LA LIBERTÉ
Depuis 1913

Clinique de Cyber-Criminologie

GÉNÉRATION CYBER-SMART

LOGICIELS DE SÉCURITÉ

****

Afin de mieux comprendre les façons par lesquelles on peut se protéger du piratage, nous considérons qu'il est nécessaire d'en savoir plus sur le fonctionnement des divers outils qui ont été conçus et développés pour détecter les cybermenaces. Dans cette section, nous présentons donc les outils et fonctions de sécurité qui existent pour vous protéger.

generationcybersmart.ca

Un projet rendu possible financièrement grâce à :

Secrétariat aux relations canadiennes Québec

Société de la francophonie manitobaine

QUELS SONT LES OUTILS DE SÉCURITÉ EXISTANTS?

Le type d'outil de sécurité le plus connu est le **logiciel antivirus**. Ce type de logiciel est conçu pour détecter, prévenir et supprimer les logiciels malveillants des systèmes, appareils et réseaux informatiques. Pour ce faire, il utilise des techniques informatiques pour analyser le code de tous les éléments de votre appareil et rechercher des thèmes ou des signatures qui ont été précédemment identifiés comme étant malveillants. Il recherche également des activités suspectes basées sur le comportement de certains programmes ou des activités anormales qui précèdent souvent la présence de logiciels malveillants, comme des programmes essayant soudainement de modifier les paramètres de votre système ou des tentatives d'accès à des informations sensibles. En fait, votre logiciel antivirus agit de la même manière que votre système immunitaire pour combattre les maladies en utilisant sa connaissance de l'apparence et du comportement des menaces potentielles.

En continuant avec cette comparaison au système immunitaire, les mises à jour du système agissent comme des vaccins : en donnant à votre système immunitaire des informations sur un agent pathogène, vos cellules peuvent apprendre à le reconnaître et à le combattre sans que vous ayez à être infecté par lui au préalable et à risquer votre santé. Les équipes de chercheurs en cybersécurité sont constamment à l'affût des nouvelles façons dont les logiciels malveillants peuvent se comporter et dont le code malveillant peut être écrit, et ils examinent également le code existant des appareils et des applications pour détecter les vulnérabilités ou les failles. Après avoir trouvé un grand nombre d'informations, les chercheurs les transmettent à votre logiciel antivirus ou à vos autres systèmes pour diffuser ces informations afin que vous soyez toujours protégé contre les nouvelles menaces.

La deuxième ligne de défense la plus commune est le **pare-feu**, qui agit comme une barrière entre votre ordinateur ou votre réseau et l'internet, contribuant à protéger votre système contre les accès non autorisés, les attaques malveillantes et le trafic réseau indésirable. Le pare-feu surveille le trafic réseau entrant et sortant, appliquant des règles de sécurité pour contrôler le flux de données et bloquer les activités potentiellement dangereuses ou suspectes.

Cet outil fonctionne comme un agent de contrôle à la frontière : il examine chaque donnée (un courriel que vous envoyez, la page Wikipédia sur les chatons que vous souhaitez consulter) qui entre ou sort de l'interface réseau de votre appareil en examinant les informations associées afin de s'assurer que chaque donnée dispose de tous leurs documents de voyage nécessaires pour entrer. Si ce n'est pas le cas, par exemple s'il provient d'une adresse IP malveillante connue, le pare-feu le bloque. Les pare-feu permettent également de contrôler le trafic dans le but de s'assurer que les passagers d'un vol ne passent pas tous en même temps au point de contrôle et ne surchargent pas les systèmes pour essayer d'entrer sans que leur passeport soit vérifié. Ils gardent aussi note des voyageurs qui sont entrés et sortis afin de garder un œil sur les comportements suspects potentiels et d'aider en cas de problèmes dans le fonctionnement du système.

Parmi les autres dispositifs de sécurité que vous avez peut-être utilisés dans votre vie quotidienne, vous trouverez aussi le **filtre anti-spam** de votre messagerie électronique, qui permet de trier les messages d'hameçonnage potentiels ; les bloqueurs de fenêtres pop-up, qui empêchent les sites web malveillants d'inonder votre écran de publicités et de notifications indésirables; les gestionnaires de mots de passe, qui permettent de sécuriser vos mots de passe uniques et complexes ; et les VPN, qui permettent de sécuriser votre connexion internet en chiffrant le trafic de données entrant et sortant de votre appareil pour vous protéger contre l'interception ou la surveillance.

Filtre anti-spam

Bloqueurs de fenêtres pop-up

COMMENT PUIS-JE M'ASSURER QUE J'UTILISE CORRECTEMENT MES OUTILS DE SÉCURITÉ?

