Phishing - Hameçonnage

Définition

L’hameçonnage (*phishing* en anglais) est une technique frauduleuse destinée à leurrer l’internaute pour l’inciter à communiquer des données personnelles (comptes d’accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance.

Il peut s’agir d’un faux message, SMS ou appel téléphonique de banque, de réseau social, d’opérateur de téléphonie, de fournisseur d’énergie, de site de commerce en ligne, d'administrations, etc.

But recherché

VOLER DES INFORMATIONS PERSONNELLES OU PROFESSIONNELLES

(comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.

Mesures Préventives

- Ne communiquez jamais d'informations sensibles par messagerie ou téléphone : aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.

- Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.

- Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.

- En cas de doute, contactez si possible directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu.

- Utilisez des mots de passes différents et complexes pour chaque site et application afin d'éviter que le vol d'un de vos mots de passe ne compromette tous vos comptes personnels. Vous pouvez également utiliser des coffres forts numériques de type KeePass pour stocker de manière sécurisée vos différents mots de passe.

- Si le site le permet, **vérifiez les date et heure de dernière connexion à votre compte** afin de repérer si des accès illégitimes ont été réalisés.

- Si le site vous le permet, **activez la double authentification pour sécuriser vos accès**.

Si vous êtes victimes

- Si vous avez malencontreusement communiqué des éléments sur vos moyens de paiement ou si vous avez constaté des débits frauduleux sur votre compte, **FAITES OPPOSITION IMMÉDIATEMENT** auprès de votre organisme bancaire ou financier et déposez plainte au commissariat de police ou à la gendarmerie la plus proche.

- Si vous avez constaté que des éléments personnels servent à usurper votre identité, **DÉPOSEZ PLAINTE** au commissariat de police ou à la gendarmerie la plus proche.

- Si vous êtes victime d'une usurpation de votre adresse de messagerie ou de tout autre compte, **CHANGEZ IMMÉDIATEMENT VOS MOTS DE PASSE**.

- Si vous avez reçu un message douteux sans y répondre, **SIGNALEZ-LE À SIGNAL SPAM** (https://www.signal-spam.fr/).

- Vous pouvez également **SIGNALER UNE ADRESSE DE SITE D'HAMEÇONNAGE À PHISHING INITIATIVE** (https://phishing-initiative.fr/contrib/) qui en fera fermer l'accès.

- Pour être conseillé en cas d'hameçonnage, contactez INFO ESCROQUERIES **AU 0 805 805 817** (numéro gratuit).

Les infractions encourues

• Escroquerie (article 313-1 du code pénal) : l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. Délit passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende.

•Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite (article 226-18 du code pénal) : une telle collecte constitue un délit passible d'une peine d'emprisonnement de cinq ans et de 300 000 euros d'amende.

•Accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal) : le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de deux ans d'emprisonnement et de 60 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 euros d'amende.

•Contrefaçon et usage frauduleux de moyen de paiement (articles L163-3 et L163-4 du code monétaire et financier) : délit passible d'une peine d'emprisonnement de sept ans et de 750 000 euros d'amende.

• Usurpation d'identité (article 226-4-1 du code pénal) : le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est passible d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende.

•Contrefaçon des marques (logos, signes, emblèmes…) utilisées lors de l'hameçonnage, prévu par les articles L.713-2 et L.713-3 du Code de la propriété intellectuelle. Délit passible d'une peine d'emprisonnement de trois ans et de 300 000 euros d'amende.