OUCH ! Janvier 2026

Les arnaques par assistance technique : la seule chose dont ils s'occupent est votre compte en banque

Comment un appel "utile" peut vous coûter cher

Aisha travaillait de chez elle lorsque une fenêtre est apparue sur son écran: **" *Votre système d'exploitation Windows n'est plus pris en charge et semble être infecté ! Vos informations personnelles, vos informations bancaires, et d'autres données sensibles sont probablement comprises. Pour votre sécurité, veuillez contacter l'assistance technique Windows immédiatement. Appelez maintenant au : 1-8XX-XXX-XXXX"***

Inquiète de perdre ses finances et ses fichiers, Aisha a appelé le numéro. Après une courte attente, un "technicien" qui semblait professionnel a répondu et lui a assuré qu'il pouvait régler le problème à distance. Il l'a guidé pour télécharger un "logiciel de sécurité" qui lui permettrait de scanner son système. Elle a vu apparaître sur son écran des dizaines de faux "virus". Le technicien lui a expliqué que son ordinateur était "extrêmement infecté", mais que pour 375$, il pouvait le nettoyer et le sécuriser. Soulagée, Aisha a payé avec sa carte de crédit.

Plus tard dans la semaine, sa banque l'a alertée de plusieurs prélèvements non autorisés sur son compte. C'est à ce moment-là qu'Aisha a compris que l'équipe de son "assistant technique" sympathique était en réalité une équipe d'arnaqueurs, et qu'ils avaient maintenant accès non seulement à sa carte de crédit, mais également à son ordinateur !

Malheureusement, la situation d'Aisha est fréquente, et c'est exactement de cette manière que beaucoup **d'arnaques par assistance technique** fonctionnent.

Que sont les arnaques par assistance technique ?

Les arnaques par assistance technique se produisent lorsque des criminels convainquent des personnes qu'il y a un problème avec leur ordinateur, leur téléphone ou leur compte en ligne, et qu'elles ont besoin d'une aide immédiate de la part de "l'assistance technique". Les escrocs se font passer pour des entreprises légitimes telles que Microsoft, Apple ou votre banque. Leur but ? **Vous piéger pour que vous leur donniez de l'argent, des informations sensibles, ou un accès à distance à vos appareils ou vos comptes.**

Ces arnaques commencent souvent par de fausses alertes de mise à jour du navigateur ou du système d'exploitation, des appels téléphoniques ou des SMS affirmant que votre ordinateur est infecté ou que votre compte a été piraté. Peu importe la manière dont ils commencent, leur but est de créer un sentiment de panique et de vous faire croire que vous devez agir **immédiatement**.

Que cherchent-ils ?

Les escrocs par assistance techniques cherchent trois choses :

1. **Votre argent :** Ils peuvent facturer la "réparation" de problèmes inexistants, exigeant souvent un paiement par carte-cadeau, virement bancaire ou cryptomonnaie, des méthodes difficiles à retracer.
2. **Vos informations :** Ils vous demandent votre nom, votre adresse, vos mots de passe ou vos coordonnées bancaires sous prétexte de vérifier votre identité ou de traiter un remboursement.

3. **Accéder à votre appareil ou à vos comptes :** En arrivant à vous convaincre d'installer un logiciel qui leur donne un accès à distance, les escrocs peuvent espionner votre activité, voler vos fichiers ou installer de réels maliciels pour des attaques futures.

Comment ces arnaques fonctionnent

Les arnaques par assistance technique reposent sur **l'ingénierie sociale** en manipulant les émotions pour créer la peur et l'urgence. Voici un schéma typique :

1. **Ils obtiennent votre attention en utilisant la peur :** Vous voyez une fenêtre apparaître ou vous recevez un message ou appel vous informant que votre système ou votre compte est corrompu. Le message contient des phrases alarmantes telles que : "Vos données seront perdues !" ou "Votre compte sera suspendu !".
2. **La confiance :**L'escroc se fait passer pour un professionnel d'une entreprise renommée, utilisant même des logos officiels ou des numéros de téléphone falsifiés.
3. **Le contrôle et le paiement :** Il vous demande d'installer un logiciel ou de cliquer sur un lien, lui donnant ainsi accès à votre appareil. Il vous facture ensuite des frais de "réparation" ou de "services de protection". Même si vous vous rendez compte de l'arnaque et que vous vous déconnectez, il peut toujours avoir accès à vos données ou votre appareil.

Comment vous protéger

1. **Restez calme et réfléchissez :** Les vraies entreprises ne font **pas** apparaître de fenêtre d'avertissement ou ne vous appellent pas sans prévenir. Si un problème vous semble urgent ou effrayant, prenez du recul et vérifiez les informations séparément.
2. **N'appelez jamais les numéros sur des fenêtres qui apparaissent sur votre ordinateur :** Si un message d'avertissement s'affiche dans une fenêtre contextuelle, fermez votre navigateur. Ne cliquez pas sur le numéro ou le lien affiché.
3. **Ne donnez jamais un accès à distance :** Ne permettez jamais à une personne que vous ne connaissez pas d'accéder à distance à vos appareils ou à vos comptes. Si elle vous a contacté ou vous pousse à lui donner un accès, c'est une arnaque.
4. **Contrôlez et sécurisez vos comptes :** Si vous pensez avoir interagi avec un escroc, changez immédiatement vos mots de passe et contrôlez vos comptes bancaires.

Dernières réflexions

Les arnaques par assistance technique exploitent la peur, l'urgence et la confiance. Elles peuvent arriver à n'importe qui, peu importe l'expérience technique. N'oubliez pas : **les entreprises légitimes n'appelleront jamais, n'enverront jamais d'emails, et n'afficheront jamais de fenêtre sur votre ordinateur vous demandant un accès à distance ou des frais pour régler un problème.** Rester calme et à l'affût est votre meilleure défense.

Rédacteur invité

Jennifer Cox est directrice du conseil en solutions chez Tines, une entreprise d'automatisation intelligente qui transforme les opérations de cybersécurité. Leader maintes fois récompensée dans le domaine de la cybersécurité, elle se passionne pour l'accompagnement des futurs professionnels du secteur et la promotion de l'innovation, de l'excellence et de l'inclusion au sein des équipes techniques de l'écosystème mondial de la cybersécurité et de l'automatisation. https://www.linkedin.com/in/jennifermcox/

Ressources

Le pouvoir de la mise à jour : https://www.sans.org/newsletters/ouch/power-updating/
Comment les cyber-criminels exploitent vos émotions : https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
Le pouvoir des phrases de passe : https://www.sans.org/newsletters/ouch/power-passphrase/

Traduit pour la communauté par : Juliette Busson

Vous pouvez trouver plus de contenu OUCH! Sur le lien suivant : https://www.sans.org/newsletters/ouch