



L'HAMEÇONNAGE



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.

COMMENT DÉTECTER UN MESSAGE D'HAMEÇONNAGE ?

7 points de contrôle qui doivent vous alerter :

UNE NOTIFICATION DE LA MESSAGERIE OU DE L'ANTIVIRUS. Votre client de messagerie ou votre antivirus peuvent vous signaler la réception d'un message malveillant. N'ignorez pas leur avertissement.

UN NOM D'ÉMETTEUR INHABITUEL. La réception d'un message inattendu d'un émetteur inhabituel, même d'apparence légitime, doit éveiller l'attention.

UNE ADRESSE D'EXPÉDITION FANTAISISTE. La plupart des messages d'hameçonnage utilisent des adresses de messagerie qui ne ressemblent pas à des adresses officielles.

UN OBJET DE MESSAGE SUCCINCT OU ALARMISTE. L'objet d'un message malveillant est généralement sommaire et vise à inciter la victime à ouvrir le message, comme « remboursement », « alerte de sécurité »...

UN MESSAGE AGUICHEUR OU INQUIÉTANT. Le contenu d'un message d'hameçonnage évoque souvent une offre ou un gain inespéré, ou encore une action urgente à réaliser.

DES FAUTES DE FRANÇAIS SURPRENANTES. Les messages d'hameçonnage comportent régulièrement des fautes d'orthographe ou de syntaxe inhabituelles dans des communications officielles.

UNE INCITATION À OUVRIR UN LIEN OU UNE PIÈCE JOINTE. Les messages frauduleux cherchent généralement à pousser la victime à ouvrir une pièce jointe qui peut contenir un virus ou à cliquer sur un lien qui les amènera sur un site 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 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.



UNE INITIATIVE INTER-RÉGIONALE DE :



RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

