- Phishing is een vorm van spam. Installeer daarom een spamfilter. Daarmee wordt de e-mail waarschijnlijk al aangeduid als ongewenste e-mail.
- Installeer een pop-up killer. Phishing gebeurt namelijk vaak door een originele site af te dekken met een pop-up, een venster dat bij het openen van een pagina ineens tevoorschijn springt.

- Wanneer u twijfelt en de website van de organisatie niets vermeldt, neem dan telefonisch contact op met de klantenservice van de organisatie die de e-mail verstuurd zou hebben.
- Waarschuw de organisatie uit wiens naam u de phishing e-mail ontvangt en doe aangifte bij de politie als u daadwerkelijk schade ondervindt.
- De nieuwste browsers bevatten een phishing filter dat het adres van elke bezochte website controleert in een centrale database. In Internet Explorer 7 kunt u dit filter inschakelen via "Extra->phishingfilter". In Firefox 2 onder "Extra->Opties-Beveiliging->

NIET DOEN!

- Reageren op verzoeken om persoonlijke informatie per e-mail of via een website. Bel bij twijfel de organisatie waar de e-mail of website van afkomstig lijkt te zijn.
- Vertrouwen op het afzendadres van de e-mail. Dit is namelijk makkelijk te vervalsen.

Meer INFORMATIE

DIGIBEWUST

Digibewust informeert over de mogelijkheden maar ook over de gevaren van digitale middelen zoals internet. Op de website vindt u informatie over veilig internetten voor uzelf, uw kinderen en uw bedrijf. Kijk op www.digibewust.nl.

WAARSCHUWINGSDIENST.NL

Via de website kunt u zich aanmelden voor het ontvangen van waarschuwingen over de nieuwste computervirussen en lekken in software.

VEILIGBANKIEREN.NL

Hier vindt u informatie over wat de bank doet om u veilig te laten bankieren.

COLOFON

Dit is een uitgave van Digibewust, een samenwerkingsverband tussen overheid en bedrijfsleven om het veilig gebruik van internet en andere digitale middelen te vergroten.



Contactgegevens:
Postbus 262, 2260 AG Leidschendam
tel 070-4190309 – fax 070-4190650
www.digibewust.nl – info@digibewust.nl

©2007, Digibewust



Nep-mails =

Phishing

Wat kunt u ertegen doen?



Het gebruik van e-mail stelt u in staat om snel en eenvoudig met familie, vrienden, collega's en zakenrelaties te communiceren. Ideaal natuurlijk!

Maar aan dit gebruik kleven soms ook nadelen. Het komt bijvoorbeeld

helaas steeds vaker voor dat mensen **E-MAILS** ontvangen die lijken te komen van betrouwbare instanties zoals een creditcardmaat-

schappij of bank, maar die in werkelijkheid afkomstig zijn van

OPLICHTERS. Nep-mails dus. Deze oplichters proberen uw

persoonlijke gegevens te ontfutselen. Deze vorm van internetcriminaliteit wordt

PHISHING genoemd. Maar wat is phishing nu precies? Hoe herkent u het?

En wat kunt u ertegen doen? Deze folder geeft u antwoord.

WAT is PHISHING?

Phishing is een vorm van oplichting via internet. Door een e-mail probeert een oplichter (phisher) uw persoonlijke gegevens als creditcardnummer, bankgegevens, pincode of identiteitsgegevens te achterhalen. Deze e-mail lijkt afkomstig te zijn van een betrouwbare instantie, zoals uw creditcardmaatschappij of bank. Met deze gegevens kan de oplichter vervolgens bijvoorbeeld geld van uw rekening halen of andere producten/diensten op uw naam aanschaffen.

HOE gaat een PHISHER te werk?

De phisher verstuurt een e-mail die afkomstig lijkt van een betrouwbare instantie. Hierin staat bijvoorbeeld dat u een prijs heeft gewonnen die u alleen kunt innen door gegevens van uw creditcard bekend te maken. Een andere vaak toegepaste manier van phishing is het uit naam van de bank vragen om klant- of inloggegevens om zogenaamd klantenbestanden te controleren of bij te werken. In de meeste gevallen wordt u verzocht de site van de organisatie te bezoeken en daar uw persoonlijke gegevens achter te laten. Deze site lijkt net als de e-mail ook op die van de betrouwbare instantie. Zelfs het websiteadres lijkt indientiek. Toch is het een subtiële variant: www.fortis.nl in plaats van www.fortis.nl. Ook is het mogelijk dat de echte website wordt getoond, maar dat direct een pop-up scherm verschijnt waarin om uw gegevens wordt gevraagd. Alle informatie die u achterlaat op de nepwebsite kan de phisher direct misbruiken.

Hoe HERKENT u PHISHING?

Het is vaak moeilijk een phishing e-mail te onderscheiden van een authentieke e-mail. Toch is er een aantal kenmerken te noemen waaraan u een phishing e-mail kunt herkennen.

- Gerenommeerde banken, creditcardmaatschappijen en andere legitieme bedrijven vragen u nooit per e-mail om persoonlijke gegevens zoals creditcardnummer of wachtwoorden.
- Phishing e-mails spelen vaak in op uw angst opgelicht te worden, uw account kwijt te raken of op een andere dringende redenen om zo snel mogelijk te reageren.
- Een phishing e-mail is meestal onpersoonlijk: de aanhef luidt bijvoorbeeld "Beste klant". Maar let op: ook gepersonaliseerde e-mail kan nog steeds nep zijn!