Comment les pirates peuvent violer votre vie privée

Les pirates peuvent violer la vie privée de plusieurs façons. Voici quelques techniques courantes que les pirates utilisent pour compromettre la vie privée des individus :

1. **Phishing** : les pirates utilisent des e-mails de phishing pour inciter les gens à fournir leurs informations sensibles, telles que les identifiants de connexion, les numéros de carte de crédit ou d'autres informations personnelles. Ils peuvent utiliser ces informations pour accéder aux données privées de la victime.
2. **Logiciels malveillants** : les pirates peuvent infecter l'ordinateur ou le smartphone d'une victime avec des logiciels malveillants, ce qui peut lui permettre d'accéder aux fichiers personnels, aux frappes au clavier et à d'autres informations sensibles de la victime.
3. **Devinette de mot de passe** : les pirates peuvent utiliser des attaques par force brute ou d'autres techniques pour deviner le mot de passe d'une victime, ce qui peut leur permettre d'accéder aux comptes et aux informations personnelles de la victime.
4. **Ingénierie sociale** : les pirates peuvent utiliser des techniques d'ingénierie sociale pour inciter les victimes à révéler leurs informations personnelles, par exemple en se faisant passer pour quelqu'un d'autre ou en gagnant la confiance de la victime.
5. **Wi-Fi non sécurisé** : les pirates peuvent intercepter et espionner les réseaux Wi-Fi non sécurisés, ce qui leur permet de voir l'activité en ligne de la victime et d'accéder potentiellement à ses informations personnelles.
6. Accès physique : les pirates peuvent accéder physiquement à l'ordinateur ou à un autre appareil d'une victime, ce qui lui permet d'installer des logiciels malveillants ou d'accéder à des données sensibles.

Dans l'ensemble, il est important que les individus prennent des précautions pour protéger leur vie privée, comme l'utilisation de mots de passe forts, la prudence face aux tentatives de phishing et l'évitement des réseaux Wi-Fi non sécurisés.

A - sur un ordinateur

Le monde de la technologie est en constante évolution, tout comme notre relation avec Internet. Dans les années 1990, la seule chose dont vous deviez apparemment vous soucier était votre e-mail. Ensuite, vous avez commencé à effectuer des opérations bancaires en ligne et maintenant, votre smartphone est connecté, vous avez Facebook… et presque toute votre vie est en ligne. Et vous êtes toujours suivi. Votre historique de navigation complet est stocké par votre FAI, suivi par Facebook et peut-être d'autres annonceurs. Même vos appareils IoT pourraient vous signaler . Donc, garder les choses privées est déjà une grande question - avant même que les pirates ne s'en mêlent..

Quelles informations sont disponibles pour les pirates ?

Vous n'avez peut-être pas réalisé à quel point vos informations personnelles sont disponibles sur Internet. Passons en revue certains des types d'informations qui s'y trouvent et pourquoi les pirates pourraient être intéressé

1. **PII** - **Informations personnellement identifiables**. Cela inclut votre nom, adresse, adresse e-mail, SSN, numéro fiscal, date de naissance, dossiers médicaux, dossiers scolaires, emploi. Il y a beaucoup dans ce type de données qu'un pirate pourrait utiliser pour voler votre identité. Il peut inclure des détails sur les achats que vous avez effectués sur Amazon ou sur les investissements effectués avec un courtier en ligne. Toutes ces informations privées pourraient également être utilisées pour compromettre vos autres comptes en ligne.
2. **Les e-mails**, SMS et messages instantanés sont tous conservés sur des serveurs quelque part. Il peut y avoir beaucoup d'informations dans vos e-mails que vous ne voulez pas que le monde voie - documents commerciaux confidentiels, lettres d'amour, détails de vos comptes bancaires. Et les pirates seront également intéressés par vos contacts, car s'ils peuvent les obtenir, ils peuvent envoyer des e-mails de phishing à tous ceux que vous connaissez.
3. **Vos données de navigation** incluent des cookies, des journaux de FAI et des plug-ins de navigateur susceptibles de stocker des données. C'est utile pour les annonceurs, et avec l'avènement du Big Data, cela pourrait être plus utile que vous ne le pensez.
4. **En temps réel**, vous utilisez peut-être Internet pour passer un appel Skype ou pour une visioconférence. Es-tu sûr que personne n'écoute

Vous ne réalisez peut-être même pas que certains de ces détails ont été stockés. Ou vous pouvez être ennuyé par la façon dont Facebook veut dire à vos amis ce que vous venez d'acheter ou d'écouter, ou la façon dont le LA Times vous montre des publicités pour quelque chose que vous avez recherché il y a deux semaines.

