Comment contrer les cybermenaces

CHUBB®

Services des risques des particuliers

Six cybermenaces courantes : comment vous protéger

Que vous voyiez aux affaires de votre foyer ou de votre entreprise, si vous utilisez Internet, un ordinateur ou d'autres appareils électroniques, vous pourriez être victime d'un cybercrime. Chez Chubb, nous cherchons à en faire plus pour nos clients, par exemple en favorisant la prévention. C'est pourquoi nous vous présentons ici six cybermenaces courantes ainsi que des conseils pour protéger votre identité, votre argent et votre famille.

1 Médias sociaux

On compte plus de 2,7 milliards d'utilisateurs actifs des médias sociaux sur la planète, soit 37 % de la population mondiale[1]. De toute évidence, ces plateformes sont des cibles de choix pour les cybercriminels.

1 utilisateur sur 10

a été victime d'une escroquerie ou d'un faux lien sur les médias sociaux2.

Chaque jour, plus de

600 000

comptes Facebook sont compromis[2].

Comment vous protéger[3]

- Publiez vos renseignements, vos messages et vos images dans un cercle restreint, soit vos **véritables amis et votre famille.**
- **Retirez votre nom** des résultats de recherches publiques.
- **Faites attention aux applications de tiers.** Elles peuvent être pratiques et divertissantes, mais certaines d'entre elles infectent votre système avec des maliciels et des virus.
- **Choisissez des mots de passe solides.** Par exemple, utilisez la première lettre de chaque mot d'une phrase pour construire votre mot de passe4; ainsi, la phrase « Quand j'avais 7 ans, ma sœur a lancé mon ourson dans la toilette » donnera le mot de passe « Qja7a,msalmodlat ».

1 We are Social, Digital in 2017: Global Overview, https://wearesocial.com/special-reports/digital-in-2017-global-overview
2 https://www.go-gulf.com/blog/cyber-crime/
3 CyberScout, Social Media Prevention Tips
4 Bruce Schneier

2 Cyberintimidation

Aujourd'hui, 90 % des adolescents sont en ligne, et 73 % d'entre eux utilisent les médias sociaux. Il allait de soi que les intimidateurs investiraient le cyberespace.

Plus de la moitié des adolescents ont été

victimes de cyberintimidation[5]

Plus de la moitié

des adolescents ont fait de la cyberintimidation.[5]

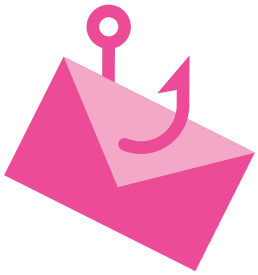
Comment protéger vos enfants contre la cyberintimidation

- Surveillez les activités de vos enfants sur leur téléphone cellulaire avec une application comme **TeenSafe.**
- Expliquez-leur votre point de vue : vous voulez **les protéger**, et non pas violer leur intimité.
- **Fixez des limites** à l'utilisation des appareils mobiles.
- Montrez l'exemple en vous déconnectant et en leur accordant **toute votre attention.**

5 « The TeenSafe Parenting Guide to Tech Safety », https://www.teensafe.com/blog/teensafe-parenting-guide-tech-safety/

3 Hameçonnage

Aux États-Unis, les travailleurs passent en moyenne 6,3 heures par jour à consulter leurs courriels[6]. Vous pourriez être surpris du nombre de courriels d'hameçonnage reçus dans le lot, où l'on joue de ruse pour que l'utilisateur clique sur une pièce jointe ou un lien malveillant.



Les courriels d'hameçonnage sont à l'origine de

90 %

des cyberattaques.[7]

Les identifiants Apple sont les

principales cibles

des voleurs d'authentifiants[8,8].

Les fausses factures sont le

principal procédé

d'hameçonnage[9].

Comment vous protéger[11]

N'ouvrez pas le courriel et ne cliquez pas sur le lien qu'il contient :

- si le ton est **urgent sans raison;**
- s'il s'agit d'une demande d'un **inconnu** ou de quelqu'un avec qui vous ne faites pas affaire actuellement;
- s'il y a **beaucoup d'erreurs de grammaire,** d'orthographe ou de syntaxe, ce qui indique que le message ne provient pas d'une source professionnelle ou fiable;
- si l'adresse URL qui s'affiche lorsque vous passez la souris sur le lien **ne correspond pas** au libellé;
- si on vous demande de fournir de l'**information sensible.**

6 Huffington Post, « U.S. Workers Spend 6.3 Hours A Day Checking Email: Survey », 13 mai 2016
7 https://blog.sonicwall.com/2018/03/phishing-emails-the-spear-of-the-cyber-attack/
8 Proofpoint, rapport Le facteur humain 2017
9 Symantec, rapport 2017 sur les cybermenaces
11 CyberScout, Phishing Protection Tips

4 Crimes liés aux appareils électroniques

De nos jours, presque tout le monde est en ligne. Les ordinateurs et les réseaux sont donc d'excellents moyens pour les cybercriminels d'accéder à vos renseignements personnels et à vos données sensibles.

Un ordinateur portable est volé toutes les

53 secondes[12]

80 %

des coûts liés à la perte d'un ordinateur portable découlent de la fuite de données[12].

Comment protéger vos appareils[13]

- **Protégez** tous vos appareils **avec un mot de passe.**
- Installez un **antivirus** et un **antimaliciel** et mettez-les à jour régulièrement.
- **Éteignez** votre ordinateur lorsque vous ne l'utilisez pas.
- **Retirez toutes les unités de stockage** avant de vous débarrasser de votre ordinateur.

