LA LIBERTÉ
Depuis 1913

Clinique de Cyber-Criminologie

GÉNÉRATION CYBER-SMART

SITES WEB INCONNUS ET HYPERLIENS ***

Lorsque les enfants découvrent l'internet, ils deviennent naturellement curieux d'en explorer toutes les facettes et donc de visiter des sites qu'ils ne connaissent pas. S'il est bon de les laisser vagabonder et de leur donner la liberté de faire leurs propres expériences en ligne, cela peut aussi les rendre plus vulnérables et les amener à tomber sur des contenus dérangeants, à divulguer des informations personnelles ou à mettre leur appareil en danger.

generationcybersmart.ca

Un projet rendu possible financièrement grâce à :

Secrétariat aux relations canadiennes Québec

Société de la francophonie manitobaine

QU'EST-CE QU'UN HYPERLIEN? ET QU'EST-CE QU'UN SITE WEB INCONNU?

Il existe plusieurs façons d'accéder à un site web. Vous avez probablement l'habitude de saisir un site web directement dans la barre URL en haut de votre navigateur, ou de cliquer sur l'un des résultats d'une recherche Google. Mais vous pouvez aussi accéder à d'autres sites web en utilisant des hyperliens, qui sont des éléments de texte ou des images trouvés en ligne et qui renvoient à une page différente. Par exemple, ce lien vous renvoie à la page de la Clinique de cyber-criminologie, tandis que ce lien vous conduit à la page d'accueil du journal ***La Liberté***.

Les hyperliens peuvent également déclencher des téléchargements : si vous avez déjà cherché une mise à jour de logiciel en ligne, vous avez peut-être vu un bouton indiquant «Cliquez pour télécharger sur Microsoft ou sur Mac», mais les liens qui lancent l'installation d'un programme ne sont pas les seuls à le faire. Tout hyperlien peut lancer un téléchargement lorsqu'on clique dessus si le lien programmé est un lien de téléchargement, la seule exception étant si vous avez paramétré votre navigateur pour vous demander de confirmer avant le téléchargement.

Vous pouvez reconnaître un hyperlien lorsqu'il s'agit de texte, car il est généralement écrit dans une couleur différente ou souligné. Pour tout hyperlien, texte ou image, vous pouvez voir le lien auquel il mène en passant votre souris sur l'objet lié : le lien du site auquel il mène apparaîtra dans le coin inférieur gauche de votre navigateur.

Techniquement, un site web inconnu est n'importe quel site web sur lequel vous n'êtes jamais allé auparavant. Par exemple, cliquer sur un lien vers une boutique que vous avez trouvée sur Instagram, ou vers un article que vous avez trouvé sur Facebook, peut être considéré comme un site web inconnu. Cela ne signifie pas automatiquement qu'il y a un danger, et en fait, la plupart des sites web sécuritaires seront inconnus pour les enfants qui commencent à utiliser l'internet. Un hyperlien n'est pas non plus automatiquement dangereux parce que vous ne reconnaissez pas l'adresse: par exemple, ce lien (rb.gy/rmu0w1) peut vous sembler étrange, mais il vous redirigera en fait à une image de chaton sur l'article Wikipédia correspondant.

QUELS SONT LES RISQUES POUR LES ENFANTS?

L'exploration libre de l'internet par un enfant comporte quelques risques. Les hyperliens peuvent mener à n'importe quel endroit voulu par l'auteur du site web, ce qui laisse beaucoup de place aux erreurs, aux publicités, voire aux sites frauduleux ou aux maliciels. Dans le meilleur des cas, un enfant peut être conduit à un lien brisé et devra revenir en arrière, mais dans le pire des cas, il peut tomber sur du contenu inapproprié ou un site frauduleux proposant une offre d'argent rapide, par exemple.

