

Vous êtes ici: [Accueil](#) > [Publications & Resources](#) > Protégez-vous des cyberattaques

Protégez-vous des cyberattaques

La cyberattaque peut être menée par une personne ou par un groupe. Elle s'entend de toute tentative d'accès non autorisé à un réseau ou système informatique. Elle peut viser à obtenir un avantage financier, à accéder à des données, ou encore à entacher la réputation d'une personne ou d'une entité. Les cyberattaques préoccupent de plus en plus le secteur des services financiers. En 2015, 8,5 millions de consommateurs canadiens ont été touchés par la cybercriminalité ([Rapport Norton 2016 de renseignements en matière de cybersécurité](#)) - anglaise seulement .

Pour faciliter les affaires, le secteur des services financiers mise de plus en plus sur les produits en ligne. Toutefois, les portails, les plateformes en ligne et les applications mobiles multiplient les fronts sur lesquels les consommateurs peuvent être attaqués.

Les secteurs réglementés par la CSFO, comme ceux des fournisseurs d'assurance, des courtiers en hypothèques et des régimes de retraite, ont la responsabilité de protéger les renseignements des consommateurs et d'offrir une plateforme de services en ligne sécuritaire. Ils doivent mettre en place des politiques et des processus qui aident à prévenir la cybercriminalité et qui établissent la marche à suivre en cas de cyberattaque.

Cela dit, les criminels trouvent sans cesse de nouveaux moyens de voler les renseignements confidentiels qu'ils convoitent, même quand le propriétaire protège avec soin son profil en ligne. Si vous faites des affaires en ligne avec une société de services financiers, soyez bien conscient des risques que ces transactions comportent et informez-vous des mesures à prendre pour vous protéger.

À quoi ressemble une cyberattaque?

Si certaines cyberattaques, comme celles prenant la forme de courriels suspects, vous paraissent évidentes, d'autres sont beaucoup plus difficiles à détecter. Voici quelques-uns des moyens les plus communément utilisés par les criminels pour voler vos renseignements :

Piratage : les cybercriminels accèdent à votre appareil ou aux systèmes de technologie de l'information d'une entreprise pour voler vos renseignements.

Maliciels : des virus, des logiciels espions ou des logiciels publicitaires sont installés sur votre appareil pour accéder à vos renseignements.

Détournement de domaine : les cybercriminels détournent le site Web légitime d'une entreprise vers un site Web d'apparence similaire pour enregistrer les renseignements personnels que vous entrez.

Hameçonnage : de faux courriels, messages textes et sites Web vous demandent des renseignements comme votre numéro d'assurance sociale (NAS).

Pourriels : des messages indésirables sont envoyés massivement, à vous ou à votre liste de contacts.

Écoute électronique par réseau Wi-Fi : votre historique de navigation est obtenu sur un réseau Wi-Fi non sécurisé.

Comment réduire les risques d'une cyberattaque?

Des examens réguliers de votre profil en ligne peuvent réduire votre vulnérabilité aux cyberattaques. De simples mesures préventives – comme utiliser des mots de passe complexes, changer régulièrement de mots de passe pour chacun de vos appareils et services et assurer la mise à niveau de vos logiciels – vous permettront d'éliminer 80 % des risques liés aux cyberattaques (Insurance Institute, 2015). Parmi les autres mesures que vous pouvez prendre pour assurer votre cybersécurité :

- Discutez avec vos fournisseurs de services financiers pour comprendre comment vos renseignements personnels sont protégés – [Questions sur la cybersécurité à poser à vos fournisseurs de services financiers](#)  Size: ## kb
- Évitez d'utiliser un réseau Wi-Fi public lorsque vous faites affaire avec votre fournisseur de services financiers en ligne; privilégiez une connexion cryptée ou sécurisée. Éteignez les fonctions Wi-Fi et Bluetooth lorsque vous ne les utilisez pas.
- Si vous recevez un courriel d'un fournisseur de services financiers vous demandant des renseignements, appelez-le pour confirmer sa légitimité (à un numéro autre que ceux fournis dans le courriel en question). Dans le doute, supprimez le courriel.
- Pour les achats en ligne, utilisez des options sécuritaires comme une carte de crédit. Évitez les transferts d'argent : il ne s'agit pas d'une pratique commune dans le secteur des services financiers.
- Vous trouverez d'autres conseils et ressources sur le site Web de Sécurité publique Canada : [Pensez cybersécurité](#) .

Visionnez cette vidéo de deux minutes pour sept façons de réduire le risque d'une cyberattaque

Transcription descriptive : Sept façons de réduire le risque d'une cyberattaque 

Que devriez-vous faire si vous pensez être victime d'une cyberattaque?

Si vous croyez avoir été victime d'une cyberattaque, communiquez avec votre service de police local. Avisez également vos fournisseurs de services financiers pour qu'ils restent à l'affût de toute activité suspecte dans votre compte ou qu'ils le bloquent. Ils pourraient aussi vous

conseiller de modifier votre mot de passe. Pour en savoir plus, rendez-vous au [Centre antifraude du Canada \(CAFC\)](#) .