Cybercriminalité : gare aux mails et SMS frauduleux (partie 2)

generations-mouvement.org/cybercriminalite-gare-aux-mails-et-sms-frauduleux-partie-2/

14 septembre 2023

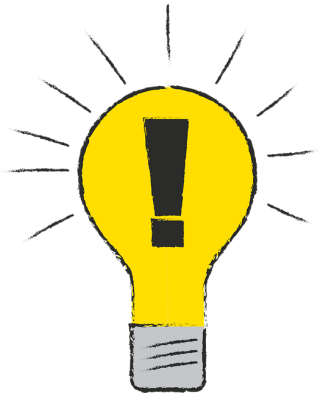
Dans cette série d'articles consacrés à la prévention contre la cybercriminalité, nous vous présentons ici les réflexes à avoir face aux tentatives d'escroquerie par mail et par SMS.

Vous pouvez consulter le précédent article consacré aux tentatives d'escroquerie par téléphone.

Les tentatives d'escroquerie par mail : la plus courante des pratiques

Hameçonnage, rançongiciel, etc. : tels sont les qualificatifs des méthodes dont peut être victime n'importe quel internaute.

Prêt de 120 000 milliards de mails sont échangés chaque année dont 75% sont des spams qui cachent ainsi des types de messages frauduleux tentant d'escroquer les destinataires. Offres alléchantes, menaces en justice, fausses confirmations de livraison de colis : derrière ces mails se cachent des entreprises hors la loi bien rodées et qui savent user de toutes les ruses possibles pour piéger les potentielles victimes.



Quelques réflexes à avoir !

Concernant les messages mails suspicieux, il existe plusieurs règles à suivre (celles-ci sont notifiées dans l'article Comment reconnaître un mail de phishing ou d'hameçonnage ? du site gouvernemental sur la cybermalveillance) .

En voici quelques unes :

Prenez bien en compte les messages de mise en garde de votre **antivirus** : ceux-ci parfois nombreux ne doivent pas être mis de côté et ils sont un bon outils de premier niveau pour vous alerter sur la malveillance d'un message mail et au besoin l'éliminer.

- Vous n'êtes pas client de la société qui vous envoie un mail : surtout, ne répondez pas à ce mail, même si une offre alléchante vous est proposée dans le cadre de dispositifs gouvernementaux tels qu'actuellement MaPrimeAdapt, MaPrimeRenov, etc. et qui sont de plus en plus sujets à des tentatives de fraudes.
- L'email de l'expéditeur est fantaisiste. un exemple de mail d'expédition : Service Client de La Poste <laposte_452152@winia.online>. Dans ce cas, le domaine internet devrait être "laposte.fr" mais certainement pas "winia.online".
- Le message mail comporte beaucoup de fautes d'orthographe et semble peu personnalisé.
- Le message mail est menaçant et prétend provenir d'un organisme gouvernemental.

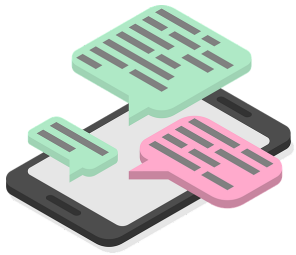
Ces réflexes de base peuvent aussi s'adapter aux SMS reçus :

Récemment une alerte a été donnée sur un message SMS invitant les victimes à renseigner leurs coordonnées bancaires dans le cadre d'un renouvellement de la carte VITALE.

Et ce n'est qu'un exemple de tentative d'escroquerie.

Dans ce dernier cas, gardez aussi le réflexe de ne jamais transmettre par SMS vos informations confidentielles (numéro de compte, numéro confidentiel, identité, téléphone,…).

Que ce soit par mail ou par SMS, si vous recevez une demande de transaction impliquant la transmission de données bancaires ou autres informations personnelles, n'engagez aucune démarche par écrit et contactez directement l'organisme à l'origine de ce message.



Des liens à visiter :

Définition de la cybercriminalité

Liens officiels du gouvernement :

- https://www.cybermalveillance.gouv.fr/
- https://www.impots.gouv.fr/actualite/attention-aux-arnaques

Lien Groupama : “Comprendre les cyber-attaques pour mieux s’en protéger”

https://www.groupama.fr/assurance-professionnels/conseils/comprendre-les-cyber-attaques/