LA LIBERTÉ
Depuis 1913

Clinique de Cyber-Criminologie

GÉNÉRATION CYBER-SMART

PIRATAGE ****

Malgré les outils et les mesures de sécurité mises en place pour nous protéger, le piratage informatique reste une menace bien réelle lorsque l'on utilise n'importe quelle forme de technologie. Nous voulons donner aux enfants plus d'informations à ce sujet afin qu'ils sachent à quoi faire attention et comment mieux se protéger.

generationcybersmart.ca

Un projet rendu possible financièrement grâce à :

Secrétariat aux relations canadiennes Québec

Société de la francophonie manitobaine

QU'EST-CE QUE LE PIRATAGE INFORMATIQUE ET QUELS SONT LES RISQUES QUI Y SONT ASSOCIÉS?

Le piratage est l'**accès non autorisé ou la manipulation de systèmes, de réseaux ou d'appareils informatiques dans le but d'obtenir des informations, de perturber les opérations ou de causer des dommages**. Cela peut se faire de différentes manières, notamment en exploitant les vulnérabilités d'un logiciel, d'un réseau ou d'un système, en devinant des mots de passe lors d'une attaque par force brute ou même en accédant à un appareil via l'installation de logiciels malveillants.

Si le piratage informatique peut être motivé par divers facteurs, comme la curiosité, l'activisme ou le piratage éthique à des fins de tests de sécurité, il implique souvent des intentions malveillantes visant à causer des dommages, à voler des informations sensibles ou à obtenir des avantages financiers ou non autorisés. Les pirates malveillants peuvent se livrer à des activités telles que le vol de données ou d'argent, la fraude, l'espionnage ou le sabotage. Les pirates utilisent toute une série de techniques et d'outils complexes pour mener à bien leurs cyberattaques qui peuvent entraîner des pertes financières, des atteintes à la réputation, des interruptions de services, des violations de données et la compromission d'informations sensibles.

QU'EST-CE QUE LE PIRATAGE NUMÉRIQUE ET QUELS SONT LES RISQUES QUI Y SONT ASSOCIÉS?

Le piratage numérique, de son côté, désigne la **copie, la distribution ou l'utilisation illégale de contenu protégé par des droits d'auteur**, comme des logiciels, de la musique, des films, des livres ou d'autres matériels numériques, sans l'autorisation du détenteur des droits d'auteur. Par exemple, en visionnant un film en streaming sans payer ou en téléchargeant un jeu sur un site de *torrent*, vous commettez également un acte de piratage.

En plus d'accéder de manière non autorisée à des fichiers et à du matériel protégé par des droits d'auteur en ligne, le piratage peut comporter certains risques. Comme le contenu auquel on accède est obtenu illégalement, il n'y a aucun moyen de vérifier si le téléchargement est sûr, corrompu ou compromis d'une manière ou d'une autre. Un site de *torrent* peut en effet vous permettre de télécharger un film que vous cherchiez, tout en ayant secrètement téléchargé un logiciel malveillant sur votre ordinateur. Les enfants peuvent également tomber sur des contenus inappropriés de cette manière, ce qui peut les exposer par erreur à des images choquantes, par exemple.

COMMENT SE PROTÉGER DU PIRATAGE INFORMATIQUE?

Une bonne cyberhygiène est essentielle pour se protéger contre le piratage : il est important d'**utiliser un logiciel antivirus sur tous ses appareils, d'utiliser des mots de passe forts et de se méfier des liens inconnus, des réseaux et des appareils publics**.

Veillez aussi à ce que vos appareils, vos applications et vos logiciels de sécurité soient toujours à jour, afin que tous les systèmes que vous utilisez disposent toujours des informations les plus récentes sur les menaces et les vulnérabilités potentielles. La plupart du temps, vous recevrez des notifications de la part de votre appareil, vos applications et votre navigateur lorsqu'une nouvelle mise à jour sera disponible, mais vous pouvez aussi paramétrer vos systèmes pour installer ces mises à jour automatiquement.

Les ressources que nous avons créées pour les enfants comprenaient un conseil qui mérite d'être rappelé : veillez à ce que tout votre entourage et tout le monde dans votre environnement de travail prennent des mesures pour assurer sa propre sécurité. Les pirates utilisent différents moyens pour s'infiltrer dans les systèmes, mais il leur est beaucoup plus facile de prendre le contrôle d'un compte ou d'un appareil à travers un autre qui a déjà été compromis. À tout le moins, le piratage des comptes d'un proche ou d'un collègue augmente la probabilité qu'un cybercriminel possède vos informations et un moyen de vous contacter, ce qui vous met également à risque. En d'autres mots, vous avez tout à gagner à promouvoir une bonne cyberhygiène auprès de votre entourage.

COMMENT SE PROTÉGER DU PIRATAGE NUMÉRIQUE?

Lorsqu'il s'agit de vous protéger contre les risques liés au téléchargement de contenus non autorisés, notre plus forte recommandation est de ne pas le faire. Non seulement est-ce illégal et peut conduire votre fournisseur Internet à mettre fin à vos services, mais les risques de sécurité potentiels l'emportent largement sur les avantages. Il est toujours préférable et plus sûr de télécharger, de visionner ou d'acheter le contenu auprès du distributeur autorisé.

Vous pouvez aussi soutenir les parents de vos élèves en leur rappelant de s'assurer que leurs antivirus et autres logiciels de sécurité fonctionnent correctement. Enseignez à vos élèves de ne surtout pas ignorer les messages d'avertissement des outils de sécurité et de ne pas contourner un dispositif de sécurité pour accéder à un site web ou pour télécharger un fichier. Vous pouvez aussi montrer à vos élèves comment analyser des fichiers sur VirusTotal afin qu'ils soient mieux équipés s'ils téléchargent beaucoup de contenu en ligne ou s'ils aiment explorer l'internet.

