Avez-vous été victime de cybercriminalité?

Novembre 2021 | ITSAP.00.037

Le Centre canadien pour la cybersécurité et la Gendarmerie royale du Canada (GRC) ont corédigé la présente publication afin de donner les grandes lignes de la définition, du processus signalement et des mesures d'atténuation des cybercrimes.

QU'EST-CE QUE LA CYBERCRIMINALITÉ?

La cybercriminalité comprend les crimes où la technologie est la cible (comme les maliciels ou les rançongiciels) et ceux où la technologie est un instrument important (comme le blanchiment d'argent ou la fraude).

DEVRAIS-JE SIGNALER L'INCIDENT?

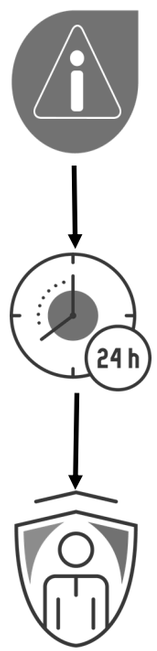
Oui! Que vous soyez la victime, que vous faisiez le signalement au nom de la victime, que vous représentiez une entreprise ou que vous soyez un témoin, nous vous encourageons fortement à signaler le cybercrime aux autorités. Vous possédez de l'information précieuse qui pourrait faire avancer une enquête, voire plus d'une. Pour obtenir les meilleurs résultats possibles, il est important de signaler l'incident dans les 24 heures suivant sa découverte.

OÙ PUIS-JE SIGNALER UN CYBERCRIME?

Vous pouvez signaler un cybercrime au service de police le plus près de chez vous. Dans les secteurs où la GRC est le service de police compétent, vous pouvez communiquer avec votre détachement. Remplissez un rapport de police et prenez en note le numéro du rapport pour vos dossiers. En plus de signaler l'incident au service de police local, vous devriez faire ce qui suit.

- Signaler l'incident dans le portail en ligne du Centre pour la criminalité afin d'obtenir du soutien et des conseils pour protéger votre organisation et éviter d'être ciblé à nouveau.
- Signaler tout incident de cybercriminalité et de fraude au Centre antifraude du Canada (CAFC), dans le Système de signalement des fraudes ou par téléphone au 1-888-495-8501. Le CAFC conserve les signalements dans un répertoire afin d'aider les organismes d'application de la loi.
- Informer vos entreprises, votre banque et vos fournisseurs de cartes de crédit pour vous assurer que vos comptes ou cartes de crédit n'ont pas été touchés ou ciblés.
- Communiquer avec les principales agences d'évaluation du crédit au Canada pour faire ajouter une alerte de fraude à votre rapport de crédit.
    - TransUnion Canada (1-866-525-0262, Québec 1-877-713-3393)
    - Equifax Canada (1-866-779-6440)
- Informer Service Canada si l'une de vos pièces d'identité émises par le gouvernement fédéral (comme votre passeport ou votre numéro d'assurance sociale) a été touchée.

Selon la nature de l'incident, votre dossier pourrait être du ressort d'un organisme fédéral. Dans un tel cas, la GRC pourrait mener l'enquête sur l'incident.



TYPES DE CYBERCRIMES

RANÇONGICIEL: Type de maliciel qui bloque l'accès d'un utilisateur à ses dossiers ou au système jusqu'à ce que l'utilisateur paye une certaine somme d'argent.

HAMEÇONNAGE: Courriels ou messages textes qui semblent provenir d'une source légitime, mais qui contiennent des pièces jointes infectées ou des liens malicieux. Si le destinataire ouvre la pièce jointe ou clique sur le lien, il pourrait télécharger un maliciel ou être dirigé vers un site Web malveillant.

POURRIEL: Message non sollicité, généralement envoyé par courriel à de nombreux utilisateurs afin de faire de la publicité ou d'arriver à une fin malveillante.

FRAUDE: Acte fautif ou criminel visant à obtenir un gain financier ou personnel.

PROTÉGEZ-VOUS

- Adoptez les pratiques exemplaires ci-dessous pour rehausser la sécurité en ligne de votre organisation.
- Utilisez un nom et un mot de passe uniques à chaque utilisateur. Augmentez la complexité en combinant des lettres, des chiffres, des caractères spéciaux ou des phrases passe. Changez les mots de passe et les phrases passe régulièrement.
- Faites les mises à jour les plus récentes pour vos applications et votre système d'exploitation (p. ex., Windows, Mac, Linux). Activez les mises à jour automatiques.
- Faites des recherches sur les applications avant de les télécharger pour éviter les arnaques. Téléchargez seulement à partir de sources fiables pour éviter les applications fausses ou malveillantes.
- Vérifiez vos paramètres de confidentialité et de sécurité dans vos comptes de médias sociaux. Faites preuve de prudence dans l'information que vous affichez en ligne.
- Établissez un plan d'intervention en cas d'incident pour améliorer votre capacité à reprendre rapidement vos activités à la suite d'un incident tout en perturbant le moins possible votre organisation.

Government of Canada | Gouvernement du Canada

Canada

 No de cat.D97-1/00-037-2021F-PDF ISBN 978-0-660-40783-8

À QUOI PUIS-JE M'ATTENDRE?

Le processus d'enquête peut sembler écrasant pour les victimes. Savoir à quoi s'attendre en tant que victime d'un cybercrime peut faciliter grandement les choses. Voici un aperçu du processus d'enquête à la suite du signalement d'un cybercrime.

PREMIÈRES ÉTAPES

- Relevez les preuves potentielles et assurez-vous que rien n'est perdu ou endommagé.
- Éliminez tout lien entre le réseau et Internet et activez le plan d'intervention en cas d'incident.
- Prenez note des personnes présentes avant, durant et après l'incident.
- Nommez une personne-ressource à qui pourront parler directement les policiers pour obtenir de l'information sur l'incident.

PROCESSUS D'ENQUÊTE

- Prenez en note le numéro du rapport de police.
- Les organismes d'application de la loi pourraient devoir accéder à votre équipement pour analyser l'aspect technologique de l'incident. Les policiers collaboreront avec vous pour recueillir des preuves sans nuire à vos affaires ni à la reprise de vos activités.
- Fournissez les registres, les déclarations d'employés, les courriels et toute autre preuve potentielle.
- Dressez une liste des personnes-ressources au sein de l'organisation pour les organismes d'application de la loi.

REPRISE DES ACTIVITÉS

- Parlez de l'incident au personnel, aux associés, aux clients et aux partenaires.
- Revoyez les politiques de cybersécurité et assurez-vous que le personnel a suivi la formation appropriée.
- Envisagez l'achat d'un anti-maliciel et d'un anti-virus pour protéger votre réseau et votre équipement.
- Améliorez la sécurité des données en appliquant des mesures de protection (p. ex., pare-feu, réseau privé virtuel, chiffrement).
- Préparez les membres concernés de l'organisation à la possibilité de devoir témoigner en cour.

ATTEINTE À LA PROTECTION DES DONNÉES

Les cybercriminels ciblent souvent les données personnelles et exclusives que vous recueillez, utilisez et conservez. Ces données peuvent être volées, puis vendues ou utilisées à des fins malveillantes. Au Canada, la Loi sur la protection des renseignements personnels s'applique au gouvernement du Canada. Les organisations du secteur privé doivent quant à eux appliquer la Loi sur la protection des renseignements personnels et les documents électroniques et suivre le processus suivant en cas d'atteinte à la protection des données:

- Signaler au bureau du commissaire à la protection de la vie privée toute atteinte à la protection des données visant des renseignements personnels qui représente un risque de préjudice réel aux personnes.
- Aviser les personnes concernées par l'atteinte.
- Conserver les dossiers visés par l'atteinte.

Pour en savoir plus sur les atteintes à la protection des données, visitez le site Web du commissaire à la protection de la vie privée.

"La cybercriminalité est la cybermenace à laquelle les citoyens et les organismes canadiens sont le plus susceptibles d'être confrontés."

POUR EN SAVOIR PLUS

Pour en savoir plus sur la cybercriminalité et le processus d'enquête connexe, visitez le site Web du Groupe national de coordination contre la cybercriminalité ou la page intitulée La cybersécurité de la GRC. Visitez le site Web du Centre pour la cybercriminalité pour en apprendre davantage sur divers sujets liés à la cybersécurité et pour consulter toutes les publications du Centre.

- Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises (ITSAP.10.035)
- Êtes-vous victime de piratage? (ITSAP.00.015)
- Rançongiciels: comment les prévenir et s'en remettre (ITSAP.00.099)
- Protéger l'organisme contre les maliciels (ITSAP.00.057)
- Reconnaître les courriels malveillants (ITSAP.00.100)

Canada