Conseils sur la sécurité informatique de base

Détectez les logiciels malveillants, utilisez des mots de passe forts et d'autres moyens de protéger vos données

Mary Landesman ⁝

Votre ordinateur contient une multitude de données personnelles et professionnelles.
Si ces renseignements tombent entre de mauvaises mains, vous pourriez vous exposer au vol d'identité, à la fraude et à d'autres cyberméfaits.
Il est important de rester vigilant face aux virus, aux logiciels malveillants, aux attaques d'hameçonnage, aux chevaux de Troie et aux autres escroqueries en ligne.
Voici un aperçu de neuf conseils de base en matière de sécurité informatique pour protéger votre argent, votre identité et vos informations personnelles.

Si vous avez été victime d'une escroquerie en ligne, il n'est pas trop tard pour renforcer votre système afin de vous protéger contre une autre attaque et de tirer des leçons de cette expérience.

Utilisez un logiciel antivirus et maintenez-le à jour

Les logiciels antivirus sont aujourd'hui une nécessité informatique fondamentale et sont essentiels à un système sécurisé.
En plus des applications payantes, une multitude de produits antivirus gratuits fonctionnent bien et protègent vos données vitales, il y a donc peu d'excuses pour ne pas en avoir un sur votre ordinateur.

Les logiciels antivirus et les scanners de logiciels espions recherchent les virus, les logiciels malveillants et autres contenus malveillants, en analysant votre ordinateur, vos courriels et les fichiers téléchargés.
La plupart des logiciels antivirus peuvent être configurés pour analyser automatiquement les fichiers et vérifier quotidiennement les nouvelles mises à jour des définitions, ce qui élimine les incertitudes liées à la protection de votre système.

Les programmes antivirus sont disponibles pour tous les systèmes d'exploitation, y compris Windows, macOS, Android, iOS et Linux.

Installer des correctifs de sécurité

De nouvelles vulnérabilités sont constamment découvertes dans les applications logicielles et les périphériques matériels.
Les pirates profitent de ces vulnérabilités pour accéder à votre ordinateur et à vos données.

Pour garder une longueur d'avance sur les méchants, maintenez votre système informatique à jour en installant tous les correctifs de sécurité disponibles et en gardant les navigateurs à jour.
Si vous disposez d'un système Windows, Windows Update recherche et applique toutes les mises à jour

disponibles au système d'exploitation et aux fichiers associés.
D'autres systèmes d'exploitation ont des utilitaires de mise à jour similaires.

Utiliser un pare-feu

Un pare-feu est une couche de protection entre votre ordinateur et Internet.
Il agit comme une barrière qui surveille les données entrantes et utilise des règles de sécurité pour déterminer si ces données sont reçues par votre ordinateur.

Windows dispose d'un pare-feu intégré qui est activé par défaut.
Il existe également des programmes de pare-feu gratuits qui peuvent répondre à vos besoins.

Ne fournissez jamais d'informations personnelles sensibles

Il est sage de se méfier de la divulgation de vos informations personnelles.
Ne révélez pas le nom de jeune fille de votre mère, votre numéro de sécurité sociale ou votre adresse.
Évitez également de mentionner ce genre de choses sur les médias sociaux.
Les voleurs d'identité et autres criminels parcourent les médias sociaux pour recueillir des informations.

Au lieu de fournir vos informations de carte de crédit lorsque vous magasinez en ligne, utilisez un service tel que PayPal ou Privacy.
Votre carte de crédit et vos informations financières sont conservées sur un seul site Web, plutôt que sur plusieurs sites.

Ne fournissez que des numéros de sécurité sociale ou de carte de crédit sur des sites Web sécurisés.
L'URL d'un site sécurisé est précédée de **https://** (Hypertext Transfer Protocol Secure).

Prenez le contrôle de vos courriels

N'ouvrez jamais une pièce jointe inattendue, quelle que soit la personne qui semble l'avoir envoyée.
Les attaquants usurpent le nom d'un expéditeur pour inciter les gens à ouvrir des pièces jointes qui collectent des informations personnelles et à les transmettre à l'attaquant.
Le contenu malveillant se cache également dans les courriels qui utilisent du HTML ou du texte enrichi ; Lisez les e-mails en texte brut pour plus de sécurité.

Traiter les messages instantanés avec méfiance

La messagerie instantanée est une cible fréquente des vers et des chevaux de Troie.
Les escrocs travaillent continuellement sur de nouvelles façons d'obtenir des informations personnelles et d'accéder à des comptes personnels.
Traitez les messages instantanés avec autant de soin que vous le feriez pour les courriels.

Utilisez des mots de passe forts ou des phrases passe

Utilisez une variété de lettres, de chiffres et de caractères spéciaux dans vos mots de passe, et plus ils sont longs et compliqués, mieux c'est.
Utilisez des mots de passe différents pour chaque compte.
Si un compte le prend en charge, utilisez l'authentification à deux facteurs.

Pour maîtriser vos mots de passe, envisagez d'utiliser un gestionnaire de mots de passe. De nombreux navigateurs Web, tels que Chrome et Opera, enregistrent les mots de passe si cette fonctionnalité est activée.
Les apps tierces comme Dashlane, 1Password et LastPass sont également utiles.
Ceux-ci agissent comme des plug-ins de navigateur qui surveillent les entrées de mot de passe et enregistrent les informations d'identification pour chaque compte.
Tout ce dont vous avez besoin de vous souvenir est le mot de passe unique que vous avez créé pour le programme de gestion.

La meilleure façon de créer un mot de passe sécurisé est de commencer par un mot de passe simple et de le transformer en un mot de passe plus complexe.
Par exemple, ajoutez des chiffres, des caractères spéciaux et des lettres majuscules.

Tenez-vous au courant des escroqueries sur Internet

N'ouvrez pas ou ne cliquez pas sur des liens dans les courriels qui racontent des histoires tristes, ne faites pas d'offres d'emploi non sollicitées ou ne promettez pas de gains à la loterie.
Méfiez-vous également des courriels qui se font passer pour des problèmes de sécurité de la part de votre banque ou d'un autre site de commerce électronique.
Ces courriels peuvent contenir des liens vers du contenu malveillant même s'ils semblent légitimes (il est remarquablement facile de falsifier un courriel d'une entreprise établie).

Si vous n'êtes pas sûr qu'un courriel de votre banque ou de la société émettrice de votre carte de crédit provient vraiment d'eux, contactez directement l'entreprise.

Regardez où vous téléchargez le logiciel

Il est essentiel de savoir comment télécharger et installer des logiciels en toute sécurité, car c'est souvent l'origine des problèmes informatiques de la plupart des gens et, en fin de compte, du vol de données.
Certains répertoires d'applications sont totalement sûrs et ont une longue histoire pour le prouver, et d'autres que vous devriez carrément éviter.
Surveillez les faux boutons de téléchargement sur les sites Web et les offres publicitaires intégrées dans les fichiers d'installation.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231101
"C'est ensemble qu'on avance"