ARNAQUE
AU FAUX SUPPORT TECHNIQUE

CENTRE CYBER DU PACIFIQUE

EN BREF

QU'EST-CE QUE C'EST ?

L'arnaque au faux support technique consiste à effrayer la victime via SMS, téléphone, chat, courriel ou un message bloquant son ordinateur, lui signalant un problème grave et un risque de perte de données. Elle est incitée à contacter un faux support officiel (Microsoft, Apple, Google…) qui la pousse à payer un dépannage fictif ou à acheter des logiciels inutiles, voire nuisibles. En cas de refus, les criminels peuvent menacer de détruire ses fichiers ou de divulguer ses informations personnelles.

BUT RECHERCHÉ : Obtenir de l'argent en prenant le contrôle de l'appareil, en simulant un dépannage et en facturant des logiciels ou des abonnements.

Voici 10 bonnes pratiques à adopter si vous êtes victime

1. IGNOREZ LES SOLLICITATIONS ET N'APPELEZ JAMAIS LE NUMÉRO INDIQUÉ
2. CONSERVEZ LES PREUVES EN PHOTOGRAPHIANT VOTRE ÉCRAN
3. REDÉMARREZ L'APPAREIL POUR TENTER DE DÉBLOQUER LA SITUATION
4. RÉINITIALISEZ LE NAVIGATEUR EN VIDANT LE CACHE ET LES COOKIES
5. SUPPRIMEZ LES APPLICATIONS SUSPECTES INSTALLÉES RÉCEMMENT
6. FAITES UNE ANALYSE ANTIVIRUS COMPLÈTE DE VOTRE APPAREIL
7. DÉSACTIVEZ L'ACCÈS À DISTANCE ET CHANGEZ TOUS VOS MOTS DE PASSE
8. FAITES OPPOSITION BANCAIRE ET DEMANDEZ UN REMBOURSEMENT
9. SIGNALEZ L'ARNAQUE SUR : INTERNET-SIGNALEMENT.GOUV.FR.
10. DÉPOSEZ PLAINTE EN CONTACTANT LA POLICE OU LE PROCUREUR

▶ Voir détail page "10 BONNES PRATIQUES À ADOPTER"

ARNAQUE
AU FAUX SUPPORT TECHNIQUE

CENTRE CYBER DU PACIFIQUE

10 BONNES PRATIQUES À ADOPTER

1. IGNOREZ LES SOLLICITATIONS
et n'appelez jamais le numéro indiqué.

2. CONSERVEZ TOUTES LES PREUVES
en photographiant votre écran au besoin.

3. REDÉMARREZ VOTRE APPAREIL
s'il semble « bloqué », cela peut suffire à régler le problème.

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

5. DÉSINSTALLEZ TOUTE NOUVELLE APPLICATION SUSPECTE
présente sur votre appareil.

6. FAITES UNE ANALYSE ANTIVIRALE COMPLÈTE
de votre appareil.

7. DÉSINSTALLEZ LE PROGRAMME DE GESTION À DISTANCE ET CHANGEZ TOUS VOS MOTS DE PASSE
si un faux technicien a pris le contrôle de votre machine et 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/diagnostic/profil.

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

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

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

ARNAQUE
AU FAUX SUPPORT TECHNIQUE

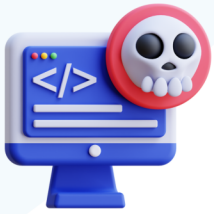
CENTRE CYBER
DU PACIFIQUE

COMMENT S'EN PROTÉGER ?

Appliquez de manière régulière et systématique les mises à jour de sécurité :
Mettez à jour votre système et les 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.

EN FONCTION DU CAS D'ESPÈCE, LES INFRACTIONS SUIVANTES PEUVENT ÊTRE RETENUES :

• 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) peut être retenue. Les articles 323- 1 à 323-7 du code pénal disposent notamment que : « le fait d'accéder ou de se maintenir frauduleusement » dans un STAD, « la suppression ou la modification de données contenues dans le système », « le fait [...] d'extraire, de détenir, de reproduire, de transmettre [...] les données qu'il contient » ou l'« altération du fonctionnement de ce système » sont passibles de trois à sept ans d'emprisonnement et de 100 000 à 300 000 euros d'amende.