LE PHISHING

BTS SiO1 2022-2023 / IZAC Matthieu

.

-SOMMAIRE

- Definition

Le phishing, ou hameçonnage, est une pratique malveillante sur la Toile qui consiste à récupérer des informations personnelles sur un Internaute. Le terme est la contraction des mots anglais fishing pour pêche et phreaking pour le piratage de lignes téléphoniques.

- Quand est apparu le Phishing ?

Le premier cas de phishing remonte au milieu des années 90, avec une attaque visant à dérober les noms d'utilisateurs et les mots de passe des utilisateurs d'AOL, élaborée à l'aide d'outils comme AOHell.

-Quel est le but du phishing ?

Le but du phishin est donc de voler, des informations personnels aux victimes tel que leurs numeros de carte bancaires, mots de passe, numero d'assurance sociale de telephone, date de naissance ou encore l'adresse postale.

-Statistiques concernant les attaques par phishing

https://tehtris.com/fr/blog/infographie-quelques-chiffres-sur-le-phishing#:~:text=%5BInfographie%5D%20%3A%20Quelques%20chiffres%20autour%20du%20phishing&text=Le%20phishing%20ou%20hame%C3%A7onnage%20est,de%20phishing%20r%C3%A9ussie%20par%20email%20%C2%BB.

- Les différents types de phishing

Courriel

Il s'agit de la forme la plus commune d'attaque d'hameçonnage. Les courriels d'hameçonnage sont conçus pour ressembler à une communication légitime provenant, par exemple, du service à la clientèle d'Amazon, de Paypal, d'une banque ou d'une autre entreprise reconnue afin de voler les informations.

Harponnage

Cette attaque d'hameçonnage ciblée utilise des données recueillies antérieurement sur la victime ou son employeur. En général, les courriels de harponnage utilisent un langage urgent et familier pour encourager la victime à agir.

Manipulation de liens

Cette attaque s'appuie sur des courriels formulés avec soin comprenant un lien malveillant vers un site Web connu comme LinkedIn. En cliquant sur le lien, les victimes sont dirigées vers un faux site Web identique au site original où elles sont encouragées à confirmer ou à mettre à jour les informations de leur compte.

Faux sites Web

Les cybercriminels envoient des courriels d'hameçonnage qui comprennent des liens vers des faux sites Web en apparence identiques aux sites originaux.

-Comment prévenir le Phishing ?

Ne communiquez jamais d'informations sensibles par téléphone ou mail.

Positionnez le curseur de votre souris sur le lien sans cliquer. Ainsi, l'adresse vers laquelle pointe le lien s'affiche. Si vous avez un doute, ne cliquez pas sur le lien et préférez aller directement sur le site de l'organisme via votre propre recherche.

Vérifiez l'adresse du site dans votre navigateur. Attention, parfois un seul caractère change, si c'est le cas vous êtes certainement sur un site frauduleux. Au moindre doute, ne donnez aucune information et fermez la page immédiatement.

Utilisez des mots de passe différents et compliqués pour chaque site et application. Vous éviterez ainsi le vol de mots de passe qui pourrait compromettre tous vos comptes personnels.

Activez la double identification pour sécuriser vos accès si le site le permet.

-Pourquoi faire des simulations de Phishing

Les attaques par hameçonnage sont difficiles à combattre, mais elles suivent des tendances qui peuvent être détectées. Chaque personne devrait donc effectuer des simulations régulières qui permettent aux d'éduquer les personnes en toute sécurité sans risquer de perdre des informations et données précieuses.

-Outils compatible linux pour phishing

Il existe plusieurs outils compatible a linux pour le phishing comme zphisher, nexhisher, AllHackingTools, onex ou encore kalimux

-Que faire en cas de phishing

S'il est trop tard et que l'on est victime d'un phishing, il faut déposer plainte au commissariat de police ou à la gendarmerie et il faut faire opposition auprès de notre banque et changer immédiatement l'ensemble de nos mots de passe. En plus de ces mesures de prévention, il est conseillé de faire appel à un expert en sécurité informatique qui garantira la sécurité des données et du système d'information notamment si on est une entreprise.