LA LIBERTÉ
Depuis 1913

Clinique de
Cyber-Criminologie

GÉNÉRATION CYBER-SMART

HAMEÇONNAGE ****

L'hameçonnage est l'une des formes de cyberattaques les plus communes de nos jours, et tant que les enfants disposent d'un moyen de communication direct comme une adresse courriel, ils n'en sont malheureusement pas à l'abri. Dans cette section, nous expliquons ce qu'est l'hameçonnage en plus de détails et donnons des conseils pour accompagner un enfant à travers ce type de cybermenace.

generationcybersmart.ca

Un projet rendu possible financièrement grâce à :

Secrétariat aux relations canadiennes Québec

Société de la francophonie manitobaine

QU'EST-CE QUE L'HAMEÇONNAGE?

L'hameçonnage, ou *phishing*, est un type de **cyberattaque** dans lequel les auteurs se font passer pour des entités légitimes, comme des entreprises, des organisations ou des personnes, afin de tromper les utilisateurs et de les amener à **divulguer des informations sensibles**. Par exemple, vous pourriez recevoir un texto vous informant que vous avez manqué la livraison d'un colis et vous invitant à cliquer sur un lien pour organiser une nouvelle livraison ; un courriel de Facebook vous demandant de vous connecter à votre compte, sans quoi celui-ci sera fermé ; ou quelqu'un peut vous envoyer un lien sur Discord vous expliquant comment réclamer une carte-cadeau gratuite pour un nouveau jeu pour ensuite vous mener à un formulaire vous demandant toutes sortes d'informations. Dans tous les cas, si vous cliquez et répondez, l'hameçonneur aura alors accès à des détails personnels, à des identifiants de connexion, voire à des données financières, qu'il pourra ensuite utiliser pour commettre des fraudes, essayer de voler votre identité ou bien les revendre sur le dark web pour que d'autres cybercriminels puissent les utiliser.

Mais pour pouvoir vous envoyer ces messages, les hameçonneurs ont besoin d'un moyen de communiquer avec vous. Cela peut se faire d'une multitude de façons : en les obtenant directement à partir de comptes de réseaux sociaux, en créant de faux formulaires dans lesquels vous avez volontairement donné vos informations personnelles, par le biais de fuites de données qui ont révélé vos coordonnées, en parcourant les contacts enregistrés d'un compte ou d'un appareil compromis, ou même en essayant massivement différentes combinaisons de numéros de téléphones, pour ne citer que quelques exemples.

Bref, les moyens par lesquels un hameçonneur peut essayer de communiquer avec vous ne manquent pas. Une fois qu'ils y parviennent, ils travaillent en nombre, jetant un énorme filet dans l'espoir d'attraper au moins quelques personnes avec leurs messages frauduleux. Ils s'efforcent constamment d'améliorer leurs tactiques - en modifiant l'apparence de courriels frauduleux de Netflix pour qu'ils ressemblent davantage aux vrais, par exemple - et peuvent utiliser des adresses courriels ou des numéros de téléphone qui ressemblent à ceux d'entités légitimes afin d'augmenter leur crédibilité.

QUELS SONT LES RISQUES LIÉS À L'HAMEÇONNAGE ET COMMENT AFFECTENT-ILS MON ENFANT?

Les messages d'hameçonnage peuvent prendre plusieurs formes différentes, ce qui signifie que les serveurs Discord et Twitch de votre enfant peuvent également être utilisés pour envoyer des messages d'hameçonnage, tout comme leur boîte de réception Roblox ou leur chat Minecraft. Certains hameçonneurs ont également pour but de télécharger des maliciels sur un appareil, incitant l'utilisateur à cliquer sur un lien qui peut infecter son appareil avec un enregistreur de frappe ou d'autres types de logiciels malveillants.

