COMMENT VOUS PROTÉGER DU VOL D'IDENTITÉ EN LIGNE

JANVIER 2021 **ITSAP.00.033**

Par **identité numérique**, on entend l'information concernant une personne, une organisation ou un dispositif qui identifie une entité dans un domaine. Lorsque vous publiez ou partagez de l'information à votre sujet et au sujet de votre organisation, vous bâtissez et étoffez votre identité. Votre identité numérique établit votre réputation et votre crédibilité lorsque vous échangez avec d'autres utilisateurs ou utilisez des produits ou des services en ligne.

L'information nominative est une cible de grande valeur pour les auteurs de cybermenace, puisqu'ils peuvent la vendre ou l'utiliser pour commettre de la fraude. Les auteurs de menace peuvent voler l'information nominative en utilisant des techniques peu sophistiquées, comme le vol de courrier, ou des techniques plus sophistiquées, comme l'hameçonnage ou une attaque visant des bases de données ou des services en ligne. Une fois que l'auteur de menace dispose de suffisamment d'attributs d'identité, il peut créer des justificatifs d'identité frauduleux ou contrôler les justificatifs d'identité existants.

VOTRE IDENTITÉ NUMÉRIQUE

Votre **identité numérique** comprend tous les attributs d'identité personnelle que l'on retrouve en ligne à votre sujet, comme votre date de naissance, votre numéro d'assurance sociale, vos renseignements médicaux, votre numéro de téléphone et vos justificatifs d'ouverture de session.

Ces données sont recueillies et échangées lorsque vous utilisez vos comptes de médias sociaux, des inscriptions en ligne, des comptes financiers et d'autres comptes de services. Vos données sont également recueillies lorsque vous utilisez des navigateurs Internet, des bases de données en ligne (dans le secteur de la santé et le milieu universitaire, par exemple) et des services infonuagiques. L'ensemble des attributs de votre identité numérique augmente à mesure que vous utilisez de nouveaux services, que vous interagissez avec des organisations dans le monde réel et que ces dernières mettent leurs données en ligne.

LES MENACES QUI PÈSENT SUR VOTRE IDENTITÉ

Toute information personnelle partagée en ligne court le risque d'être compromise ou volée. Vous trouverez ci-dessous certaines des principales menaces qui pèsent sur votre identité numérique.

HAMEÇONNAGE

Un fraudeur vous appelle, vous envoie un texto ou un courriel, ou communique avec vous par l'entremise des médias sociaux pour vous inciter à cliquer sur un lien malveillant, à télécharger un maliciel ou à divulguer de l'information sensible.

PIRATAGE PSYCHOLOGIQUE

Un fraudeur utilise une attaque par hameçonnage plus personnalisée pour vous cibler directement. Les attaques par piratage psychologique ajoutent souvent des détails personnels à propos de vous ou de votre organisation pour vous inciter à fournir de plus amples détails vous concernant.

HYPERTRUCAGE

Un auteur de menace utilise des supports synthétiques (p. ex. des vidéos, des extraits audio et des photos) afin d'usurper votre identité ou celle de votre organisation aux fins d'authentification ou de falsification en vue de voler de l'information sensible ou de répandre de la mésinformation.

ATTEINTES À LA PROTECTION DES DONNÉES PAR UNE TIERCE PARTIE

Le réseau et les données sensibles de votre fournisseur sont compromis par des auteurs de menace. Les réseaux externes et l'information (p. ex. les données des clients et les justificatifs d'identité) traitée par le fournisseur compromis sont à risque. Les justificatifs d'identité compromis peuvent être utilisés pour accéder à d'autres comptes et étendre la portée de l'attaque.

SÉRIE SENSIBILISATION

PROTÉGEZ VOTRE IDENTITÉ

Pour protéger votre identité numérique, il convient de mettre en place des pratiques exemplaires en matière de sécurité comme celles indiquées ci-dessous.

UTILISEZ UN RÉSEAU WI-FI SÉCURISÉ

Sécurisez votre réseau Wi-Fi en modifiant le nom par défaut du réseau (SSID) et le mot de passe qui ont été fournis avec votre routeur et votre compte. Il est préférable de ne pas utiliser les réseaux Wi-Fi publics, en particulier si vous devez transmettre de l'information sensible ou vous connecter à des comptes de nature sensible. Si vous devez utiliser un réseau Wi-Fi public, protégez votre information sensible au moyen d'un réseau privé virtuel (RPV).

UTILISEZ DES OUTILS ET DES LOGICIELS DE SÉCURITÉ

Installez un pare-feu pour filtrer et bloquer le trafic malveillant, et protéger votre réseau des menaces externes. Installez un antivirus pour analyser vos dispositifs et détecter les maliciels, et un logiciel anti-hameçonnage pour bloquer les tentatives d'hameçonnage. Assurez-vous de mettre à jour régulièrement tous les logiciels et toutes les applications.

SÉCURISEZ VOS COMPTES

Utilisez des mots de passe et des phrases de passe robustes combinés à l'authentification multifacteur (MFA pour *Multi-Factor Authentication*) pour sécuriser tous les comptes. La MFA ajoute une couche de sécurité additionnelle et protège votre compte advenant la compromission de votre mot de passe.

Gardez vos comptes de médias sociaux personnels privés en limitant le nombre d'utilisateurs autorisés à voir le contenu que vous mettez en ligne (p. ex. réduire les risques d'hypertrucage). Dans le cas des comptes de médias sociaux d'entreprise, rappelez aux employés qui gèrent les comptes de faire preuve de prudence quant à l'information qu'ils publient en ligne.

PARTAGEZ JUDICIEUSEMENT

Avant de vous inscrire à un service ou à un compte, vous devriez effectuer des recherches sur l'entité à qui vous confierez vos données. Passez en revue les politiques de l'entreprise en matière de protection de la vie privée pour déterminer si votre information personnelle est traitée par une tierce partie.

Si on vous envoie une demande non sollicitée, réfléchissez bien avant de fournir votre information personnelle. Ne cliquez pas sur les liens contenus dans les messages texte et les courriels. Vérifiez l'identité de la personne ou de l'entreprise qui vous demande de fournir cette information et la légitimité de la demande. En cas de doute, communiquez avec l'entreprise (p. ex. votre banque) au moyen des coordonnées publiées sur le site Web officiel.

GÉREZ ET SURVEILLEZ VOS COMPTES

Vérifiez vos comptes régulièrement et surveillez vos comptes financiers pour toute activité suspecte. Si vous n'utilisez plus un compte (p. ex. un compte d'achats en ligne), assurez-vous de supprimer l'information personnelle qu'il contient, puis de supprimer le compte.

SIGNALEZ TOUT VOL D'IDENTITÉ

Si votre identité numérique a été compromise, prenez immédiatement les mesures suivantes :

1. