FICHE N°5 : HAMEÇONNAGE / PHISHING

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... Ces techniques d'attaque évoluent constamment. Les conseils suivants vous aideront à déterminer si un message est légitime ou non.

MESSAGE DE PRÉVENTION

1- Attention aux expéditeurs inconnus : soyez particulièrement vigilants sur les courriels provenant d'une adresse électronique que vous ne connaissez pas ou qui ne fait pas partie de votre liste de contact.

2- Soyez attentif au niveau de langage du courriel : même si cela s'avère de moins en moins vrai, certains courriels malveillants ne sont pas correctement écrits. Si le message comporte des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées, c'est qu'il n'est pas l'œuvre d'un organisme crédible (banque, administration...).

3- Vérifiez les liens dans le courriel : avant de cliquer sur les éventuels liens, laissez votre souris dessus. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime. Ne faites pas confiance aux noms de domaine du type impots.gouvv.fr, impots.gouvfr.biz, infocaf.org au lieu de www.caf.fr.

4- Méfiez-vous des demandes étranges : posez-vous la question de la légitimité des demandes éventuelles exprimées. Aucun organisme n'a le droit de vous demander votre code carte bleue, vos codes d'accès et mots de passe. Ne transmettez rien de confidentiel même sur demande d'une personne qui annonce faire partie de votre entourage.

5- L'adresse de messagerie source n'est pas un critère fiable : une adresse de messagerie provenant d'un ami, de votre entreprise, d'un collaborateur peut facilement être usurpée. Seule une investigation poussée permet de confirmer ou non la source d'un courrier électronique. Si ce message semble provenir d'un ami (par exemple pour récupérer l'accès à son compte) contactez-le sur un autre canal pour vous assurer qu'il s'agit bien de lui !

Source : plateforme Cybermalveillance.gouv.fr

Je suis victime, que faire ? Comment signaler les tentatives d'escroquerie sur internet ?

Comment s'en prémunir ?

Utilisez un logiciel bloqueur de publicités, de filtre anti-pourriel, ou activer l'option d'avertissement contre le filoutage présent sur la plupart des navigateurs. Installez un anti-virus et mettez-le à jour. Désactivez le volet de prévisualisation des messages. Lisez vos messages en mode de texte brut.

Comment réagir ?

Si vous avez un doute sur un message reçu, il y a de fortes chances que celui-ci ne soit pas légitime : N'ouvrez surtout pas les pièces jointes et ne répondez-pas. Supprimez le message puis videz la corbeille.

S'il s'agit de votre compte de messagerie professionnel : transférez-le au service informatique et au responsable de la sécurité des systèmes d'information de votre entreprise pour vérification. Attendez leur réponse avant de supprimer le courrier électronique.

Si vous voyez une fenêtre POP-UP, ne cliquez jamais sur l'annonce, même si le bouton de fermeture est énorme. Utilisez toujours la croix (X) dans le coin. Si l'escroquerie que vous souhaitez signaler vous est parvenue par un spam (pourriel), rendez-vous sur www.signal-spam.fr.

Signalez les escroqueries auprès du site https://www.internet-signalement.gouv.fr/, la plateforme d'harmonisation, d'analyse de recoupement et d'orientation des signalements. Pour s'informer sur les escroqueries ou pour signaler un site internet ou un courriel d'escroqueries, un vol de coordonnées bancaires ou une tentative d'hameçonnage : contacter Info Escroqueries au 08.11.02.02.17.

Rendez-vous sur https://www.cybermalveillance.gouv.fr/, la plateforme nationale d'assistance aux victimes d'actes de cybermalveillance. Que vous soyez un particulier, une entreprise ou une administration, retrouvez :
- des conseils / vidéos pour sensibiliser votre entourage professionnel ou personnel,
- des services de proximité en cas de dommages causés par une attaque informatique.