Cybercriminalité : gare aux appels téléphoniques frauduleux (partie 1)

generations-mouvement.org/cybercriminalite-gare-aux-appels-telephoniques-frauduleux-partie-1/

7 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 téléphone.

Nous vous présenterons dans de prochains articles les autres formes de tentative d'escroquerie ainsi que les solutions mises en place à Générations Mouvement et les actions pour se protéger au mieux face au phénomène croissant de la cybercriminalité.

Les tentatives d'escroquerie par mail, message téléphonique, sms (etc.) abondent de façon exponentielle depuis l'avènement d'internet il y a plus de 25 ans maintenant : c'est ce que l'on nomme la **cybercriminalité**.

Il faut vivre avec son temps mais avoir toujours le réflexe de ne pas se laisser submerger par les flux d'informations que nous recevons via nos ordinateurs et nos téléphones (fixes ou mobiles).

Dans un moment de stress, nous sommes tous (jeunes ou moins jeunes) des potentielles victimes de nombreuses tentatives d'arnaque. Alors, restons mobilisés et solidaires autour des dangers que peuvent engendrer notre monde ultra numérisé.

Si vous êtes méfiant, vous consulterez le numéro qui vous contacte et vous constaterez que le numéro appelant est bien celui de votre banque. Et pour cause : celui-ci a été usurpé ! Et la personne au bout du téléphone tentera par tous les moyens -et de manière très professionnelle- de vous faire faire toute une série d'opérations à distance sur votre compte.

Consultez ces deux articles concernant cette dernière innovation en matière de tentative d'escroquerie : Les arnaques aux faux conseillers bancaires en forte hausse, comment faire pour s'en protéger ? Fraude aux faux conseillers.

La dernière innovation en matière de tentative d'escroquerie :

La dernière escroquerie connue est l'usurpation du numéro de téléphone de votre banque, sous prétexte d'un paiement frauduleux :

"Bonjour Monsieur, Madame, je suis conseiller/conseillère de votre banque et vous informe que des paiements frauduleux ont été signalés sur votre compte, (etc)".

Quelques réflexes à avoir !

Dans le cas de suspicion d'appel frauduleux concernant votre banque :

- Ne donner aucune information confidentielle (numéro de compte, numéro confidentiel, identité précise de personnes de votre entourage et de vous-même, numéros de téléphone tiers)
- Demander l'identité de la personne (nom, prénom, fonction)
- Mettre fin à l'appel au plus vite, et ne pas donner suite
- Puis rappeler directement votre agence bancaire

Ces réflexes peuvent s'appliquer dans le cadre de tentative d'escroquerie concernant d'autres organismes (organismes sociaux, assurances, prestataires de service,…) et sont à mémoriser voire à noter sur une notice papier car les escrocs savent agir sur le mental des victimes qui dans ce mode de communication peuvent être plus faciles à manipuler.

D'autres réflexes sont à noter notamment refuser que le fraudeur prenne le contrôle de votre ordinateur grâce à un outils de prise de contrôle à distance : le numérique nous offre des logiciels de plus en plus pratiques et de plus en plus faciles à installer, mais qui se révèlent être de véritables armes à double tranchant.

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/