LES FRAUDES AUX FAUSSES RÉPARATIONS INFORMATIQUES OU « FAUX SUPPORTS TECHNIQUES »

Le mode opératoire

Les victimes à l'occasion d'une navigation sur internet sont inopinément interrompues par **un message de sécurité anxiogène** ayant les apparences d'une fenêtre d'alerte légitime du système d'exploitation. Ce message est fréquemment généré par le navigateur internet.
Cette alerte peut faire état de la présence d'un maliciel ou de tout autre forme de problème technique a priori en dehors du champ de compétence de l'utilisateur moyen. **Cette alerte incite la victime à contacter un service de support technique afin de remédier à la difficulté fictive avec l'aide d'un téléopérateur.** Le message comporte généralement une contrainte temporelle indiquant qu'à l'expiration d'un délai de quelques minutes l'appareil compromis sera rendu inutilisable à moins de contacter le service indiqué.

MESSAGE DE PRÉVENTION

1- 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.

2- Tenez à jour votre antivirus et activez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications et services légitimes.

3- 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.

4- N'installez pas d'application ou de programme « piratés », ou dont l'origine ou la réputation sont douteuses.

5- N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.

6- 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.

7- Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine.

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

Source : plateforme Cybermalveillance.gouv.fr

Je suis victime, que faire ?

- **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, **purger le cache, supprimez les cookies, réinitialiser 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 http://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/.

- **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.