Les hyperliens peuvent aussi déclencher des téléchargements, parfois sans avertissement ni indication, et les enfants tentés de cliquer sur un lien pourraient en fait télécharger un maliciel sans le savoir. Les enfants curieux ne réfléchissent pas toujours avant de cliquer sur des liens, des bouts de texte ou des images au hasard, et peuvent ainsi causer des dommages sans s'en rendre compte.

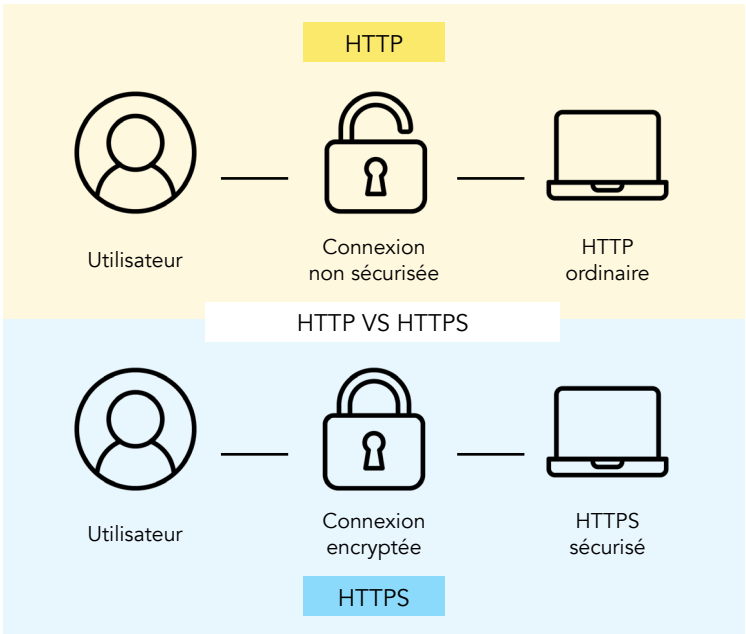
Les enfants qui visitent des sites web qu'ils ne connaissent pas peuvent également être tentés d'entrer leurs informations là où ils ne le devraient pas. Des études montrent que les enfants n'ont pas encore l'esprit critique nécessaire pour naviguer seuls en ligne et qu'ils peuvent avoir tendance à prendre les choses au pied de la lettre. Cela signifie qu'ils sont susceptibles de participer à des concours frauduleux ou de croire des publicités et des contenus sponsorisés par des influenceurs. Même lorsqu'ils ne sont pas conduits vers des contenus inappropriés, les enfants peuvent être affectés négativement par les sites web qu'ils visitent, se faire voler des informations personnelles ou être traqués lorsqu'ils visitent d'autres pages.

Les sites web inconnus peuvent également poser un problème, car ils ressemblent parfois à des sites web normaux et légitimes. Certains cybercriminels achètent des noms de site web qui ressemblent, à la lettre près, à ceux de sites fréquemment visités dans l'espoir d'attirer les personnes qui se trompent ou qui effectuent une erreur de frappe. Ils structurent le faux site web de manière à ce qu'il soit presque identique à l'original, mais avec des traceurs ou des liens qui mènent à des logiciels malveillants. Même pour les faux sites web auxquels on n'a pas accédé en se trompant d'adresse, les cybercriminels savent que leurs victimes ont plus de chance de faire confiance à un site web qui semble légitime, et ils consacrent donc beaucoup d'efforts à créer de fausses pages de connexion pour voler des identifiants et mots de passe.

Les enfants qui n'ont pas l'habitude de naviguer en ligne peuvent ne pas comprendre ce que signifie un site web qui tente d'accéder à des données sensibles, comme des informations de géolocalisation ou l'accès à la caméra ou au microphone, et ils risquent donc d'autoriser ces accès sans réfléchir. Cela peut être dangereux, car une fois l'accès accordé, les cybercriminels peuvent utiliser ces informations pour menacer les utilisateurs. De nombreuses victimes ont renoncé à de l'argent ou ont cédé à des menaces après avoir reçu un message d'un cybercriminel contenant leur adresse personnelle ou des captures d'écran de leur ordinateur.

