LA LIBERTÉ
Depuis 1913

Clinique de Cyber-Criminologie

GÉNÉRATION CYBER-SMART

MOTS DE PASSE ****

Les mots de passe constituent non seulement la première ligne de défense de chaque internaute contre les pirates informatiques et les fraudeurs, mais aussi la base d'une bonne cyberhygiène. En prenant l'habitude de créer des mots de passe forts, les enfants apprennent à penser à leur sécurité chaque fois qu'ils se connectent au réseau Wi-Fi de leur domicile, à leur appareil ou à leurs comptes.

generationcybersmart.ca

Un projet rendu possible financièrement grâce à :

Secrétariat aux relations canadiennes Québec

Société de la francophonie manitobaine

QU'EST-CE QU'UN MOT DE PASSE ET COMMENT FONCTIONNE-T-IL?

Un mot de passe est **un code secret qui utilise un système complexe de cryptage afin de protéger des systèmes, des comptes ou des appareils**.

COMMENT ÇA MARCHE?

En fait, le système dans lequel vous saisissez la combinaison spécifique de lettres, de chiffres et de symboles qui constituent votre mot de passe convertit ce dernier en quelque chose de totalement illisible, souvent une équation mathématique incroyablement complexe qui prendrait des millions d'années à résoudre : c'est ce qu'on appelle le **cryptage ou le chiffrement**.

Étant donné la durée extrêmement longue qu'il faudrait aux pirates pour deviner les mots de passe, ceux-ci mettent davantage l'accent sur les codes qui ont une plus grande probabilité statistique d'être utilisés - les combinaisons **courantes ou faciles** comme «password123», «abcdefg», etc. sont utilisées par un si grand nombre de personnes qu'en essayant ces mots de passe en premier, les pirates ont plus de chances d'accéder aux comptes d'utilisateurs et d'en prendre le contrôle.

De plus, les pirates connaissent les mauvaises habitudes des utilisateurs lorsqu'il s'agit de créer des mots de passe (utilisation d'informations personnelles, mots de passe plus courts plus faciles à retenir, même s'ils sont choisis au hasard, et le remplacement de certaines lettres d'un mot courant par un symbole similaire, comme la transformation de «password» en «p@ssword», par exemple), ils sont susceptibles d'exploiter aussi ces faiblesses lorsqu'ils essaient de deviner les mots de passe, et ils y parviennent généralement très bien.

Dans cette même logique, les pirates informatiques peuvent également utiliser des listes des mots de passe et de comptes ou de courriels qui ont déjà été **divulgués lors de fuites de données**. Sachant que les gens réutilisent leurs mots de passe dans leurs différents comptes et appareils, et qu'ils changent rarement leurs mots de passe, les pirates essaieront ces combinaisons trouvées dans les fuites de données sur d'autres sites et ils obtiendront **un meilleur taux de réussite** qu'en essayant aveuglément et au hasard toutes les combinaisons possibles qui existent. C'est pourquoi il est important de créer des mots de passe uniques pour chaque compte, afin d'éviter qu'un mot de passe compromis ou deviné ne permette de compromettre un autre compte.

Et finalement, plus un mot de passe est long, plus il faudra de temps à un ordinateur pour essayer de le deviner s'il essaie toutes les combinaisons possibles. Les caractères spéciaux complexifient la tâche aux ordinateurs qui tentent de deviner les mots de passe, renforçant donc leur sécurité. Par exemple, un mot de passe de 6 caractères, même s'il possède un ou des symboles, sera découvert en quelques secondes alors qu'une combinaison de 25 caractères ou plus, accompagné de caractères spéciaux, prendra énormément plus de temps. C'est pour ces raisons qu'il est conseillé d'utiliser des **mots de passe longs, uniques, aléatoires et complexes**.

Selon les meilleures pratiques actuelles pour créer un mot de passe fort, on recommande l'utilisation d'une combinaison de plus de huit caractères, sans utiliser de mots trouvés dans le dictionnaire, et en incluant de préférence des symboles. On avise également de l'importance de ne pas réutiliser deux fois le même mot de passe et de ne pas réutiliser des mots de passe qui sont apparus dans des fuites de données antérieures. Malgré tout, un mot de passe de huit caractères demeure un mot de passe assez faible.

