RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

COMPRENDRE LES RISQUES

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

L'arnaque au faux support technique (***Tech support scam*** en anglais) consiste à effrayer la victime, par SMS, téléphone, chat, courriel, ou par l'apparition d'un message qui bloque son ordinateur, lui indiquant un problème technique grave et un risque de perte de ses données ou de l'usage de son équipement afin de la pousser à contacter un prétendu support technique officiel (Microsoft, Apple, Google...), pour ensuite la convaincre de payer un pseudo-dépannage informatique et/ou à acheter des logiciels inutiles, voire nuisibles. Si la victime refuse de payer, les criminels peuvent la menacer de détruire ses fichiers ou de divulguer ses informations personnelles.

BUT RECHERCHÉ

Soutirer de l'argent à la victime en la poussant à laisser prendre le contrôle de sa machine pour faire semblant de la lui dépanner et lui installer des logiciels et/ou faire souscrire des abonnements qui lui seront facturés.

SI VOUS ÊTES VICTIME

NE RÉPONDEZ PAS AUX SOLLICITATIONS et n'appelez jamais le numéro indiqué.

CONSERVEZ TOUTES LES PREUVES. Photographiez votre écran au besoin.

S'il semble « bloqué », **REDÉMARREZ VOTRE APPAREIL**. Cela peut suffire à régler le problème.

Si votre navigateur reste incontrôlable, **PURGEZ LE CACHE, SUPPRIMEZ LES COOKIES, RÉINITIALISEZ LES PARAMÈTRES PAR DÉFAUT** et si cela ne suffit pas, supprimez et recréez votre profil.

DÉSINSTALLEZ TOUTE NOUVELLE APPLICATION SUSPECTE présente sur votre appareil.

FAITES UNE ANALYSE ANTIVIRALE COMPLÈTE de votre appareil.

Si un faux technicien a pris le contrôle de votre machine, **DÉSINSTALLEZ LE PROGRAMME DE GESTION À DISTANCE ET CHANGEZ TOUS VOS MOTS DE PASSE**. En cas de doute ou si vous n'arrivez pas à reprendre le contrôle de votre appareil, vous pouvez faire appel à un professionnel référencé sur www.cybermalveillance.gouv.fr.

Si vous avez fourni vos coordonnées de carte bancaire, **FAITES OPPOSITION SANS DÉLAI**. Si un paiement est débité sur votre compte, **EXIGEZ LE REMBOURSEMENT** en indiquant que vous déposez plainte.

SIGNALEZ LES FAITS sur la plateforme Internet-signalement.gouv.fr du ministère de l'Intérieur.

En fonction du préjudice subi, **DÉPOSEZ PLAINTE** au commissariat de police ou à la gendarmerie ou en écrivant au procureur de la République dont vous dépendez en fournissant toutes les preuves en votre possession.

MESURES PRÉVENTIVES

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine, en particulier vos navigateurs.

Tenez à jour votre antivirus et activez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications et services légitimes.

Évitez les sites non sûrs ou illicites, tels ceux qui hébergent des contrefaçons (musique, films, logiciels...) ou certains sites pornographiques qui peuvent infecter votre machine ou héberger des régies publicitaires douteuses.

N'installez pas d'application ou de programme « piratés », ou dont l'origine ou la réputation sont douteuses.

N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.

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.

Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine.

Un support technique officiel ne vous contactera jamais pour vous réclamer de l'argent.

FAUX SUPPORT TECHNIQUE

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION