Phishing

Voorstelling	Phishing is een poging om toegang te krijgen tot de vertrouwelijke gegevens van slachtoffers, door zich uit te geven als een bekend bedrijf, over het algemeen een bank. In de letterlijke zin van het woord is phishing het 'vissen' naar persoonlijke informatie (zoals wachtwoorden, bankgegevens, kredietkaarten) per e-mail, telefoon of SMS. Deze oplichting lijkt op internetfraude (*link fiche internetfraude*), behalve dat de dader in deze gevallen geen gegevens manipuleert maar personen. Er bestaan verschillende vormen van phishing: - **Spoofing/spam based phishing** = oplichting per e-mail. - **Instant messaging based phishing** = de gebruiker ontvangt een link in zijn instant message box (MSN, Facebook of andere) die hem naar een nepsite stuurt waar men hem vraagt om bepaalde vertrouwelijke gegevens in te vullen. - **Vishing** = voice phishing, door het gebruik van de IP-stem. - **Phishing door zoekmachines** = tijdens opzoekingen op het internet, stelt de zoekmachine goedkope producten/diensten voor. Als iemand deze goederen aankoopt, zullen de bedriegers zich meester maken van zijn bankgegevens. - **Phishing door sociale netwerken** = phishers zetten links naar neplinks op bepaalde sociale netwerken. - **Spear-phishing** = phishing die gericht is op een specifiek slachtoffer. - **Whaling** = phishing die gericht is op ondernemingen, regeringen of groepen van hoge ambtenaren. - **Trojans** = een software die het mogelijk maakt om vertrouwelijke informatie te verzamelen die wordt overgezonden aan de misdadigers. - **Key loggers** = registreert de input van het klavier, die wordt overgezonden aan de misdadigers. - **Screen Grabbing** = oplichterij door middel van screenshots. - **Web-based delivery** = wanneer iemand op een phishinglink klikt, zorgt het openen van deze link ervoor dat er een kwaadaardige software wordt geïnstalleerd die het mogelijk zal maken om vertrouwelijke gegevens over te zenden zodra de persoon transacties uitvoert. - **Session hacking** = de phisher gebruikt een controlemechanisme van de lopende sessie (waardoor men het wachtwoord niet meer kan invoeren tijdens een sessie) om persoonlijke informatie van de gebruiker te ontfutselen. - **Wi-phishing** = daders installeren een gratis WIFI-netwerk waarmee mobiele toestellen van gebruikers automatisch verbinding maken, hetgeen het mogelijk maakt om kwaadaardige software te downloaden om gegevens te ontfutselen.
Wettelijke basis	- Art. 496 van het Strafwetboek
Adviezen	- Installeer een antispamfilter. - Blijf kritisch ten opzichte van e-mails. Wanneer het adres van de afzender vreemd lijkt, de mail slecht is opgesteld, niet in uw taal is en de nadruk legt op de negatieve gevolgen bij gebrek aan antwoord, dan gaat het waarschijnlijk om een phishingbericht. Antwoord er niet op en klik nooit op de links in deze mails! Deze links leiden naar pagina's die sprekend lijken op de echte internetpagina's van dit bedrijf, maar het zijn misdadigers die zich erachter verschuilen. - Geef uw persoonlijke gegevens niet per e-mail of telefonisch (codes, wachtwoorden, klantnummer, bankgegevens, etc.). - Maak steeds verbinding met de website van uw bank door het adres in uw browser te typen, gebruik hiervoor geen zoekrobotten omdat er valse websites tussen de zoekresultaten kunnen verschijnen. - Wees steeds aandachtig voor het internetadres waarnaar men u stuurt en vergewis u ervan dat u surft via 'https://' (niet via www. …) wanneer u online aankopen doet, wat betekent dat u via een beveiligde verbinding surft. - Indien u op een mogelijk phishingbericht stuit, kunt u dit naar verdacht@safeonweb.be sturen. - In geval van fraude met uw bankkaart, bel dan onmiddellijk Card Stop op het nummer 070 344 344 om uw kaart te laten blokkeren. - In geval van twijfel met betrekking tot een verdachte mail of iets anders, neem dan contact op met het betrokken bedrijf om uzelf gerust te stellen. Neem ook contact met hen op indien u slachtoffer bent geworden.
Nuttige links	www.safeonweb.be/nl www.safeinternetbanking.be