Les pirates et les outils d'intelligence artificielle sont maintenant capables de deviner un mot de passe de huit caractères presque **instantanément**. Nous avons tout de même gardé ce conseil dans les ressources pour les enfants, principalement parce que le souci de mémorabilité est le principal obstacle à l'usage unique d'un mot de passe et nous craignons qu'en leur demandant un minimum de caractère plus élevé pourrait les décourager. Alors qu'ils commencent à penser à la force de leurs mots de passe, le minimum de huit caractères est un bon point de départ ; cependant, si vous pensez que l'enfant est capable de se rappeler (et de bien orthographier!) un mot de passe plus long, ou si vous lui recommandez d'utiliser un gestionnaire de mot de passe, ce sont des habitudes beaucoup plus sécuritaires à adopter.

POURQUOI CRÉER DES MOTS DE PASSE FORTS EN PREMIER LIEU?

Comme nous l'avons déjà mentionné, le mot de passe est la forme de protection de base lorsque vous naviguez sur le web. Compte tenu des nombreux outils de protection existants, il est beaucoup plus simple et accessible pour un cybercriminel de tenter de deviner votre mot de passe que d'infecter et pirater votre appareil. En d'autres termes, les pirates peuvent avoir beaucoup à gagner en essayant de déchiffrer vos mots de passe, qui pourraient potentiellement leur donner accès à votre adresse courriel, à vos comptes bancaires, à votre ordinateur et à bien d'autres choses encore, vous exposant ainsi à des pertes financières. Ces informations peuvent même être vendues, de sorte que plusieurs pirates peuvent avoir accès à vos informations et peuvent les utiliser à des fins malveillantes allant de l'usurpation d'identité à des taches sur votre cote de crédit.

Comme le démontre ce sondage, les parents ne considèrent pas toujours la force d'un mot de passe comme étant l'enjeu de sécurité affectant leurs enfants le plus - après tout, ils n'ont peut-être pas encore leurs propres appareils ou même accès à une carte de crédit.

Cependant, **il est nécessaire de leur enseigner ces concepts très tôt** afin qu'ils grandissent en sachant que l'utilisation de l'internet comporte des **risques**, mais qu'ils peuvent s'en protéger. Il est également très probable qu'ils aient accès à un réseau Wi-Fi à la maison, qu'ils utilisent un compte sur l'ordinateur familial ou qu'ils doivent se connecter à l'adresse électronique qui leur a été attribuée par l'école, ce qui les oblige à créer et utiliser des mots de passe. Ce sont là d'excellents points d'approche pour leur apprendre à utiliser des mots de passe complexes et uniques, afin que cela devienne une seconde nature pour eux une fois qu'ils seront totalement autonomes en ligne.

Vous pouvez utiliser un **testeur de mot de passe comme celui créé par le gouvernement français** (economie.gouv) pour vérifier si vos mots de passe sont suffisamment forts et s'ils ont déjà fuité. Vous pouvez même en faire une activité amusante avec vos élèves et jouer avec l'outil pour essayer d'obtenir le mot de passe le plus complexe possible.

QUE PUIS-JE FAIRE POUR PROTÉGER MES ÉLÈVES?

Outre le fait de les aider à modifier leurs mots de passe pour qu'ils soient uniques, longs et complexes, il existe **d'autres moyens pour encourager une plus grande protection** en ce qui concerne la protection par mot de passe.

La première consiste à leur présenter les **gestionnaires de mots de passe** et de recommander leur usage aux parents. Il s'agit d'un outil qui aide à stocker les mots de passe en toute sécurité dans un coffre-fort chiffré qui peut être ouvert à l'aide d'un mot de passe maître ou d'une autre méthode d'authentification sécurisée comme la reconnaissance faciale.