Tant que vos outils de sécurité sont activés, que vous recevez leurs messages d'alerte, et que vous respectez leurs consignes, vous êtes sur la bonne voie. Vous devez tout de même surveiller votre antivirus et votre pare-feu de temps en temps pour vous assurer que toutes les fonctions sont activées et que les deux programmes indiquent qu'ils fonctionnent. Confirmez que la protection en temps réel est activée : il s'agit d'une fonction dont sont dotés la plupart des logiciels antivirus qui garantissent que toute l'activité de votre appareil est surveillée en permanence et que les menaces sont détectées et bloquées dès qu'elles se présentent.

Il est aussi important de vous assurer de vous familiariser avec le logiciel antivirus que vous utilisez. Certains sites malveillants essaieront de vous amener à cliquer sur un pop-up semblant provenir de votre antivirus, alors qu'il s'agit en réalité d'un faux message pouvant télécharger un maliciel ou tenter d'accéder à des informations sensibles. Par exemple, vous pourriez cliquer sur un message vous demandant de renouveler la licence de votre antivirus Norton, en oubliant que vous utilisez en fait le logiciel Kaspersky. Apprenez à reconnaître les messages que vous envoie votre antivirus afin d'éviter de vous faire piéger par de fausses alertes.

Votre ordinateur est généralement équipé d'un pare-feu intégré, qui fonctionne très bien dans le cadre d'une utilisation quotidienne. Les ordinateurs PC comprennent généralement le pare-feu Microsoft Defender, qui est activé par défaut. Microsoft propose un guide pour en vérifier l'état en fonction de la version de Windows que vous utilisez.

Pour les ordinateurs Apple, choisissez le menu Apple dans le coin supérieur gauche de votre écran, puis sélectionnez Paramètres du système, cliquez sur Réseau dans la barre latérale, puis cliquez sur Pare-feu pour trouver le bouton permettant de l'activer, ou pour vérifier qu'il a déjà été allumé.

RESSOURCES

Guide Microsoft pour activer son pare-feu :
https://support.microsoft.com/fr-fr/windows/activer-ou-d%C3%A9sactiver-le-pare-feu-de-microsoft-defender-ec0844f7-aebd-0583-67fe-601ecf5d774f

Guide Apple pour activer son pare-feu :
https://support.apple.com/fr-ca/guide/mac-help/mh11783/mac#:~:text=D%C3%A9couvrez%20comment%20bloquer%20les%20connexions,faire%20d%C3%A9filer%20vers%20le%20bas

Guide Protégez-vous pour choisir un bon logiciel antivirus :
https://www.protegez-vous.ca/technologie/securite-internet/comment-choisir-un-bon-antivirus

GLOSSAIRE

- **Logiciel de sécurité** : Les logiciels de sécurité sont des programmes ou des applications informatiques conçus pour protéger les systèmes informatiques, les réseaux et les données contre diverses cybermenaces et vulnérabilités.
- **Antivirus** : Un antivirus est un type de logiciel de sécurité conçu pour détecter, prévenir et supprimer les logiciels malveillants (maliciels) des systèmes informatiques.
- **Pare-feu** : Un pare-feu est un dispositif de sécurité réseau ou une application logicielle conçue pour surveiller, filtrer et contrôler le trafic réseau entrant et sortant sur la base de règles ou de politiques de sécurité prédéterminées.
- **Mise à jour** : Une mise à jour fait référence au processus d'application de changements, d'améliorations ou de correctifs à un système afin d'en améliorer la fonctionnalité, les performances, la sécurité ou la stabilité.
- **Pop-up** : Un pop-up est une petite fenêtre qui apparaît soudainement au-dessus de la fenêtre ou de la page web consultée par l'utilisateur et contient généralement des informations supplémentaires, des alertes, des publicités ou des éléments interactifs.
- **Message d'alerte** : Un message d'alerte est une notification ou un message généré par le logiciel pour informer l'utilisateur d'une menace potentielle pour la sécurité, d'une activité suspecte ou d'un problème système détecté sur son ordinateur ou son réseau.
- **Protection en temps réel** : La protection en temps réel fait référence à la surveillance continue et à la réponse immédiate aux menaces potentielles de sécurité en temps réel, dès qu'elles se produisent.
- **Analyse antivirus** : Une analyse antivirus est un processus d'examen des fichiers, des programmes, de la mémoire système et d'autres zones d'un système informatique pour détecter la présence de maliciels.

- **Trafic réseau** : Le trafic réseau désigne les données transmises entre les appareils d'un réseau informatique.
- **Logiciel malveillant ou maliciel** : Les maliciels, mot-valise pour logiciels malveillants, désignent tout type de logiciel spécifiquement conçu pour perturber, endommager ou obtenir un accès non autorisé à des systèmes, réseaux ou appareils informatiques, souvent à l'insu ou sans le consentement de l'utilisateur.

Balayez ce QR code à l'aide de votre caméra pour visionner nos vidéos