Enfin, il existe des risques associés à ce que nous appelons les sites non sécurisés, ou les sites qui ne disposent pas d'un certificat de sécurité. Les sites web dont l'URL commence par HTTPS sont ceux qui disposent d'un certificat de sécurité vérifié, ce qui signifie que le navigateur a vérifié que les informations saisies sur le site web sont chiffrées et ne peuvent pas être interceptées par un tiers - les informations sont envoyées directement au propriétaire du site web. Dans une URL commençant par HTTP, ce n'est pas le cas : les informations saisies sont envoyées en texte clair et sont susceptibles d'être interceptées ou lues par des tiers.

Qu'est-ce que cela signifie? En tant qu'utilisateur, cela veut dire qu'il n'est pas sécuritaire de saisir ses informations, surtout ses mots de passe, sur un site web qui ne dispose pas du certificat de sécurité. Les enfants ne savent pas nécessairement qu'il faut faire attention à ce dispositif de sécurité ou ne pensent pas toujours à vérifier sa présence et peuvent saisir leurs informations personnelles alors qu'ils ne le devraient pas. Attention, cela ne signifie pas pour autant que les sites HTTPS sont toujours sûrs : les certificats de sécurité s'achètent et ne garantissent pas que le propriétaire du site est bien intentionné.



Source : https://static.semrush.com

COMMENT POUVONS-NOUS AIDER LES JEUNES?

Il est tout d'abord important d'être bien équipé pour savoir comment répondre aux questions des enfants s'ils se tournent vers vous avec un problème. Le premier conseil que nous donnons aux enfants est d'**apprendre à vérifier les liens hypertextes et à les examiner avant de cliquer**. Lorsque vous passez votre souris sur l'hyperlien, notez le nom du site web : le texte entre «www.» et «.com» ou «.ca». Effectuez une recherche rapide en ligne à propos de ce site web, en prenant note des sources qui en parlent et de la date à laquelle chaque message ou article a été écrit. Recherchez des sites web qui existent depuis plus de quelques mois, car les sites les plus récents ont plus de chance d'avoir été créés à des fins frauduleuses. Vous pouvez également trouver des informations utiles sur les forums, avec des détails sur les pratiques frauduleuses, des expériences négatives suivant la visite du site en question et d'autres risques de sécurité connus et signalés par la communauté.

Avant de télécharger un fichier sur un site inconnu, vous pouvez copier l'URL du site et le scanner à l'aide de VirusTotal pour vérifier qu'aucun maliciel ne s'y cache. C'est une ressource qui analyse les fichiers et URLs à l'aide, entre autres, des systèmes de plus de 70 antivirus et d'outils qui ont pour but de détecter et bloquer les sites créés à des fins malveillantes.

VirusTotal est également un outil que vous pouvez garder à portée de main lorsque vous aidez vos élèves à vérifier si un lien peut être dangereux. Dans nos ressources pour les enfants, nous leur disons de se méfier des liens qu'ils ne reconnaissent pas et qui leur sont envoyés par courriel ou par message personnel. Nous avons inclus ce conseil parce que les pirates essaient souvent de piéger leur prochaine victime en utilisant des comptes dont ils se sont déjà emparés en envoyant à tous leurs contacts un lien compromis, espérant attraper une victime en exploitant son lien de confiance envers la personne piratée. Si vous avez déjà reçu un message sur les réseaux sociaux de la part d'une personne dont le compte a été piraté, vous avez peut-être constaté que le message était assez vague et court, ou que l'autre personne avait entamé une conversation étrange avec vous pour vous demander de l'aide, avant d'envoyer un lien ou de demander de l'argent - la même chose peut arriver à un de vos élèves, et ces messages peuvent être envoyés autant par des amis piratés que par des personnes qu'ils ont rencontrées dans un jeu en ligne. Si vous avez des doutes sur un lien qu'un élève vous montre, vous pouvez rechercher dans les moteurs de recherche les termes exacts utilisés dans le message envoyé, car les pirates se contentent souvent de copier et de coller le même message à plusieurs personnes, ce qui augmente les chances que vous trouviez un avertissement d'un internaute. Vous pouvez également effectuer des recherches sur le site web en question en vérifiant le lien avec des sites comme VirusTotal, Scamadviser ou Scamdoc.