Les hackers font constamment évoluer leurs techniques. Par exemple, le phishing est une méthode standard depuis plus d'une décennie, qui consiste à envoyer de faux e-mails qui vous demandent de vous connecter à un site Web usurpé qui ressemble à un site Web en lequel vous avez confiance ou qui contient des liens qui installent des logiciels malveillants sur votre ordinateur. Mais maintenant, les faux liens sur les réseaux sociaux et les comptes de réseaux sociaux piratés servent également de moyens d'empiéter sur votre vie privée et de voler vos données.

Le Wi-Fi public est une chose merveilleuse, vous permettant de travailler à partir de n'importe quel Starbucks, mais c'est aussi une énorme vulnérabilité de sécurité. Les points d'accès non protégés offrent aux pirates un autre moyen de pénétrer dans

votre appareil et de voler vos données. Étant donné que les pirates constituent une menace massive pour votre vie privée en ligne, que pouvez-vous faire à ce sujet ?

Utilisez un VPN pour vous protéger contre les pirates

Le Wi-Fi public ne nécessite pas d'authentification pour y accéder. C'est très bien pour vous, et c'est très bien pour les pirates, car ils n'ont pas non plus besoin d'authentification. Ils peuvent utiliser des attaques Man-in-the-Middle (MTM) pour voler vos données ou, dans certains cas, ils peuvent même configurer un point d'accès Wi-Fi «honeypot» pour aspirer vos données.

Si vous avez besoin d'une connexion Wi-Fi pour votre ordinateur portable, il peut être préférable de partager votre connexion mobile 4G en configurant votre mobile en tant que point d'accès Wi-Fi et en laissant votre ordinateur portable s'y connecter en toute sécurité.

Mieux encore, utilisez un réseau privé virtuel (VPN) , qui crée pour vous une passerelle privée vers Internet.

Comment un VPN empêche-t-il le piratage ?

En redirigeant votre trafic Internet pour dissimuler votre adresse IP, il est impossible de vous suivre. Et en cryptant les informations que vous envoyez sur Internet ; il empêche toute personne souhaitant intercepter vos informations de pouvoir les lire. Cela inclut votre FAI. Ainsi, un VPN est un très bon moyen de protéger votre vie privée en ligne.

Un VPN n'est pas seulement bon pour votre confidentialité et votre sécurité en ligne ; il a quelques autres avantages. Il peut vous permettre de visiter des sites Web qui peuvent être bloqués par le fournisseur Wi-Fi - dans certains endroits, cela inclut Facebook et Twitter. Et parce qu'il peut accéder au contenu bloqué par géolocalisation, il peut être utile si vous voyagez à l'étranger et que vous souhaitez accéder à des comptes financiers qui peuvent être bloqués pour les utilisateurs « étrangers ».

Vous pouvez obtenir des VPN gratuits - mais ils peuvent être assortis de conditions. Si vous voulez vraiment protéger votre vie privée en ligne, vous devez utiliser un **VPN premium** ; ça vaut le coup de payer.

Comment le cryptage protège votre vie privée

Vous pouvez également envisager d'utiliser le cryptage pour protéger votre vie privée en ligne. En fait, vous le faites probablement déjà dans une certaine mesure, car les entreprises qui traitent vos données les chiffrent parfois. Votre banque, par exemple, utilise probablement le cryptage sur son site Web, via des certificats SSL et TLS .

Si vous voyez un cadenas au début de la barre d'adresse de votre navigateur, le lien entre votre navigateur et le serveur est crypté. Si vous remplissez un formulaire sans le cadenas, un pirate pourrait attacher un programme malveillant au serveur qui héberge le site Web qui pourrait écouter vos communications et voler vos données. Si vous le remplissez *avec* SSL/TLS, personne ne peut écouter.

Une autre façon de savoir si un site Web utilise SSL/TSL est de savoir si l'URL commence par https:// plutôt que par http://. HTTPS est un protocole beaucoup plus sûr que HTTP. N'oubliez pas, cependant, que le cryptage ne fait que protéger votre communication. Une fois que vos informations se trouvent sur le serveur de l'entreprise, elles peuvent être vulnérables à toute attaque sur le réseau de l'entreprise.

Il convient également de savoir que les appels téléphoniques sur **Skype** sont cryptés à 100 % - tant qu'ils sont passés à 100 % sur Skype. Mais si vous passez un appel Skype vers un numéro de téléphone ordinaire, le lien sur le RTPC (réseau téléphonique ordinaire) n'est pas crypté. Cela pourrait permettre à quelqu'un d'écouter. Vous pouvez également profiter du cryptage de vos messages sur Facebook, en utilisant des «conversations secrètes», si vous êtes sur un iPhone ou un smartphone Android - mais pas sur votre PC ou votre ordinateur portable.

L'une des raisons pour lesquelles WhatsApp est devenu si populaire est son cryptage de messagerie de bout en bout. D'autres applications offrent le cryptage mais ne l'activent pas en standard. Cherchez le réglage pour l'activer - pourquoi diable ne le voudriez-vous pas ?

