Phishing

Phishing (naar analogie van *phreaking*, is het afgeleid van *fishing*: "vissen", "hengelen") 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, om ze daar – nietsvermoedend – te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer. Hierdoor krijgt de fraudeur de beschikking over deze gegevens met alle gevolgen van dien. De fraudeur doet zich hierbij voor als een vertrouwde instantie, zoals een bank. De meeste vormen van phishing gebeuren via e-mail. De slachtoffers worden hierbij met een e-mail naar deze valse website gelokt. De mail bevat een link naar de (valse) website met het verzoek om zogenaamd "de inloggegevens te controleren".

Een variante vorm van phishing is *spear fishing*, waarbij de persoonlijke gegevens (naam, e-mailadres, telefoonnummer) van het slachtoffer worden gebruikt om hem een gevoel van vertrouwen te geven.

Kenmerken

In een phishing-bericht zijn vaak de volgende elementen te vinden:[1][2]

- De mail is niet aan de klant persoonlijk gericht, maar begint met een algemene opening als "geachte klant".
- De mail bevat taal- en stijlfouten.
- Er wordt gesuggereerd dat het account "geverifieerd" (op juistheid onderzocht en bevestigd) moet worden met de inloggegevens van de klant.
- Er wordt gedreigd met gevolgen als niet onmiddellijk gehoor gegeven wordt aan de mail.
- De link waarnaar wordt verwezen bevat subtiele verschillen met de originele link, zoals een andere extensie of andere schrijfwijze.

Een veelgebruikte methode is dat de fraudeur een e-mail stuurt met een bijlage waarin een keylogger zit verborgen. De mail functioneert dan als een Trojaans paard. Zodra de gebruiker de bijlage heeft geopend, wordt – op de achtergrond – de keylogger geactiveerd. Hierdoor kan de fraudeur via internet zien welke wachtwoorden de gebruiker gebruikt bij het inloggen bij zijn of haar bank.