Enseignez aussi à vos élèves de ne pas accepter automatiquement lorsqu'un site web lui demande une certaine permission : plusieurs sites demandent à accéder à la caméra, au microphone, ou à la localisation et il est souvent plus facile d'accepter sans y penser juste pour faire disparaître la bulle de notification. Assurez-vous de souligner l'importance de se demander s'ils ont vraiment besoin de donner ces permissions afin qu'ils ne donnent pas accidentellement un accès à un pirate ou à un site compromis.

RESSOURCES

Conseils de sécurité créés par HabiloMédias sur les habitudes en ligne des enfants par tranche d'âge :

- 5 à 7 ans: https://habilomedias.ca/ressources-pedagogiques/conseils-de-securite-par-age-5-7-ans
- 8 à 10 ans: https://habilomedias.ca/ressources-pedagogiques/conseils-de-securite-par-age-8-10-ans
- 11 à 13 ans: https://habilomedias.ca/ressources-pedagogiques/conseils-de-securite-par-age-11-13-ans

VirusTotal : https://www.virustotal.com/gui/

Scamadviser : https://www.scamadviser.com/fr/accueil

Scamdoc : https://fr.scamdoc.com/

GLOSSAIRE

- **URL** : Un URL (Uniform Resource Locator) est une référence ou une adresse utilisée pour identifier des ressources sur internet. Elle précise l'emplacement d'une ressource, comme une page web, un document, une image ou un fichier, et les autres informations que votre navigateur utilise pour y accéder.
- **Navigateur internet** : Un navigateur est une application logicielle utilisée pour accéder et visualiser des informations sur internet. Il récupère et affiche des pages web, des documents, des images, des vidéos et d'autres contenus à partir de serveurs web.
- **Moteur de recherche** : Un moteur de recherche est un outil Web conçu pour aider les utilisateurs à trouver des informations sur l'internet. Il permet aux utilisateurs de rechercher un contenu spécifique en saisissant des mots-clés ou des phrases en rapport avec leur requête.
- **Hyperlien** : Un hyperlien est un élément cliquable sur une page web qui permet aux utilisateurs de naviguer entre différentes ressources sur l'internet. Il est généralement représenté par un texte souligné, une image ou un autre élément interactif qui, lorsqu'il est cliqué, dirige l'utilisateur vers une autre page web, un autre document, une autre image, une autre vidéo ou un autre contenu en ligne.
- **Site web inconnu** : Un site web inconnu est un site qui n'est pas reconnu ou familier à l'utilisateur.
- **HTTPS** : HTTPS (Hypertext Transfer Protocol Secure) est la version sécurisée de HTTP, le protocole utilisé pour transmettre des données entre un navigateur et un site web. HTTPS ajoute une couche de sécurité supplémentaire en cryptant les données échangées entre le navigateur et le site web, ce qui les rend plus sûres contre l'interception et la falsification.

- **Paramètres de sécurité et de confidentialité** : Les paramètres de sécurité et de confidentialité d'un navigateur font référence aux fonctions et contrôles intégrés conçus pour protéger les utilisateurs contre diverses menaces et vulnérabilités en ligne lorsqu'ils naviguent sur l'internet. Ces contrôles peuvent inclure des bloqueurs de fenêtres pop-up, des paramètres de localisation, des modes de navigation privée, l'accès à l'appareil photo et au microphone, etc.
- **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.
- **Forum** : Un forum est une plateforme qui permet aux utilisateurs d'engager des discussions, de partager des informations, de poser des questions et de communiquer avec d'autres personnes sur divers sujets d'intérêt.

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