**Comment repérer une arnaque reçue dans votre messagerie ou votre boîte mail ?**

Votre messagerie ou votre antivirus peuvent vous signaler la réception d’un mail frauduleux. N’ignorez pas leur avertissement et assurez-vous régulièrement que votre antivirus est activé et à jour.

Est-ce que le message/courriel vous est réellement destiné ?

Généralement, les messages malveillants sont envoyés à destination d’un grand nombre de cibles, ils ne sont pas ou peu personnalisés. Les emails officiels qui vous sont adressés mentionnent votre nom, or l’hameçonnage « bon marché » consiste à envoyer à échelle industrielle le même mail de phishing de manière dépersonnalisée à une large base de données d’adresses mail. Si le message ne mentionne pas votre nom ou encore qu’il utilise une formule un peu vague de type « Cher client privilégié », méfiez-vous.

Le message évoque un dossier, une facture, un thème qui ne vous parle pas ? Il s’agit certainement d’un courriel malveillant.

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.

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 !

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 …).

Un mail de phishing fait souvent part d’une offre, d’un remboursement ou d’un gain inespéré. Vous venez de remporter un lot important alors que vous n’avez pas joué et que vous n’êtes pas client de l’entreprise qui vous a soi-disant envoyé le message ? Il s’agit probablement d’une tentative de phishing. Un mail frauduleux peut également faire état d’un besoin urgent ou d’une menace imminente qui requiert une action immédiate, comme la fermeture de votre compte si vous n’agissez pas tout de suite. En pressant leurs victimes, les cybercriminels tentent de les déstabiliser et de les pousser à prendre des décisions erronées.

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.

\* A noter : cette manipulation est impossible à effectuer depuis un écran de smartphone.

Un mail peut également vous inciter à ouvrir ou télécharger une pièce jointe (une image, un fichier audio ou vidéo, un document PDF, une pièce jointe au format HTML…). Évitez ainsi de cliquer sur des pièces jointes que vous n’attendiez pas, envoyées par des expéditeurs inconnus ou douteux. Une fois ouverte, la pièce jointe peut vous rediriger vers un site frauduleux vous réclamant des informations confidentielles, voire installer un virus sur votre ordinateur ou votre téléphone.

L’objet du mail est généralement sommaire et cherche à inciter la victime à ouvrir le message. Un intitulé aguicheur ou inquiétant – comme « remboursement » ou « alerte de sécurité » – qui transmet un sentiment d’urgence inhabituel.

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.

En règle générale, les demandes d’informations personnelles – identifiants de connexion, informations bancaires… – ne se font jamais par email. Aucune entité légitime, gouvernementale, professionnelle ou autre n’est en droit de vous demander votre code de carte bancaire ou vos codes d’accès personnels par message. Ne communiquez rien de confidentiel par écrit, même s’il s’agit d’un expéditeur qui prétend faire partie de votre entourage.

**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.