SYNDESIN
ACCOMPAGNEMENT NUMERIQUE

Mes fiches mémos

INTRODUCTION

Il y a des cybercriminalités qui effraient plus que d'autres. C'est notamment le cas de l'arnaque au faux support technique, où vous vous retrouvez démuni face au blocage de votre appareil et l'affichage d'un message qui veut voir faire croire que vous avez un virus et que vous risquez de perdre des données ou l'usage de votre équipement.

Pour vous prémunir de ce type de cybermalveillance, voici quelques conseils-phares pour savoir **comment éviter au mieux les arnaques au faux support technique et en réduire les dommages si vous en êtes tout de même victime.**

QU'EST-CE QU'UNE ARNAQUE AU FAUX SUPPORT TECHNIQUE ?

Une arnaque au faux support technique a pour objectif de pousser une victime potentielle à contacter un prétendu support technique officiel et connu comme Microsoft, Apple, ou Google, par exemple. Le cybercriminel tente ensuite de **convaincre la victime de payer un pseudo-dépannage technique informatique et/ou d'acheter des logiciels** inutiles, voire nuisibles.

Le mode opératoire d'une arnaque au faux support technique est bien souvent le même :

- En naviguant sur Internet, la victime peut se retrouver sur une page qui lui indique **un problème technique grave (bien souvent que son PC est infecté)** et qui bloque son navigateur. La page affiche un message qui alerte sur le fait que la victime risque de perdre ses données ou l'usage de son équipement.

- Un numéro de téléphone d'un faux support technique est alors affiché sur la page avec un message qui incite la victime à le rappeler.

- Par la suite, au téléphone, l'arnaqueur va demander à la victime de **télécharger un logiciel de prise en main à distance** qui lui permettra de reprendre le contrôle de l'ordinateur. Une fois qu'il a pris le contrôle, il effectuera quelques manipulations pour lui faire croire qu'il "nettoie" l'ordinateur de la victime.

- L'arnaqueur va ensuite proposer d'installer d'autres logiciels. Bien souvent, il s'agit de soit-disant antivirus ou de logiciels de sécurité. Cela peut également être de vrais logiciels mais avec de fausses clés de licence.

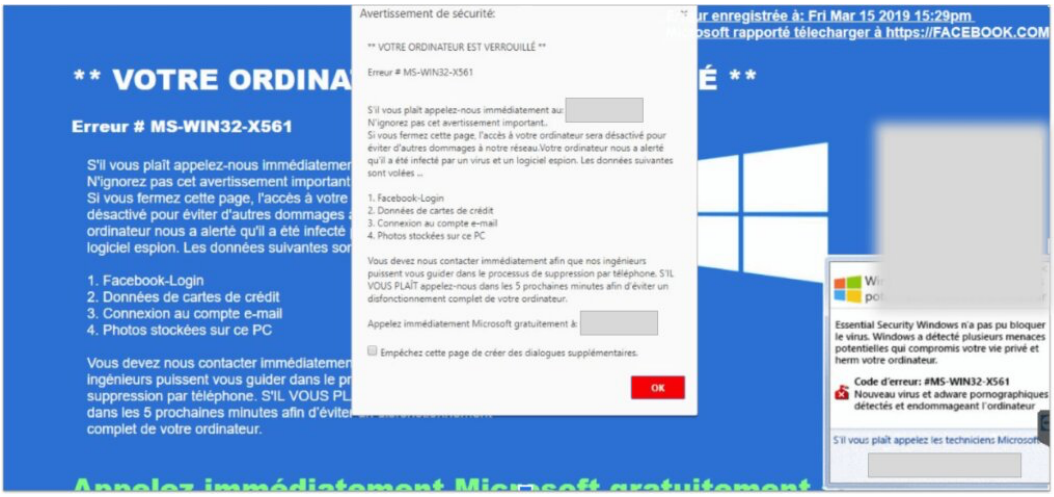
- À l'issue de la conversation téléphonique, **l'arnaqueur demande le paiement de la prestation** : les montants peuvent aller de 100 à plusieurs centaines d'euros.

SACHEZ RECONNAITRE UNE ARNAQUE AU FAUX SUPPORT TECHNIQUE

Sachez tout d'abord **qu'aucun support technique officiel ne vous contactera jamais pour vous réclamer de l'argent.** Si c'est le cas, il s'agit clairement d'une arnaque.

Les pages d'arnaques au faux support technique sont aisément reconnaissables. Tout y est fait pour être anxiogène pour la victime : ses couleurs sont criardes, et les messages d'alerte qui s'y affichent peuvent être très angoissants.

Un exemple de page d'arnaque au faux support technique :



ÉVITEZ LES SITES NON SURS OU ILLICITES

Certains sites sont des espaces sur Internet où les arnaques sont particulièrement courantes. L'un des conseils les plus évidents est donc d'éviter **de vous rendre sur des sites non sûrs ou illicites.** Ces sites peuvent infecter votre machine ou héberger des régies publicitaires douteuses. Parmi ces sites, on compte notamment :

- Les sites qui hébergent des contrefaçons de logiciels
- Les sites de téléchargement ou de streaming illégaux
- Certains sites pornographiques

Prenez également garde **à ne pas ouvrir les courriels et leurs pièces jointes, et à ne pas cliquer sur leurs liens lorsque** :

- Les virus par messagerie – Cybermalveillance.gouv.fr
- Il s'agit d'une chaîne de messages
- Vous ne connaissez pas l'expéditeur
- Vous connaissez l'expéditeur, mais la structure du message est inhabituelle ou vide.