Cela permet de créer des mots de passe longs, aléatoires, complexes et uniques pour chaque compte sans avoir à se souvenir de chacun d'entre eux ou, pire encore, à les écrire sur papier ou dans un document texte au hasard, qui peuvent tous deux être facilement volés ou piratés.

Les gestionnaires de mots de passe utilisent, pour la plupart, un algorithme de chiffrement égalant ceux utilisés par l'armée américaine, garantissant la sécurité de tous les mots de passe, et ils sont souvent dotés de certaines fonctions qui en facilitent l'utilisation, comme une fonction qui génère aléatoirement des mots de passe forts lors de la création d'un nouveau compte pour épargner l'effort d'en créer un à chaque fois. Ils ont aussi une option de création de différents dossiers sécurisés pour que l'enfant puisse lui aussi sauvegarder des notes ou d'importantes informations sensibles en toute sécurité. Il existe de nombreux gestionnaires de mots de passe gratuits, fréquemment accompagnés de courts tutoriels pour faciliter leur utilisation et leur adoption.

En plus de l'utilisation d'un gestionnaire de mots de passe, vous pouvez recommander aux parents l'**activation de l'authentification multifactorielle**, surtout sur le gestionnaire de mot de passe lui-même. Il s'agit d'un processus qui utilise plus d'un "facteur" d'identification pour vous permettre d'accéder à votre compte.

Ces facteurs additionnels ajoutent une couche de sécurité et impliquent souvent l'accès à un appareil que le parent possède ou une demande d'information biométrique, comme des empreintes digitales.

Par exemple, en plus de vous demander votre mot de passe, votre banque peut être amenée à vous envoyer par texto un code d'authentification unique en utilisant le numéro de téléphone associé à votre compte pour confirmer que vous êtes bien la personne qui tente de se connecter. Cette fonction empêche les pirates d'accéder aux comptes même s'ils parviennent à déchiffrer un mot de passe, puisqu'ils n'ont pas accès à ce deuxième facteur. Ce conseil est particulièrement utile pour les enseignants dont les élèves possèdent déjà leur propre appareil.

RESSOURCES

Pour en savoir plus, vous pouvez également consulter notre ressource au sujet des mots de passe.

Testeur de mot de passe : https://ssi.economie.gouv.fr/motdepasse

GLOSSAIRE

- **Mot de passe** : Un mot de passe est une combinaison secrète de caractères, généralement composée de lettres, de chiffres et/ou de symboles, utilisée pour authentifier l'identité d'un utilisateur et lui permettre d'accéder à un système, un compte ou une ressource sécurisée.
- **Chiffrement ou cryptage** : Le chiffrement est un processus de conversion d'informations, de données ou de communications dans un format codé ou illisible, souvent par l'utilisation d'algorithmes ou de transformations mathématiques. Le but du chiffrement est de sécuriser le contenu et d'empêcher l'accès non autorisé par des personnes ou des entités qui ne possèdent pas la clé de déchiffrement correspondante.
- **Authentification multifactorielle** : L'authentification multifactorielle est un mécanisme de sécurité qui exige des utilisateurs qu'ils fournissent plusieurs formes d'identification avant d'accorder l'accès à un système, un compte ou une application. L'objectif de l'authentification multifactorielle est de renforcer la sécurité du processus d'authentification en ajoutant une couche supplémentaire de vérification au-delà du nom d'utilisateur et du mot de passe.
- **Gestionnaire de mot de passe** : Un gestionnaire de mots de passe est une application logicielle ou un service conçu pour aider les utilisateurs à stocker, organiser et gérer leurs mots de passe en toute sécurité. L'objectif principal d'un gestionnaire de mots de passe est d'atténuer les enjeux liés à la création, à la mémorisation et à la conservation de mots de passe forts et uniques pour plusieurs comptes en ligne. Par exemple, le site internet 1password.com propose de gérer des mots de passe.
- **Piratage** : Au sens général, le piratage informatique désigne l'obtention d'un accès non autorisé à des systèmes ou réseaux informatiques, impliquant souvent la manipulation, l'exploration ou l'exploitation de la technologie pour atteindre cet objectif.

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