Faux support technique

Définition

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.

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.

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

Si vous êtes victimes

- 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 ANTIVIRUS approfondie de votre machine.

- 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 équipement par vous-même, vous pouvez faire appel à un prestataire référencé sur https://www.cybermalveillance.gouv.fr/.

- Si vous avez fourni vos coordonnées bancaires ou n° de carte de crédit, **FAITES OPPOSITION** sans délai. Si un paiement est débité sur votre compte, **EXIGEZ LE REMBOURSEMENT** en indiquant que vous déposez plainte.

- Si vous avez été contacté par un faux support technique, **SIGNALEZ LES FAITS AU MINISTÈRE DE L'INTÉRIEUR** sur sa plateforme https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action.

- DÉPOSEZ PLAINTE au commissariat de police ou à la brigade de gendarmerie ou en écrivant au procureur de la République dont vous dépendez. Faites vous, au besoin, assister par un avocat spécialisé.

Les infractions encourues

• L'incrimination principale qui peut être retenue est l'escroquerie. L'article 313-1 du code pénal dispose que : « *l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge* ». L'escroquerie est passible de cinq ans d'emprisonnement et de 375 000 euros d'amende.

• Si la victime est menacée de suppression de ses fichiers ou en est victime, de tels procédés relèvent de l'extorsion de fonds. En effet, ils se caractérisent par une contrainte physique – le blocage de l'ordinateur ou la destruction de fichiers – obligeant à une remise de fonds non volontaire. L'article 312-1 du code pénal dispose que : « *l'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque* ». L'extorsion est passible de sept ans d'emprisonnement et de 100 000 euros d'amende.

• L'infraction d'atteinte à un système de traitement automatisé de données (STAD) pourra également être retenue. Les articles 323-1 à 323-7 du code pénal disposent que : « *le fait d'accéder ou de se maintenir frauduleusement » dans un STAD, « la suppression ou la modification de données contenues dans le système* », ou l'« *altération du fonctionnement de ce système* » sont passibles de deux ans à sept ans d'emprisonnement et de 60 000 euros à 300 000 euros d'amende.