Comment protéger votre réseau[13]

- **Optez toujours pour le chiffrement** (WPA ou WEP), de façon à sécuriser votre réseau et votre routeur sans fil.
- Configurez le réseau sans fil **pour qu'il ne diffuse pas son nom.**
- **Évitez d'utiliser les réseaux publics** et désactivez le Wi-Fi sur votre appareil lorsque vous ne l'utilisez pas.

12 ChannelPro Network, « Mobile Device Security: Startling Statistics on Data Loss and Data Breaches », http://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches

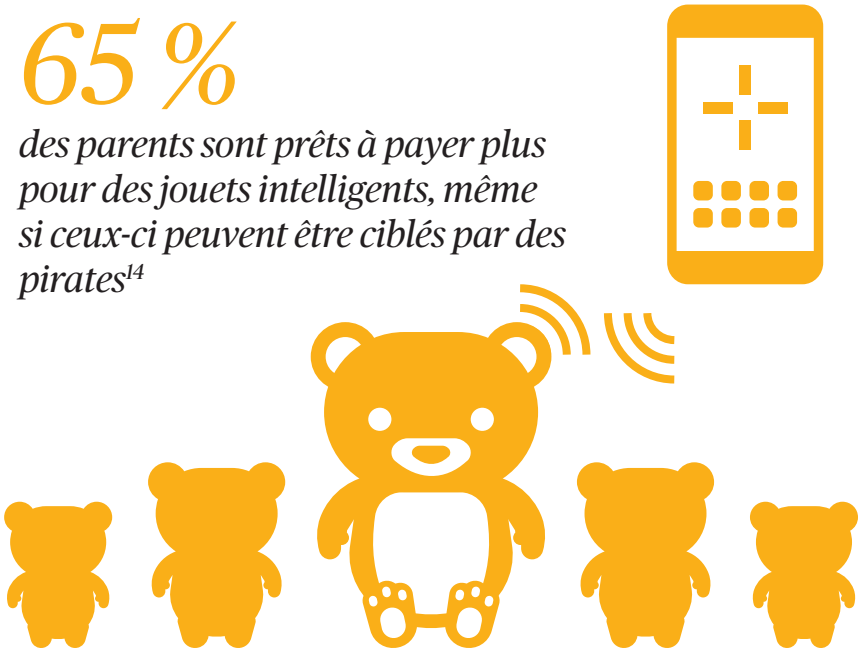
13 CyberScout, System Protection Tips

5 Jouets intelligents et maisons connectées

Dans notre monde de plus en plus connecté, les cybercriminels ne se contentent plus des cibles qui vont de soi et se tournent vers les appareils intelligents pour la maison et les jouets intelligents.

65 %

des parents sont prêts à payer plus pour des jouets intelligents, même si ceux-ci peuvent être ciblés par des pirates[14]



En 2017, les attaques visant des appareils connectés à l'Internet des objets (webcaméras, magnétoscopes numériques, thermostats connectés, etc.) ont augmenté de

600% [15]

Comment vous protéger[14]

- **Faites une recherche** dans Google sur le produit en question pour connaître les mises en garde concernant la sécurité et la confidentialité.
- **Montrez à vos enfants** ce qu'ils peuvent partager avec leur jouet intelligent, et éteignez celui-ci lorsqu'il n'est pas utilisé.
- Surveillez comment votre enfant utilise son jouet intelligent. **Éteignez-le lors** de discussions privées.
- **Modifiez le mot de passe par défaut** et mettez le logiciel à jour régulièrement.

14 CyberScout, The Dark Side of Smart Toys
15 Symantec, rapport 2018 sur les cybermenaces

6 Rançongiciel

Une attaque par rançongiciel sur votre ordinateur ou sur votre réseau a pour effet de verrouiller ou de crypter vos données afin de vous soutirer de l'argent. Selon les experts, il ne faut jamais payer la rançon, car de toute façon, il est peu probable que vous récupériez vos données. Il vaut donc mieux prévenir que guérir.

Les attaques par rançongiciel sur les appareils mobiles ont augmenté de

250 % *dans les premiers mois de 2017.*[16]

On prévoit que les coûts liés aux rançongiciels dans le monde s'élèveront à

$5 milliards de dollars

pour 2017, comparativement à 325 millions de dollars pour 2015.[17]

Comment vous protéger

- Sauvegardez vos données.
- Installez un antivirus et mettez à jour votre système régulièrement.
- Ne payez jamais la rançon demandée – vous donnerez ainsi d'autres renseignements aux pirates.

16 Kaspersky Lab Malware Report for Q1, 2017, https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-reports-mobile-ransomware-dramatically-increased-in-q1-2017

17 Cybersecurity Ventures, rapport 2017 sur les dommages causés par les rançongiciels, https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

Pour en savoir plus

Veuillez communiquer avec votre agent ou votre courtier, ou visitez le

www.chubb.com/ca-fr/personal

Chubb offre des services d'assurance de premier ordre destinés aux familles et personnes accomplies qui en ont plus à protéger. Actifs depuis plus d'un siècle et présents dans 54 pays, nous sommes fiers de tout mettre en œuvre pour que nos clients soient satisfaits et de toujours chercher à en faire davantage pour eux.

Code de formulaire : 02-01-0806 (Ed. 5/18)