COMMENT SAVOIR SI J'AI ÉTÉ PIRATÉ? QUE DOIS-JE FAIRE SI UN DE MES ÉLÈVES PENSE QU'UN APPAREIL A ÉTÉ PIRATÉ?

Si certains logiciels malveillants sont conçus pour ne pas être détectés, comme les enregistreurs de frappe et les logiciels espions, d'autres peuvent affecter le fonctionnement de certains appareils et dévoiler leur présence. Voici quelques signes indiquant qu'un appareil a peut-être été piraté :

- **Ralentissement** significatif et inexpliqué de l'appareil.
- L'appareil **plante soudainement** à plusieurs reprises.
- Le système **redémarre plus fréquemment** qu'en temps normal et sans sollicitation.
- Les programmes **s'ouvrent et se ferment seuls, ne parviennent plus à s'exécuter ou génèrent des messages d'erreurs étranges**.
- Installation de **programmes non demandés**.
- Les périphériques (souris, clavier, disque dur externe…) réagissent **anormalement** en disparaissant ou en n'étant plus accessibles, par exemple.
- Des onglets de notifications **s'ouvrent soudainement**.
- Le navigateur accède spontanément à des sites Internet qui vous sont **inconnus**.

Si un élève vous parle de quelque chose sur lequel il a cliqué ou s'il remarque que quelque chose ne va pas sur un appareil, il est important de rester calme et de ne pas le punir pour avoir fait une erreur. Il vaut mieux qu'il reconnaisse le problème et qu'il vous en parle plutôt que de le cacher et de risquer des conséquences plus graves.

RESSOURCES

Qu'est-ce que le piratage?
https://www.clinique-cybercriminologie.ca/post/piratage-maliciels

Cybermalveillance - Piratage d'un système informatique :
https://www.cybermalveillance.gouv.fr/diagnostic/73096c02-5572-42a0-b864-6371ad4c4c3d

Centre antifraude du Canada :
https://antifraudcentre-centreantifraude.ca/report-signalez-fra.htm

Centre canadien pour la cybersécurité :
https://cyber.gc.ca/fr/cyberincidents

Récupérer un compte piraté : une course contre la montre :
https://www.protegez-vous.ca/nouvelles/technologie/recuperer-un-compte-pirate-une-course-contre-la-montre

Quoi savoir avant de fréquenter les sites de torrents - Radio-Canada :
https://ici.radio-canada.ca/recit-numerique/5684/sites-torrents-telechargements-streaming

GLOSSAIRE

- **Piratage informatique** : Le piratage informatique est l'accès non autorisé ou la manipulation de systèmes, de réseaux ou d'appareils informatiques dans le but d'obtenir des informations, de perturber les opérations ou de causer des dommages.
- **Piratage numérique** : Le piratage numérique désigne la copie, la distribution ou l'utilisation non autorisée de matériel protégé par des droits d'auteur, tels que des logiciels, de la musique, des films, des livres ou d'autres contenus numériques, sans l'autorisation du détenteur des droits d'auteur.
- **Attaque par force brute** : L'attaque par force brute est un type d'attaque de piratage qui consiste à essayer systématiquement de deviner ou de craquer des mots de passe ou des clés de cryptage en essayant toutes les combinaisons possibles jusqu'à ce que la bonne soit trouvée.
- **Vulnérabilité informatique** : Une vulnérabilité informatique est une faiblesse ou une faille dans un système matériel, logiciel ou réseau qui peut être exploitée par des acteurs malveillants pour compromettre la sécurité, l'intégrité ou la disponibilité du système.
- **Distributeur autorisé** : Un distributeur autorisé est une entité ou une organisation légalement reconnue qui a obtenu les droits ou autorisations nécessaires du détenteur des droits d'auteur pour distribuer, vendre ou concéder des œuvres protégées par des droits d'auteur à des utilisateurs finaux ou à des consommateurs.
- **Site de streaming** : Un site de streaming (diffusion en continu) est une plateforme en ligne qui permet aux utilisateurs d'accéder et de regarder des contenus médiatiques numériques, tels que des films, des émissions de télévision ou de la musique, sur l'internet en temps réel, sans qu'il soit nécessaire de télécharger les fichiers sur leur appareil.

- ***Torrenting*** : Le *torrenting* est une méthode de téléchargement et de partage de fichiers sur l'internet qui permet de distribuer des fichiers volumineux entre plusieurs utilisateurs en les divisant en petits morceaux.
- **Mise à jour** : Une mise à jour logicielle fait référence à la publication d'un code logiciel nouveau ou révisé, de corrections ou d'améliorations fournis par le vendeur ou le développeur du logiciel pour remédier aux failles de sécurité, améliorer les performances, corriger les bogues, ajouter de nouvelles fonctionnalités ou améliorer la compatibilité avec d'autres logiciels ou appareils.
- **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.
- **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.
- **Enregistreur de frappe** : Un enregistreur de frappe est un type de logiciel ou de matériel de surveillance qui enregistre chaque touche tapée sur un clavier et les mouvements de souris, souvent de manière secrète et à l'insu de l'utilisateur.
- **Logiciel espion** : Un logiciel espion est un type de logiciel malveillant conçu pour surveiller secrètement et recueillir des informations sur les activités informatiques d'un utilisateur à son insu ou sans son consentement.
- **Rançongiciel** : Un rançongiciel est un type de logiciel malveillant conçu pour crypter des fichiers ou verrouiller l'accès au système informatique ou aux données d'une victime, la tenant ainsi en otage jusqu'au paiement d'une rançon.

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