Vous pourriez également être intéressé par l'utilisation de **Tor**, un réseau de navigateur anonyme et crypté, pour éviter que votre historique de navigation ne soit suivi. Les journalistes d'investigation utilisent souvent Tor, tout comme les ONG qui travaillent dans des environnements hostiles. Cependant, Tor n'est pas parfaitement sûr ; il est connu pour diffuser des logiciels malveillants, et il est toujours vulnérable aux attaques de type "man in the middle".

Le cryptage est un avantage considérable lorsque vous souhaitez protéger votre vie privée en ligne. Mais les gouvernements ne sont pas toujours d'accord. Certains tentent de forcer les fournisseurs de technologie à inclure une porte dérobée permettant à l'agence de sécurité d'accéder aux données. Le problème, bien sûr, est que dès que vous laissez une porte dérobée ouverte, les pirates essaieront d'y pénétrer.

Réduisez votre empreinte numérique pour protéger votre vie privée

Lorsque vous réfléchissez à la manière de protéger votre vie privée en ligne, pensez à réduire votre empreinte numérique. Nous avons tellement l'habitude de publier des

photos en ligne , de dire à nos amis ce que nous venons d'écouter ou d'où nous avons été sur les réseaux sociaux… Nous ne pensons pas toujours où ces informations sont stockées ou à quoi elles pourraient potentiellement être utilisées. .

Cela peut signifier résister à certaines des suggestions faites par les médias sociaux et d'autres sites, comme les balises pour les personnes avec lesquelles vous étiez. Cela peut signifier désactiver les services de localisation pour certains de vos médias sociaux. Élaguer votre présence en ligne peut être très utile pour protéger votre vie privée. Vous pouvez également réfléchir aux moyens suivants de réduire la quantité de vos informations personnelles disponibles sur le Web, et à qui :

- **Gardez vos médias sociaux privés** et limitez vos publications Facebook à vos amis uniquement plutôt que de permettre à quiconque sur Internet d'y accéder.
- **Définissez qui peut vous envoyer des demandes d'amis** , de « n'importe qui » aux « amis d'amis » par exemple.
- **Désactivez la localisation, la reconnaissance faciale, les boutons "centres d'intérêt" et les annonceurs sur les réseaux sociaux** . Certaines plateformes de médias sociaux publieront en fait votre position en ligne, que vous le vouliez ou non - ce n'est pas bon pour votre vie privée, et la publicité "Je ne suis pas chez moi" aux cambrioleurs est un gros risque pour la sécurité. Ou vous pouvez simplement désactiver la géolocalisation en désactivant le GPS de votre téléphone.
- **Désabonnez-vous des anciennes listes de diffusion sur lesquelles vous ne souhaitez pas figurer.** Envisagez d'utiliser une adresse e-mail secondaire pour les achats ponctuels, les demandes de devis d'assurance, etc. Gardez votre e-mail personnel gratuit pour vos amis et votre famille.
- **Soyez prudent avec les appareils Internet des objets (IoT) qui surveillent vos habitudes personnelles** - protégez-les par mot de passe, exécutez-les sur un réseau invité séparé afin qu'ils ne puissent pas être utilisés pour accéder à vos comptes Internet et supprimez les appareils plus anciens ou ceux que vous n'avez pas pas utiliser depuis le réseau.
- **N'hésitez pas à expurger**. Si vous voulez montrer que vous avez réussi votre examen de conduite, par exemple, vous voudrez peut-être publier une photo du résultat de votre test - mais avoir le bon sens de masquer votre adresse, votre numéro de téléphone et d'autres informations d'identification sur la photo.
- **Vérifiez automatiquement ce qui est fait pour vous.** Certaines personnes ne veulent pas que Google enregistre automatiquement les plans de voyage dans leur calendrier, par exemple.

N'oubliez pas que les médias sociaux n'ont pas commencé comme une entreprise de publicité. Il a commencé comme un service qui, selon les utilisateurs individuels, rendait leur vie plus agréable. Tous ces conseils peuvent sembler être un travail

acharné, mais ils ne sont qu'un moyen de récupérer les médias sociaux en tant que service amusant, plutôt qu'une perte de votre vie privée.

Protégez votre vie privée avec un logiciel anti-piratage

Il existe désormais une large gamme de logiciels disponibles pour vous permettre de protéger votre confidentialité et votre sécurité en ligne. Certains visent à empêcher les sites Web de vous suivre, d'autres à empêcher les pirates d'installer des logiciels malveillants sur votre PC ; certains sont disponibles en tant qu'extensions pour votre navigateur Web, tandis que d'autres nécessitent une installation séparée. Peut-être que l'appeler logiciel anti-piratage va un peu loin - cela n'arrêtera pas un pirate informatique déterminé, mais l'utilisation d'un tel logiciel peut rendre très difficile pour un pirate informatique d'accéder à votre ordinateur ou d'accéder à vos données.

