OUCH! Novembre 2023

Votre bulletin mensuel sur la sensibilisation à la sécurité

J’ai été piraté, et maintenant ?

Ai-je été piraté ?

L'internet peut être une source d'inquiétude, les nouvelles technologies évoluant sans cesse. Quelle que soit la protection que vous vous efforcez d'apporter, vous risquez tôt ou tard d'être victime d'un piratage. Plus tôt vous détectez un problème et plus vite vous y répondez, plus vous pouvez en minimiser l'impact. Vous trouverez ci-dessous des signes indiquant que vous avez peut-être été piraté et, si c’est le cas, des suggestions pour y remédier.

Indices qu’un de vos comptes a été piraté

- Votre famille ou vos amis disent qu’ils ont reçu des messages ou des invitations inhabituels de votre part et vous savez que vous n’avez rien envoyé.
- Le mot de passe de l’un de vos comptes ne fonctionne plus, alors que vous savez que ce mot de passe est correct.
- Vous recevez des notifications de sites vous informant que quelqu’un s’est connecté à votre compte et vous savez que ce n’est pas vous.
- Vous recevez des e-mails confirmant des modifications de votre profil en ligne que vous n'avez pas effectuées.

Indices de piratage de votre ordinateur ou de votre appareil mobile

- Votre programme antivirus génère une alerte pour vous signaler que votre système est infecté. Assurez-vous que ce soit bien votre logiciel antivirus qui génère l’alerte et que ce ne soit pas une fenêtre pop-up venant d’un site essayant de vous berner pour que vous appeliez un numéro ou installiez quelque chose. Vous n’êtes pas sûrs ? Ouvrez et vérifiez votre programme antivirus pour savoir si votre ordinateur est vraiment infecté.
- Quand vous naviguez sur internet, vous êtes souvent redirigé vers des pages que vous ne vouliez pas visiter ou bien de nouvelles pages indésirables apparaissent.
- Vous avez une fenêtre pop-up vous informant que votre ordinateur a été chiffré et que vous devez payer une rançon pour récupérer vos dossiers.

Indices que votre carte de crédit ou vos finances ont été piratées

- Il y a des frais douteux ou inconnus sur votre carte de crédit ou votre compte en banque qui ne viennent pas de vous.

Et maintenant ? - Comment reprendre le contrôle

Si vous pensez avoir été piraté, restez calme. Vous vous en sortirez. Si le piratage est en lien avec votre travail, n'essayez pas de régler le problème vous-même ; signalez-le immédiatement. Au contraire, il faut le signaler immédiatement. Si c'est votre système ou compte personnel qui a été piraté, voici quelques étapes que vous pouvez suivre :

- **Récupérer vos comptes en ligne :** Si vous avez toujours accès à votre compte, connectez-vous à partir d'un ordinateur de confiance et réinitialisez votre mot de passe avec un nouveau mot de passe unique et fort - plus il est long, mieux c'est. Si vous n'avez pas activé l'authentification multifactorielle (MFA), c'est le moment de le faire. Si vous n'avez plus accès à votre compte, contactez le site et informez-les que votre compte a été piraté. Si vous avez d'autres comptes qui partagent le même mot de passe que votre compte piraté, changez également ces mots de passe immédiatement.
- **Récupérer votre ordinateur ou appareil personnel :** Si votre programme d'antivirus ne peut pas réparer votre ordinateur infecté ou que vous voulez être sûr que votre système est sûr, envisagez la possibilité de réinstaller un système d'exploitation et de réparer l'ordinateur. Ou si votre ordinateur ou appareil est vieux, il est peut être temps d'en acheter un nouveau.
- **Impact financier :** Pour les problèmes avec votre carte de crédit ou tout compte bancaire, appelez votre banque immédiatement. Plus tôt vous les appellerez, plus vous aurez de chances de récupérer votre argent. Appelez-les en utilisant un numéro sûr comme le numéro inscrit au dos de votre carte bleue, celui sur votre relevé bancaire ou même celui sur le site. Surveillez vos relevés bancaires régulièrement. Si possible, activez les notifications automatiques à chaque fois qu'il y a un prélèvement ou un transfert d'argent.

Que faire pour garder une longueur d'avance sur les cyberattaquants ?

Le bulletin d'information OUCH Security Awareness est publié tous les mois et comporte une série complète sur la manière de se protéger. Dans la section Ressources ci-dessous, nous dressons la liste des bulletins d'information OUCH les plus importants à lire pour se protéger. Ces ressources se concentrent sur trois étapes clés:

1. Maintenez tous vos systèmes et appareils à jour et à la dernière version.
2. Utilisez des mots de passe forts et uniques pour chacun de vos comptes, gérez ces comptes à l'aide d'un gestionnaire de mots de passe et activez le MFA.
3. Soyez méfiants - restez attentifs aux tactiques d'ingénierie sociale telles que les e-mails d'hameçonnage (phishing).

Rédacteur Invité

Sarah Morales (@SarahManley) est gestionnaire de programme senior au sein de l'équipe de Google chargée de la protection de la vie privée, de la sécurité et de la sûreté. Elle dirige l'engagement externe en mettant l'accent sur la création de communautés, de collaborations et de partenariats. Elle est membre du conseil d'administration de Wicys et participe activement aux efforts de l'IED au sein de la communauté de la cybersécurité.

Ressources

Gestionnaires de mots de passe : https://www.sans.org/newsletters/ouch/power-password-managers
MFA : une étape simple pour sécuriser vos comptes : https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
Déclencheurs émotionnels - comment les cyber-attaquants vous piègent-ils ? :
https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Les attaques par hameçonnage deviennent de plus en plus travaillées :
https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

Traduit pour la communauté par : Juliette Busson