SE PROTÉGER ET RÉAGIR FACE AUX ARNAQUES AU FAUX SUPPORT TECHNIQUE

Qu'est-ce que l'arnaque au faux support technique ?

L'arnaque au faux support technique consiste à effrayer les victimes en indiquant un problème technique grave sur leur ordinateur afin de les pousser à payer pour un dépannage informatique fictif.

Comment se déroule l'arnaque ?

1. Le message surgit
Il occupe tout l'écran de votre ordinateur et vous demande d'appeler un numéro de téléphone.

2. Vous appelez
(il ne faut surtout pas !)
Le faux technicien vous rassure et vous recommande de suivre ses instructions.

3. Il vous demande d'installer un logiciel
qui lui donne le contrôle de votre ordinateur.

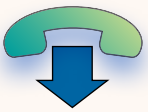
4. Il fouille votre appareil
Il peut voler vos mots de passe, documents personnels, photos et même installer des logiciels malveillants.

5. Il vous demande de l'argent
pour payer cette "intervention" (souvent plusieurs centaines d'euros). Parfois, il tente d'accéder directement à vos comptes bancaires ou vous fait croire qu'ils sont piratés, puis vous manipule pour valider des paiements ou des virements frauduleux.

Que faire si cela vous arrive ?

1. 

SURTOUT, N'APPELEZ PAS LE NUMÉRO INDIQUÉ !

2. 

Si vous êtes appelé(e), raccrochez immédiatement.
Les véritables entreprises, comme Microsoft, ne vous appellent jamais par elles-mêmes.

3. 

Ne faites **aucune manipulation** sur votre ordinateur si l'on vous y pousse par téléphone.

4. 

Essayez de fermer la fenêtre
(la touche "Échap" sur le clavier de votre ordinateur). Si vous y arrivez : **BRAVO !** Vous avez déjoué l'arnaque.

5. 

Si votre ordinateur semble bloqué
ÉTEIGNEZ VOTRE APPAREIL ET REDÉMARREZ-LE
Maintenez le bouton d'alimentation enfoncé si besoin.

6. Si le message réapparaît après redémarrage, demandez de l'aide à un proche ou **faites appel à un professionnel référencé sur la page diagnostic de Cyberbermalveillance.gouv.fr**

aka.ms/17Cyber-Diagnostic

Que faire si vous avez déjà appelé et suivi les instructions ? >

1. **Désinstallez immédiatement**
   toute nouvelle application suspecte que le faux technicien vous a fait installer.

2. **Conservez toutes les preuves**
   prenez des photos du message, des factures si vous avez payé, des num. de téléphone appelés, références du faux technicien.

3. Si vous avez fourni vos coordonnées bancaires :
   contactez immédiatement votre banque pour faire opposition
   et signaler la fraude.

4. Reportez votre problème à Cybermalveillance sur la page internet d'assistance
   cybermalveillance.gouv.fr/17cyber

5. **Déposez plainte**
   au commissariat de police, à la brigade de gendarmerie, ou écrivez au Procureur de la République.

Comment vous protéger pour l'avenir ?

- **Faites régulièrement les mises à jour** de votre ordinateur.
- **Utilisez un antivirus.**
- **Optez pour une navigation prudente** en évitant les sites non sûrs ou illicites. Soyez vigilant face aux liens publicitaires.
- **N'installez jamais d'applications d'origine douteuse.**
- **N'ouvrez pas les pièces jointes** et ne cliquez pas sur les liens **dans les messages dont vous n'êtes pas certain de l'origine.**
- **Faites des sauvegardes régulières** de vos données importantes (photos, documents) sur un support externe (disque dur, clé USB) ou un service en ligne sécurisé.
- **Rappelez-vous : aucun support technique officiel ne vous contactera spontanément.**

Pour plus de conseils et pour trouver des professionnels près de chez vous, consultez le site officiel :

AKA.MS/17CYBER