Par exemple, les plug-ins de navigateur peuvent être utilisés pour empêcher les sites Web de vous suivre. Facebook vous suit pendant qu'il est ouvert même si vous n'êtes pas sur le site à ce moment-là, rassemblant votre historique de navigation à utiliser pour diffuser des publicités ciblées. C'est peut-être un objectif assez innocent, mais les pratiques de collecte et de partage de données de Facebook ont souvent été critiquées, alors pensez à vous protéger.

Utilisez un bon logiciel anti-virus et anti-malware. Si un cheval de Troie enregistreur de frappe parvient à s'installer sur votre PC, adieu la confidentialité en ligne ! Nettoyer de temps en temps votre PC ou votre téléphone est également une bonne idée ; assurez-vous qu'aucun programme pirate n'écoute.

Vous pouvez également télécharger une application capable d'effacer les données de votre téléphone en cas de perte ou de vol. Si vous synchronisez des appareils Google, vous pouvez déjà supprimer les données de n'importe quel appareil à distance. Ne laissez pas votre liste de contacts ou vos applications bancaires tomber entre les mains de pirates - essuyez simplement le téléphone.

Ce n'est pas strictement un logiciel anti-piratage, mais un bon gestionnaire de mots de passe vaut son pesant d'or. L'utilisation de mots de passe forts et de mots de passe différents pour différents comptes et réseaux est ce que nous recommandons comme précaution de base pour quiconque souhaite minimiser le risque d'intrusion - mais ce n'est pas si facile à faire si vous avez plusieurs comptes à sécuriser. L'utilisation d'un gestionnaire de mots de passe permet de sécuriser vos comptes ; Assurez-vous simplement que vous avez sécurisé votre gestionnaire de mots de passe lui-même avec un mot de passe fort.

Vous pouvez installer toutes ces protections séparément. Vous pouvez également profiter de Total Security de Kaspersky, qui regroupe toute la protection dont vous avez besoin dans un seul ensemble.

Comment protéger votre vie privée

Protéger votre vie privée en ligne signifie assurer la sécurité de vos appareils et de vos réseaux. Nous avons déjà mentionné certaines façons de le faire, comme l'utilisation d'un bon gestionnaire de mots de passe. Cependant, voici quelques conseils supplémentaires qui peuvent vous aider à protéger votre vie privée contre les pirates :

- **Activez l'authentification à deux facteurs sur vos comptes** . Par exemple, lorsque vous utilisez PayPal, vous recevrez un message SMS pour vérifier chaque transaction. D'autres comptes utilisent des marqueurs biométriques tels que les empreintes digitales, les modèles ou même un porte-clés physique ou un dongle pour fournir une deuxième méthode de vérification.
- **Ne téléchargez pas d'applications non officielles sur votre smartphone** - utilisez l'App Store d'Apple ou Google Play.
- **Faites attention aux autorisations que vous accordez aux applications pour smartphone .** Si une application de traitement de texte souhaite utiliser votre caméra et votre microphone, les informations de localisation et les achats intégrés, ainsi que l'accès à votre compte Google, interrogez-la et cherchez pourquoi.
- **Désinstallez les logiciels et les applications que vous n'utilisez plus ou dont vous n'avez plus besoin.**
- **Désactivez "exécuter en tant qu'administrateur" sur tous vos appareils** et ne rootez pas ou ne jailbreakez pas votre téléphone. Cela signifie que si un pirate parvient à prendre le contrôle d'un programme, il ne pourra pas prendre le contrôle du téléphone ou modifier les paramètres et ne pourra probablement pas installer de logiciel sur votre téléphone ou votre ordinateur.
- **Gardez tous vos logiciels à jour.** Les pirates découvrent régulièrement de nouvelles vulnérabilités dans des logiciels et des systèmes d'exploitation obsolètes.
- **Désactivez l'option de remplissage automatique.** C'est une fonction qui fait gagner du temps, mais si c'est pratique pour vous, c'est aussi pratique pour les pirates. Toutes les informations de remplissage automatique doivent être conservées quelque part, par exemple dans le dossier de profil de votre navigateur. C'est le premier endroit où un pirate ira chercher votre nom, votre adresse, votre numéro de téléphone et toutes les autres informations dont il a besoin pour voler votre identité ou accéder à vos comptes.
- **Lorsque vous avez une transaction particulièrement sensible à effectuer, utilisez un VPN** ou un mode de navigation privée.
- **Les téléphones sont petits et faciles à égarer.** Ce sont aussi les cibles préférées des voleurs. Assurez-vous d'avoir un verrouillage d'écran et, comme mentionné ci-dessus, installez un logiciel qui peut effacer votre téléphone s'il est perdu.

