GRANNY GEEK

TOUS AU NUMEREEK

ASSISTANCE ET ACCOMPAGNEMENT À DISTANCE DES SENIORS AU NUMÉRIQUE

SYLVAIN CALLOT

GRANNY GEEK®

SOMMAIRE

LES GESTES DE 1ER SECOURS EN CAS D'ESCROQUERIE EN LIGNE

GRANNY GEEK®

QUELQUES QUESTIONS

QUESTION 1 : Avez-vous déjà été confronté à une arnaque en ligne ?

QUESTION 2 : Si oui, sous quelle forme ?

QUESTION 3 : Comment vous sentiez-vous face à ce problème ?

DÉFINITION

LES DIFFÉRENTS TYPES D'ARNAQUES

E-MAILS, SMS : Phishing, hameçonnage (31%)

> E-mail d'un proche en difficulté (ami, connaissance...)
> Gains, cadeaux, promotions
> Accès à un service arrêté (banques, administrations...)
> Problème de sécurité, livraison, factures (FAI, La Poste...)
> Infraction, message d'interpole, de la gendarmerie
> CPF, accès à un compte

PIRATAGE D'UN COMPTE : (19%)

> Compte e-mail, comptes utilisateurs

FAUX SUPPORT TECHNIQUE: (13%)

> Écran bleu avec un son strident
> Message que votre ordinateur est infecté avec N° gratuit

E-MAILS

LES GESTES DE PRÉVENTION

DANS TOUS LES CAS :

> Ne répondez **JAMAIS** et ne cliquez sur aucun lien en cas de doute

> Téléphonez directement à la personne si c'est le mail d'un(e) ami(e)

> Les banques ne vous demanderont jamais de cliquer sur un lien pour refaire vos mots de passe sauf si c'est vous qui en faites la demande expressément

> Le gouvernement et les administrations non plus

> Repérez les fautes d'orthographe

> Rendez vous sur votre boite mail de votre ordinateur et vérifiez où mènent les liens en plaçant le curseur dessus

> Supprimez les mails et videz la corbeille

E-MAILS

LES GESTES POUR SOIGNER

SI VOUS AVEZ RÉPONDU :

> Faites opposition à votre carte bancaire

> Installez et exécutez Malwarebytes, Spybot, AdwCleaner

> Faites une analyse antimalware et supprimez ou mettez en quarantaine les programmes néfastes.

> Faites une bonne analyse antivirus en privilégiant les analyses complètes. Elles sont beaucoup plus longues mais aussi plus rigoureuses et efficaces.

> Faites un nettoyage de vos navigateurs internet (caches, cookies, fichiers temporaires), vous pouvez le faire facilement avec un utilitaire de nettoyage (BleachBit, CCleaner, Glary Utilities...)

PIRATAGE

LES GESTES DE PRÉVENTION

DANS TOUS LES CAS :

> Créez des mots de passe complexes (min 15 caractères avec majuscules, minuscules, chiffres et caractères spéciaux)

> Modifiez la sécurité en optant pour la double authentification

> Ne rentrez jamais vos identifiants sur un site non sécurisé : http:// au lieu de https://

PIRATAGE

LES GESTES POUR SOIGNER

SI VOUS AVEZ ÉTÉ PIRATÉ :

> Avertissez le service sur lequel est votre compte (FAI, administration)

> Avertissez vos proches

> Si vous avez encore accès à votre compte, changez les mots de passe (min 15 caractères avec majuscules, minuscules, chiffres et signes spéciaux)

> Modifiez la sécurité en optant pour la double authentification si vous ne l'aviez pas fait

> Faites une analyse antivirus et antimalware en profondeur

FAUX SUPPORT

LES GESTES DE PRÉVENTION

DANS TOUS LES CAS :

> Ce blocage n’intervient que lorsque vous naviguez sur internet

> Installez des extensions de sécurité de navigation

> Vous pouvez installer aussi des bloqueurs de pub (pop-up)

> Mettez régulièrement à jour vos navigateurs internet

> Mettez à jour votre système d’exploitation

FAUX SUPPORT

LES GESTES PENDANT L'ALERTE

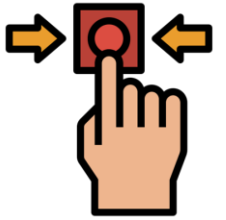
EN CAS DE BLOCAGE :

> N'appelez **JAMAIS** le numéro indiqué

> Fermez votre navigateur en cliquant sur "**Esc**" ou "**F 11**"

> Si votre navigateur ne se ferme pas facilement cliquez sur "**Alt** + **Ctrl** + **Suppr**" et cliquez sur "**Gestionnaire de tâches**", cliquez sur votre navigateur et "**Fin de tâches**"

> Si cela ne fonctionne pas non plus, éteignez votre ordinateur en appuyant quelques secondes sur le bouton **Marche/Arrêt**



> Ne **JAMAIS** donner d'informations, vos coordonnées bancaires, vos mots de passe

> **N'ACCEPTEZ JAMAIS** de télécharger un programme ou une prise de contrôle à distance

FAUX SUPPORT

LES GESTES POUR SOIGNER

SI VOUS AVEZ APPELÉ ET DONNÉ LES INFORMATIONS :

> Faites opposition à votre carte bancaire

> Supprimez tous les logiciels qu'ils vous ont installés

> Changez tous vos mots de passe

> Faites une analyse antimalware, une analyse antivirus complète, nettoyez votre navigateur

> Prévenez votre entourage (en copie caché CCI et non copie conforme CC pour ne pas faire apparaître les différents mails) et les plateformes gouvernementales

> Redoublez de vigilance car les escrocs vous auront repéré comme cible potentielle et seront susceptibles de vous contacter par la suite.

PENSE-BÊTE

GRANNY GEEK VOUS CONSEILLE

> Faites régulièrement vos mise à jour de sécurité

> Installez des extensions web safe browser sur vos navigateurs

> N’ouvrez pas les courriels, leurs pièces jointes et ne cliquez pas sur les liens provenant de chaînes de messages, d’expéditeurs inconnus, ou d’un expéditeur connu mais dont la structure du message est inhabituelle ou vide.

> Évitez les sites non sûrs ou illicites, privilégiez les sites sécurisés (https)

> Cachez votre caméra lorsque vous ne l’utilisez pas (avec un cache ou un scotch spécial)

> Aucun support officiel ne vous contactera pour vous demander de modifier vos mots de passe ou vous demander de l’argent

> Dans le doute abstenez-vous !

> Appelez Granny Geek, un ami ou un technicien local pour intervenir

> Lire l’article sur notre site : la parenthèse du 11 mars 2021

GRANNY GEEK

VOUS REMERCIE

TOUS AU NUMEREEK

Granny Geek SAS est une entreprise de l'économie sociale et solidaire au capital de 12000 euros enregistrée au RCS de Nice le 27 janvier 2020 sous le numéro 882 014 855 0010.

CONTACT : sos@sos-grannygeek.com
TEL : 04 89 41 92 29
SITE INTERNET : WWW.SOS-GRANNYGEEK.COM

ILS PARLENT DE NOUS

https://www.facebook.com/SOSGrannyGeek/

https://www.linkedin.com/company/sosgrannygeek

https://twitter.com/SOSGrannyGeek

https://instagram.com/sos.grannygeek

Cliquer sur l'image pour voir la vidéo de présentation de la hotline GRANNY GEEK®