Les messages d'hameçonnage sont aussi souvent bien conçus : le message que votre enfant reçoit lui demandant de se connecter à sa plateforme de jeu en ligne peut le rediriger vers une page qui ressemble exactement à la page de connexion habituelle, mais qui a en fait été créée pour envoyer toutes les informations d'identification à la base de données d'un cybercriminel. Une autre arnaque courante est celle qui consiste à dire aux utilisateurs des réseaux sociaux qu'ils ont été sélectionnés pour devenir ambassadeur ou influenceur pour une certaine marque, et qui promet d'envoyer à l'utilisateur des produits gratuits en échange de frais de livraison minimes, facturés sur une boutique en ligne apparemment légitime. Cette pratique peut être particulièrement dangereuse, car elle joue sur le désir des jeunes de gagner de l'argent en tant que créateurs de contenu sur les réseaux sociaux et de gagner en popularité, tout en risquant de voler leurs données financières et leurs coordonnées.

COMMENT ÉVITER QUE MON ENFANT SOIT VICTIME D'HAMEÇONNAGE ?

Il est important d'apprendre très tôt aux enfants à développer leur esprit critique face aux communications qu'ils reçoivent sur n'importe quelle plateforme et s'assurer qu'ils comprennent que cliquer sur des liens inconnus ou répondre à des messages d'hameçonnage comporte des risques. Dès leur plus jeune âge, et surtout avant qu'ils ne commencent à avoir accès aux réseaux sociaux, il faut leur apprendre à toujours vérifier avant de cliquer. Apprenez-leur à confirmer où mène un lien en passant la souris sur le lien, et à revenir en arrière s'ils pensent que la page sur laquelle ils ont atterri n'est pas sécuritaire.

À cet âge, la boîte courriel d'un enfant ne devrait pas être très active, permettant de lui apprendre à ignorer les courriels provenant d'expéditeurs inconnus et à ne pas y répondre. Il en va de même pour ses textos, s'il possède son propre appareil et son propre numéro de téléphone : rappelez-lui que s'il reçoit un lien ou un message d'un inconnu, qu'il vaut mieux le supprimer. N'hésitez pas non plus à lui présenter ceux que vous recevez. Il s'agit d'un bon prétexte pour amorcer la discussion. Si vous ou votre enfant recevez des courriels concernant la sécurité d'un compte, ne cliquez pas, et connectez-vous au compte comme vous le feriez normalement plutôt que de cliquer sur quoi que ce soit dans le courriel.

Nous recommandons également à chaque membre de la famille d'utiliser un système d'adresses courriel multiples, comme mentionné dans la fiche sur les informations personnelles. Vous devriez utiliser une adresse courriel pour les comptes importants, une autre pour les opérations secondaires, mais quotidiennes, et une troisième qui ne contiendra aucune information personnelle, mais que vous pourrez utiliser pour vos abonnements à des infolettres et à des courriels promotionnels. Ce système nécessite plus d'étapes, mais il garantira la sécurité de vos communications les plus importantes, contrairement à l'adresse que vous partagez publiquement, qui sera susceptible de faire l'objet de fuites et où vous saurez donc que vous êtes le plus susceptible de recevoir des messages d'hameçonnage - en d'autres mots, vous serez davantage assuré que les communications suspicieuses envoyée à cette adresse ne sont pas légitimes.

RESSOURCES

Article de la Clinique de cybercriminologie sur l'hameçonnage : https://www.clinique-cybercriminologie.ca/post/hameconnage#:~:text=Les%20fraudeurs%20envoient%20un%20faux,de%20cr%C3%A9dit%2C%20NAS%2C%20etc

Pour en savoir plus sur le hameçonnage, consultez le magazine de ***La Liberté***, ***Cybercriminalité, pour e-voir plus clair*** : https://www.lalibertemagazine.ca

GLOSSAIRE

- **Hameçonnage (phishing)** : L'hameçonnage est un type de cyberattaque où les auteurs tentent de tromper les individus en leur faisant divulguer des informations sensibles en se faisant passer pour une entité digne de confiance dans le cadre d'une communication électronique.
- **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.
- **Informations personnelles** : Les informations personnelles sont des données qui identifient ou peuvent être utilisées pour identifier une personne, comme son nom et son adresse physique.
- **Fraude** : La fraude est la tromperie intentionnelle ou la déformation des faits dans le but d'obtenir un avantage injuste ou malhonnête, souvent à des fins financières. Elle implique l'utilisation de pratiques trompeuses pour amener des individus, des organisations ou des systèmes à croire ou à agir sur la base de fausses informations.

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