Enfin, **n'installez pas d'application ou de programme "piratés"**, ou dont l'origine ou la réputation sont douteuses. Eux aussi sont bien souvent infectés.

https://www.dailymotion.com/video/x5s2fp2

APPLIQUEZ LES BONNES PRATIQUES DE SECURITE TECHNIQUE

Quelques pratiques simples à adopter lorsque vous utilisez vos machines et que vous naviguez sur Internet sont essentielles pour éviter au mieux les arnaques au faux support technique, et plus généralement tous les types de cybermalveillance.

- Pour naviguer sur Internet ou consulter vos messages, **n'utilisez pas un compte avec des droits "administrateur" mais préférez un compte utilisateur. En effet, un compte administrateur possède des permissions élevées sur votre ordinateur, ce qui facilitera la tâche du cybercriminel** pour prendre le contrôle de votre machine, et/ou y installer des logiciels malveillants ou inutiles.

- Appliquez de manière régulière et systématique **les mises à jour de sécurité du système d'exploitation de votre appareil et des logiciels installés sur votre machine**, en particulier vos navigateurs Internet. Les cyber-criminels peuvent exploiter des failles de sécurité contenues dans leurs versions non mises à jour pour vous approcher et vous arnaquer.

- **Tenez à jour votre antivirus et activez votre pare-feu.** Vérifiez qu'il ne laisse passer que des applications et des services légitimes. Pour en savoir plus, consultez notre article « Comment se protéger sur Internet ? »

FAITES DES SAUVEGARDES REGULIERES DE VOTRE SYSTEME

Les arnaques au faux support technique jouent sur une crainte très spécifique : celle qu'a la victime de perdre le contrôle de sa machine, mais aussi de ses données personnelles ou professionnelles. En sauvegardant régulièrement votre système sur un stockage externe par exemple, vous pourrez éventuellement **le réinstaller dans son état d'origine** si besoin.

Pour protéger vos données, il est également conseillé de les sauvegarder régulièrement. Ainsi, si elles sont effacées ou dégradées, vous en aurez conservé une copie sur un support de stockage externe ou sur un service en ligne.

https://www.dailymotion.com/video/x7n00wg

VICTIME D'ARNAQUES PAR MESSAGE ELECTRONIQUE : COMMENT REAGIR ?

Il arrive que, malgré les précautions, l'on réponde à une demande par courriel qui semblait légitime. Dans ce cas, voici les premiers réflexes à adopter :

- si vous avez envoyé **un mot de passe**, changez-le immédiatement sur le site usurpé et partout où vous l'auriez utilisé.
- si ce mot de passe concerne votre mot de passe d'adresse de messagerie, changez immédiatement votre mot de passe de messagerie ainsi que tous les mots de passe des comptes connectés à l'adresse de messagerie concernée.
- si vous avez transmis **des informations bancaires** ou si vous constatez **des débits frauduleux** sur votre compte, faites opposition à votre carte et déposez une plainte au commissariat de police ou à la gendarmerie la plus proche.
- de même, déposez plainte si vous constatez que **des éléments personnels servent à usurper votre identité**.

Si vous avez repéré l'arnaque avant d'envoyer vos données personnelles, celles-ci ne sont a priori pas en danger.

Enfin, notre dernière recommandation vaut à chaque fois que vous faites face des tentatives d'arnaques par message électronique : **signalez-les !** Pour cela, utilisez la plateforme de signalement Signal Spam. Vous pouvez ainsi contribuer à stopper les arnaques par hameçonnage et éviter que de nombreuses personnes se fassent piéger.
Une fois que vous aurez entrepris les démarches nécessaires et noté toutes les informations utiles relatives au message d'arnaque (comme l'adresse de messagerie de l'expéditeur, etc.), veillez **à supprimer le message** de votre système de messagerie.

En cas de doute ou de problème persistant concernant la sécurité de vos données, n'hésitez pas à solliciter l'aide de spécialistes. Pour être conseillé dans vos démarches, contactez la **plateforme Info Escroqueries** du ministère de l'Intérieur au 0 805 805 817 (numéro gratuit). Le service est ouvert de 9h à 18h30 du lundi au vendredi.

CONCLUSION

Il est essentiel de se tenir informé pour comprendre et éviter le risque d'arnaques par hameçonnage. N'hésitez pas **à expliquer les principes de précaution à vos proches, enfants, etc**.

Notre dernier conseil : restez vigilant(e) ! Les pratiques évoluent rapidement. Vous savez désormais comment vous prémunir et réagir en cas d'arnaques via messages électronique, mais des escroqueries similaires se déploient sur d'autres médias, comme les appels téléphoniques.