- **Configurez votre routeur avec un nouveau nom de routeur et un mot de passe sécurisés** . Si vous modifiez le mot de passe à l'aide de l'authentification WPA, vous avez réduit le risque que quelqu'un pirate votre routeur. Mais pourquoi changer le nom d'utilisateur ? Simple - la plupart des noms d'utilisateur indiquent le type de routeur ou le réseau sur lequel il s'exécute. Changez-le en quelque chose d'autre (de préférence pas votre nom, cependant) et vous privez également les pirates de cette information.
- **N'oubliez pas de vous déconnecter !** Lorsque vous avez fini d'utiliser un compte, déconnectez-vous. Lorsque vous laissez vos comptes fonctionner en arrière-plan, il s'agit d'une faille de sécurité majeure. Heureusement, la plupart des banques déconnectent désormais les clients après un certain temps. Mais la grande menace pour votre vie privée ne vient pas d'eux - elle vient des réseaux sociaux

Ces conseils devraient aider à bloquer toutes les petites portes dérobées que les pirates aiment utiliser pour accéder aux réseaux, aux applications et aux appareils. Avec les autres actions que vous avez entreprises - réduire votre empreinte numérique, utiliser un VPN et utiliser le cryptage - elles devraient vous aider à garder votre vie privée comme vous le souhaitez : privée.

Enfin, si vous vous souciez de protéger votre vie privée en ligne, assurez-vous de vous tenir au courant de la cybersécurité. De nouvelles menaces émergent constamment et de nouvelles façons de faire face à ces menaces émergent en réponse. Tout comme vous mettriez à jour votre logiciel informatique,

Compléments

Ce dont les logiciels malveillants ont besoin pour prospérer

Selon l'institut AV-TEST, plus de 390 000 nouveaux malwares sont détectés chaque jour. Le grand nombre de programmes malveillants donne aux pirates une grande opportunité de choisir leurs cibles. Les utilisateurs commettent souvent les mêmes erreurs courantes qui sont facilement exploitées. Voici un aperçu des 10 principales erreurs commises par les utilisateurs et comment les éviter pour assurer votre sécurité et celle de votre réseau.

1) Cliquer sur des liens douteux

Comme l'a noté Inc., les utilisateurs sont souvent pris au piège des sites "excentriques" par le bouche à oreille virtuel, ou lorsqu'ils téléchargent de la musique ou récupèrent des photos gratuites. Cliquer sur un lien douteux peut ajouter des logiciels malveillants à votre système qui pourraient donner accès à vos informations personnelles, y compris les comptes bancaires et les numéros de carte de crédit. Pour rester en sécurité, restez toujours sur des sites réputés avant de cliquer. Généralement, les liens les plus sécurisés apparaîtront en

haut de toute recherche Google, mais si vous avez un doute, ne cliquez pas sur le lien.

2) Utilisation de lecteurs flash inconnus

La sauvegarde de vos fichiers et de votre système est importante, mais soyez toujours prudent lorsque vous insérez la clé USB ou la clé USB de quelqu'un d'autre dans votre ordinateur. Les disques externes peuvent être remplis de logiciels malveillants, et tout ce qu'il faut, c'est qu'un disque "laissé derrière" bien placé infecte tout un réseau. L'essentiel : si ce n'est pas votre appareil, ne l'utilisez pas. Analysez régulièrement votre appareil à la recherche de virus et d'autres programmes malveillants pour vous assurer que vous n'infectez pas d'autres machines.

3) Téléchargement d'un logiciel antivirus non sollicité

Tout le monde est tombé sur un avertissement contextuel indiquant que votre PC sera en danger à moins que vous ne téléchargiez immédiatement un logiciel antivirus **gratuit**. Les pirates sont des experts pour vous faire télécharger des fichiers avant que vous ne sachiez ce qui se passe, et l'une de leurs astuces préférées consiste à prétendre que leur code infectieux est en fait un programme d'analyse antivirus pour vous aider à vous défendre contre les menaces en ligne. Cependant, cliquer sur ce logiciel malveillant pourrait empêcher votre ordinateur d'utiliser des solutions antivirus légitimes. Assurez-vous toujours que votre logiciel antivirus est toujours à jour avec un bloqueur de fenêtres contextuelles pour empêcher les liens dangereux d'apparaître sur votre écran.

4) Laisser votre webcam ouverte aux attaques

Comme indiqué dans le Daily Mail, les piratages de webcam peuvent être une violation effrayante de votre vie privée. Un certain type de logiciel malveillant permet à un attaquant d'accéder à distance à votre ordinateur et d'activer votre webcam. La caméra de votre ordinateur n'est pas protégée de la même manière que les autres appareils compatibles réseau, alors apprenez les signes révélateurs que votre caméra est allumée (et potentiellement en train d'enregistrer) - généralement une lumière apparaîtra. Il ne suffit pas de placer un morceau de ruban adhésif sur la caméra, car il ne bloque pas le son, et assurez-vous de savoir comment le désactiver .

