

Arnaque au faux support technique

L'arnaque au faux support technique est une pratique courante qui a première vue peut faire peur. Ce tutoriel permet de s'en débarrasser facilement.

 Difficulté Facile

 Public Grand public

 Licence CC-BY-SA

 Type de contenu

Mediation

Sommaire

Introduction

Étape 1 - Fausse alerte

Étape 2 - Bonne pratiques

Commentaires

Introduction

Comment :

Apparition d'un message qui bloque l'ordinateur, indiquant un problème technique grave afin de pousser à contacter un prétendu support technique officiel.

Objectif :

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

Étape 1 - Fausse alerte

Sur cette image, un message apparaît faisant croire que l'ordinateur est infecté par un virus.

L'escroc se fait passer pour Windows et invite l'utilisateur à ne pas éteindre l'ordinateur et appeler le soi-disant support technique pour résoudre le problème, au risque de perdre des données importantes (mots de passes, informations bancaires, fichiers).



Cette page qui bloque le PC est bien souvent accompagnée d'une alarme intempestive qui a pour objectif que l'utilisateur appelle le numéro indiqué.

Votre ordinateur a été verrouillé

Votre ordinateur nous a averti qu'il était infecté par un virus et un logiciel espion. Les données suivantes sont à risque :

- Identifiant Facebook, identifiants de messagerie
- Information de carte de crédit, accès bancaires
- Fichiers sur cet ordinateur

Ne redémarrez pas votre ordinateur et contactez Windows, sinon nous ne pourrions garantir la sécurité de vos données.



Pour plus d'informations sur ce problème et sur les solutions possibles, consultez le site <https://www.windows.com/topcode>

Si vous contactez l'assistance, transmettez leur ces informations :

Code d'arrêt : SPYWARE

Appelez le support technique Windows: 09 77 19 94 56
(Appel gratuit)

Étape 2 - Bonne pratiques

Pour éviter de tomber dans le piège de cet arnaque qui est de vous vendre et vous installer un soit-disant pack de sécurité, voici les recommandations :

- S'il semble « bloqué », redémarrez votre appareil. Cela peut suffire à régler le problème.
- N'appellez pas le numéro indiqué

source de l'image : cybermalveillance.gouv.fr

