Phishing

Présentation	Le phishing ou le hameçonnage, c'est la tentative d'accéder aux données confidentielles des victimes, en se faisant passer pour une entreprise connue, typiquement une banque. C'est littéralement la « pèche » aux renseignements personnels (tels que les mots de passe, les informations bancaires, les cartes de crédits) par mail, téléphone ou SMS. Cette escroquerie ressemble à la fraude informatique, sauf que dans ce cas-ci, l'auteur ne manipule pas des données mais bien des personnes. Il existe différentes formes de phishing: - **Spoofing/spam based phishing** = escroquerie par e-mail - **Instant messaging based phishing** = l'utilisateur reçoit un lien dans sa messagerie instantanée (MSN, Facebook ou autre) qui le guide vers un site web factice où on lui demande de remplir certaines données confidentielles - **Vishing =** hameçonnage vocale, par l'utilisation de la voix IP - **Phishing par moteurs de recherche** = lors de recherches sur internet, le moteur de recherche propose des produits/services bon marché. Quand quelqu'un achète ces biens, ses données bancaires seront saisies par les imposteurs - **Phishing par les réseaux sociaux** = des phishers mettent des liens vers des liens factices sur certains réseaux sociaux - **Spear-phishing** = phishing qui cible une victime particulière - **Whaling** = phishing qui cible des entreprises, gouvernements ou groupes de hauts fonctionnaires - **Trojans** = logiciel qui permet de rassembler des informations confidentielles qui sont transmis aux malfaiteurs - **Key loggers =** enregistre l'input du clavier qui est transmis aux malfaiteurs - **Screen Grabbing =** escroquerie par le biais de captures d'écran - **Web-based delivery** = lorsqu'une personne clique sur un lien de phishing, l'ouverture de ce lien entraine l'installation d'un logiciel malveillant qui permettra de transmettre des données confidentielles une fois que la personne fera des transactions - **Session hacking** = le phisher utilise un mécanisme de contrôle de session en cours (qui permet de ne plus introduire le mot de passe durant une session) pour soustraire des informations personnelles de l'utilisateur - **Wi-phishing** = installez un réseau WIFI gratuit auquel les appareils mobiles des utilisateurs se connecte automatiquement, ce qui permet de télécharger des logiciels malveillants pour soustraire des données
Base légale	- Art. 496 du Code pénal
Conseils	- Installez un filtre anti-spam - Gardez un sens critique par rapports aux e-mails. Si l'adresse de l'expéditeur parait étrange, si le mail est mal rédigé, parfois pas dans votre langue et insiste sur les conséquences négatives en cas d'absence de réponse de votre part, il s'agit probablement d'un message de phishing. N'y répondez pas et ne cliquez jamais sur les liens dans ces mails! Ils vous dirigeront vers des pages qui ressemblent à s'y méprendre aux vraies pages internet de cette entreprise, mais ce sont des malfaiteurs qui se cachent derrière - Ne donnez pas vos données personnelles par e-mail ou par téléphone (codes, mots de passe, numéro de client, coordonnées bancaires, etc.). - Connectez-vous toujours au site de votre banque en tapant l'adresse dans votre navigateur, n'utilisez pas les moteurs de recherche pour ceci car de faux sites web peuvent y apparaitre. Soyez toujours attentif à l'adresse internet (www…) vers laquelle on vous envoie et assurez-vous que vous surfer via https:// quand vous faites des achats en ligne, ce qui signifie que vous surfez sur une connexion sécurisée - Si vous tombez sur un possible message de phishing, vous pouvez l'envoyer à suspect@safeonweb.be - En cas de fraude à la carte bancaire, appelez immédiatement Card Stop au 070 344 344 afin de faire bloquer votre carte - En cas de doute ou si vous avez été victime, contactez l'entreprise pour qui l'imposteur se fait passer
Liens utiles	www.safeonweb.be www.safeinternetbanking.be