5) Utilisation du même mot de passe sans l'authentification à deux facteurs

Lorsque vous faites en sorte que tous vos mots de passe pour les sites Web de commerce électronique, bancaires et gouvernementaux soient identiques, vous faites vraiment la journée d'un pirate informatique. Ce soi-disant " chaînage en

guirlande " permet à tous vos comptes d'être compromis en s'introduisant dans un seul. Assurez-vous d'avoir plusieurs mots de passe pour vos différents comptes et essayez de nouvelles variantes tous les six mois environ. Bien qu'il puisse être difficile de se souvenir d'autant de mots de passe, cela vaut la peine d'éviter le casse-tête géant et la piste du vol d'identité qui peuvent suivre si un attaquant accède à tous vos comptes.

6) Utiliser des mots de passe faibles

Lorsque vous utilisez plusieurs mots de passe qui ne sont pas assez complexes, vous vous exposez au risque d'attaques par force brute. C'est une sorte d'attaque lorsqu'un attaquant utilise un logiciel spécial pour deviner le mot de passe de votre compte. Plus le mot de passe que vous utilisez est court et simple, plus tôt un pirate le devinera.

7) Procrastiner sur les mises à jour logicielles

Traîner des pieds pour installer les mises à jour nécessaires (pour des programmes comme Windows, Java, Flash et Office) est un faux pas qui peut aider les cybercriminels à y accéder. Même avec de solides programmes antivirus en place, de grandes failles de sécurité dans les programmes populaires peuvent vous rendre vulnérable aux attaques. Comme indiqué par V3, par exemple, Microsoft a récemment déployé le correctif MS15-081, qui corrige plusieurs vulnérabilités dans Office. En ne téléchargeant pas la mise à jour, vous manquez le correctif et laissez votre système ouvert à une attaque et à une éventuelle violation de données.

8) Répondre aux e-mails de phishing

Comme le rapporte le site CyberSafe du gouvernement canadien, 80 000 utilisateurs tombent chaque jour dans le piège des escroqueries par hameçonnage. La prochaine fois que vous recevez un e-mail d'hameçonnage, qui indique que vous avez gagné à la loterie, que vous devez « cliquer ici » pour éviter les amendes de l'IRS ou pour voir une « vidéo choquante », supprimez-le immédiatement. La plupart des systèmes de messagerie ont des filtres anti-spam pour intercepter ces messages, mais vérifiez toujours l'expéditeur (pas seulement le nom, mais aussi l'adresse e-mail) et assurez-vous qu'il s'agit d'un contact de confiance avant de cliquer sur un lien que vous recevez par e-mail.

9) Désactivation des fonctionnalités de contrôle de compte d'utilisateur

Les fonctionnalités de contrôle de compte d'utilisateur (UAC) de Windows peuvent être ennuyeuses, et il peut sembler que la simple désactivation des notifications est un moyen facile de les faire disparaître. Cependant, ceux-ci

sont importants, car ils vous permettent de savoir quand des changements se produisent sur votre ordinateur et vous permettent de contrôler les mises à jour. Si vous désactivez les notifications, vous donnez essentiellement un chèque en blanc aux pirates, car ils pourront apporter des modifications à votre ordinateur sans votre permission, et ainsi accéder à vos fichiers

10) Utiliser le Wi-Fi public

N'utilisez jamais un réseau Wi-Fi public pour accéder à vos informations personnelles. Ces réseaux ne sont souvent pas sécurisés, et pire encore, ils pourraient être un piège. Les malfaiteurs savent que les utilisateurs s'attendent à voir un réseau appelé "Coffeshop WiFi" lorsqu'ils s'arrêtent au café local pour une boisson chaude, et créent un point d'accès tentant et chargé de logiciels malveillants pour quiconque souhaite le rejoindre. Dès que vous rejoignez le réseau, vous pourriez donner à un pirate l'accès aux mots de passe et autres données personnelles. Vous souhaitez payer des factures ou consulter votre déclaration de revenus ? Faites-le depuis chez vous, là où vous savez que votre réseau est en sécurité.

Prime! Cliquer sur les liens courts

Les liens longs qui ne s'intègrent pas bien dans les mises à jour ou les tweets de Facebook sont souvent raccourcis à quelques caractères, ce qui rend l'URL du site Web invisible. Cliquer sur un lien abrégé signifie que vous ne savez pas où vous allez et que vous cliquez peut-être sur un logiciel malveillant. Pour éviter ce piège, utilisez un navigateur avec des aperçus de liens, qui affichent le titre et la description de la page Web, ainsi qu'une image miniature, afin que vous sachiez ce qui s'en vient avant de cliquer. Si cela ne semble pas légitime, ne cliquez pas dessus.

