

# **Courbois Software**

## **Phishing**

**Phishing** is het oplichten van mensen door een vertrouwde website te kopiëren, en niets-vermoedende personen persoonlijke en vertrouwelijke gegevens, zoals hun kredietkaartnummer en de bijhorende geheime code, te laten ingeven. De slachtoffers kunnen naar de valse website gelokt worden door een e-mail met een link naar de website.

Bij phishing wordt dikwijls gebruik gemaakt van URL-spoofing, dit is het nabootsen van de URL van bijvoorbeeld een bank, zodat de gebruiker denkt de echte site te bezoeken, terwijl de URL die van de bedrieger is. Phishing kan hiervan gebruik maken door een echte domeinnaam na te bootsen met gelijkaardige buitenlandse tekens, zodat de gebruiker niet merkt dat het adres niet klopt.

## **Gevaren**

Een voorbeeld van een phishing-mail. Het logo van de bank wordt misbruikt om "officiëler" over te komen.

Nog een voorbeeld: Niet alleen kan met phishing naar kredietkaarten gehengeld worden, ook wachtwoorden van sites (zoals Hotmail, of van een banksite) zijn populair. Met deze info kan de vreemde onder een andere naam mails versturen. Met voldoende persoonlijke gegevens kan een fraudeur zich voordoen als iemand anders; we spreken dan van identiteitsdiefstal of ID-diefstal. De nepmailtjes kunnen ook gaan over het aanbod een grote financiële transactie te doen of niet-bestaande producten en diensten af te nemen. Denk daarbij aan de berichten over Nigeriaanse e-mailfraudeurs (Nigerian scams).

## **Gevaar voorkomen**

### **Herken phishing mails**

- De brief is onpersoonlijk, en start met algemene groeten (geen vermelding van uw naam);
- Een officieel aandoend "From"-veld (dit kan eenvoudig vervalst worden);
- De e-mails betreffen meestal een zeer dringend verzoek om persoonlijke informatie door te geven. En u moet vooral snel reageren. Hierbij wordt ingespeeld op uw angsten, bijvoorbeeld om iets te missen, zoals een tijdelijke actie. Of dat uw account niet meer actief zal zijn als u niet snel inlogt, zoals bijvoorbeeld uw Hotmail-account.
- In de e-mail wordt vermeld dat uw gegevens verloren gingen, en dat u ze dringend opnieuw moet ingeven (het is erg onwaarschijnlijk dat uw bank of bijv. eBay uw gegevens kwijtraken);
- De e-mail is opgesteld in gebrekkig Engels/Nederlands;
- Vanuit de e-mail wordt via een pop-up naar de site doorgelinkt (pop-ups zijn onveilig en zullen daardoor nooit gebruikt worden).
- Meestal staan er in zulke emails dingen die erg onwaarschijnlijk zijn, bijvoorbeeld gouden horloges voor erg weinig geld.

- Kijk op de officiële website of iets waar is. Als bijvoorbeeld alle emailgegevens van Hotmail verloren zouden zijn gegaan, dan staat dat op de site van Hotmail. Staat dat er niet, trap er dan niet in!
- Gezond verstand
- Besef dat u wel eens phishing-mails kunt krijgen, en dat vreemden maar al te graag persoonlijke info van u krijgen;
- Vertrouw een e-mail nooit omdat die er officieel uitziet of de URL van een bekende organisatie aanbiedt;

## **Technische hulpmiddelen**

- Phishing-mails zijn spam, een spamfilter kan dan ook deze e-mails voorkomen.
- Er bestaan browserhulpmiddelen (bijv. Spoofstick, voor Internet Explorer en Firefox (extensie)) die de effectieve URL van de site aangeven. Misbruik wordt zo gedeeltelijk bemoeilijkt.
- Stel uw e-mailaccount zo in, dat u uw e-mails niet in HTML bekijkt. In HTML is het erg eenvoudig een tekst aan te maken die lijkt alsof het een link naar een grote, bekende site is, maar in feite is het een link naar een site van de verzender van de mail. Ook kunt u uw muis boven de link houden en linksonderin kijken naar welke website die leidt.

Hieronder staat een typische SPAM-mail, verstuurd naar het Wikipedia-antwoordkanaal.

Titel: Last warning from Paypal[1]

PayPal[2]

Dear Member,

Paypal is constantly working to ensure security by regulary screening the accounts in our system.[3]We recently reviewed your account,and we need more information to help us provide you with secure service.Until we collect this information,your access to sensitive account features will be limited.We would like to restore your acces as soon as possible,and we apologize for the inconvenience.

Why is my account access limited?

Your account access has been limited for the following reason(s):

August 10,2006:We would like to ensure that your account was not accessed by an unauthorized third party.Because protecting the security of your account is our primary concern,we have limited access to sensitive Paypal account features.We understand that this may be an inconvenience but please understand that this temporary limitation is for your protection.[4]

Case ID Number:PP-072-838-482

You must click the link below and enter your information to review your account

Click here[5] to visit the Resolution Center and complete the Steps to Remove Limitations

## **Opmerkingen**

1. Er moet dringend op deze mail geantwoord worden ('laatste waarschuwing')
2. Onpersoonlijke brief, geen vermelding van de naam
3. Let in deze mail op de gebrekkige interpunctie en spatiëring
4. Hier wordt de reden opgegeven waarom de gegevens zgn. verloren zijn gegaan
5. In de originele mail werd hier verwezen met een onveilige pop-up naar de paypal-site