Les utilisateurs font tout le temps des erreurs de sécurité informatique et les pirates sont plus qu'heureux d'en profiter ! Mais la connaissance, c'est le pouvoir - connaissez leurs favoris et ne leur donnez pas la satisfaction ou l'accès à vos informations personnelles, fichiers ou données

---

B – SMARTPHONE

Comment protéger votre téléphone contre le piratage

Le piratage de téléphone peut compromettre **votre identité** et votre **vie privée** sans même que vous vous en rendiez compte. Les escrocs évoluent et améliorent constamment leurs techniques de piratage, ce qui complique leur démasquage. Cela signifie que l'utilisateur lambda pourrait ne pas être conscient des nombreuses cyberattaques. Heureusement, vous pouvez vous protéger en vous tenant au courant des derniers piratages.

Les smartphones ont regroupé tous nos comptes privés et nos données en un seul endroit pratique, ce qui en fait la cible idéale pour un pirate informatique. Tout est associé à votre téléphone, que ce soient les services bancaires, la messagerie électronique ou les réseaux sociaux. Cela signifie qu'une fois qu'un criminel a accès à votre téléphone, toutes vos applications sont des portes ouvertes au cybervol.

Qu'est-ce que le piratage de téléphone ?

Le piratage de téléphone implique toute technique par laquelle une personne force l'accès à votre téléphone ou aux communications de celui-ci. Cela peut inclure aussi bien des failles de sécurité avancées qu'une simple mise sur écoute des connexions Internet non sécurisées. Il peut également s'agir d'un vol physique de votre téléphone et de son piratage par des techniques, comme la force brute. Le piratage de téléphone peut se produire sur toutes sortes de téléphones, y compris sur les appareils Android et sur les iPhones. Comme tout le monde peut être vulnérable au piratage de téléphone, nous recommandons à tous les utilisateurs d'apprendre à reconnaître un appareil compromis.

Comment reconnaître si quelqu'un est en train de pirater votre téléphone ?

Quelqu'un a peut-être accédé à votre téléphone si au moins un de ces vertissements est présent

1. **Votre téléphone se décharge rapidement.** Les logiciels malveillants et les applications frauduleuses utilisent parfois des codes malveillants qui ont tendance à consommer beaucoup d'énergie.
2. **Votre téléphone fonctionne de manière anormalement lente.** Il se peut qu'un téléphone piraté accorde toute sa puissance de traitement aux applications douteuses du pirate informatique. Cela peut ralentir votre téléphone. Des blocages inattendus, des plantages et des redémarrages inopinés peuvent parfois en être des symptômes.
3. **Vous remarquez une activité étrange sur vos autres comptes en ligne.** Lorsqu'un pirate informatique s'introduit dans votre téléphone, il tente d'accéder à vos comptes importants. Consultez vos réseaux sociaux et votre messagerie électronique à la recherche d'invites de réinitialisation de mot de passe, de lieux d'identification inhabituels ou de vérifications d'inscription à un nouveau compte.
4. **Vous remarquez des appels ou des messages inhabituels dans vos journaux.** Il se peut que des pirates informatiques mettent votre téléphone sur écoute à l'aide d'un cheval de Troie par SMS. Ils peuvent aussi se faire passer pour vous afin de voler des informations personnelles à vos proches. Ayez l'œil ouvert, car les deux méthodes laissent des traces, par exemple, des messages sortants.

Que faire si votre smartphone a été piraté

Vous avez appris à reconnaître si quelqu'un est en train de pirater votre téléphone. À présent, vous êtes prêt à vous défendre. Voici comment vous pouvez écarter ces cybercriminels de votre appareil.

D'abord, vous devez éliminer tout logiciel malveillant qui s'est infiltré dans votre appareil. Une fois que vous avez éliminé l'atteinte à la protection des données, vous pouvez commencer à protéger vos comptes et à empêcher les pirates informatiques d'accéder à votre téléphone.

Comment se débarrasser du pirate informatique de votre téléphone

Installez un antivirus mobile pour rechercher et supprimer tout logiciel malveillant. Les produits Android, comme Kaspersky Android Security, peuvent également vous protéger des regards indiscrets grâce à la création de mots de passe particuliers pour chaque application.

Une fois que vous avez neutralisé les piratages de votre téléphone, modifiez les mots de passe de tous vos comptes principaux.

Il peut s'agir de ce qui suit :

- Banque en ligne
- Email (professionnel et personnel)
- Compte Apple ID ou Google
- Code d'accès au téléphone
- Tous les réseaux sociaux

Contrôlez également tous les services financiers ou d'achat en ligne qui ont enregistré vos cartes de crédit ou vos données bancaires (comme Amazon, eBay, etc.). Cela vous permettra de repérer toute transaction frauduleuse et de veiller à signaler et à contester ces frais auprès de votre banque.

Comment empêcher quelqu'un de pirater à nouveau votre téléphone

La sécurité en matière de piratage de téléphone est de plus en plus importante à mesure que la quantité d'informations personnelles numérisées et connectées à un téléphone portable ne cesse de croître. Comme les techniques utilisées sont en constante évolution, vous devrez être toujours vigilant sur le plan de la sécurité.

La meilleure façon de se protéger est de faire attention à son comportement numérique et, heureusement, il existe de nombreuses pratiques connues qui ont fait leurs preuves et qui réduisent les risques de piratage.

Comment protéger votre téléphone contre le piratage

- **Ne téléchargez aucune application douteuse ou peu fiable**. Si vous n'êtes pas certain, consultez les avis et effectuez vos recherches avant l'installation. Si vous doutez de la sécurité de l'application, ne l'installez pas.

- **Ne débridez pas votre téléphone.** Bien que cette opération vous permette de télécharger des applications à partir de boutiques non officielles, le fait de débrider votre appareil augmente le risque de piratage sans que vous vous en rendiez compte. Outre les logiciels malveillants ou les logiciels espions, cela signifie que vous ne disposerez pas des correctifs de sécurité intégrés aux dernières mises à jour du système d'exploitation. Pour que l'appareil reste débridé, l'utilisateur est contraint de ne pas effectuer de mises à jour. Le risque de piratage est donc encore plus élevé qu'en temps normal

.

- **Gardez votre téléphone sur vous en permanence.** L'accès physique est le moyen le plus simple pour un pirate informatique de compromettre votre téléphone. Il suffit d'un vol et d'une seule journée d'efforts pour que votre téléphone soit piraté. Si vous pouvez garder votre téléphone sur vous, un pirate informatique devra se donner beaucoup plus de mal pour y accéder.

- **Utilisez toujours un verrouillage par code d'accès et utilisez des mots de passe complexes.** N'utilisez pas de codes PIN faciles à deviner, comme des dates d'anniversaire, des dates de remise de diplômes ou des valeurs par défaut élémentaires comme « 0000 » ou « 1234 ». Si possible, utilisez un code d'accès long, comme ceux à six caractères. *Ne réutilisez jamais un mot de passe dans plusieurs endroits.*

- **Ne stockez aucun mot de passe sur votre appareil.** Il peut être difficile de se souvenir de mots de passe uniques pour chaque compte. Utilisez donc plutôt un gestionnaire de mots de passe sécurisé, comme Kaspersky Password Manager. Ces services vous permettent de stocker tous vos identifiants sécurisés dans un coffre-fort numérique, ce qui vous permet d'y accéder facilement *et* de bénéficier de la sécurité dont vous avez besoin.
- **Effacez fréquemment votre historique de navigation.** Il peut être simple de dresser un profil des tendances de votre vie à partir de toutes les informations contenues dans l'historique de votre navigateur. Donc, effacez tout, y compris les cookies et le cache.

- **Activez un service de suivi des appareils perdus.** Si vous ne retrouvez plus votre appareil dans un lieu public, vous pouvez utiliser un système de recherche d'appareils perdus pour retrouver sa position à ce moment-là. Certains téléphones possèdent une application native pour cela, tandis que d'autres peuvent avoir besoin d'une application tierce pour ajouter cette fonctionnalité.

- **Maintenez toutes les applications à jour.** Même les applications fiables peuvent comporter des bogues de programmation que les pirates informatiques exploitent. Les mises à jour des applications sont accompagnées de corrections de bogues visant à vous protéger contre les risques connus. Il en va de même pour votre système d'exploitation, alors mettez votre téléphone à jour dès que vous le pouvez.

- **Activez toujours l'authentification à deux facteurs (2FA).** Il s'agit d'une deuxième méthode de vérification qui suit une tentative d'utilisation de votre mot de passe. L'authentification 2FA fait appel à un autre compte privé ou à un objet que vous possédez physiquement. Les comptes Apple ID et Google proposent d'utiliser l'authentification 2FA pour vous protéger des cas où votre appareil serait utilisé par des individus peu recommandables. Activez donc toujours cette fonctionnalité pour renforcer la sécurité. Les données biométriques, comme les empreintes digitales et l'identification du visage, deviennent des solutions populaires. Les clés USB physiques sont également un excellent choix lorsque ce mode de protection est proposé.

- **Faites attention à ne pas utiliser de messages texte ni d'emails pour votre authentification 2FA.** Les messages texte et les emails d'authentification 2FA sont plus efficaces que l'absence de protection, mais ils peuvent être interceptés par des pirates informatiques, par exemple en procédant à un échange de la carte SIM.

- **N'utilisez pas de réseau Wi-Fi public sans un réseau privé virtuel (VPN).** Des produits, comme Kaspersky VPN Secure Connection, chiffrent vos données et les rendent anonymes afin que les personnes indésirables ne puissent pas les voir.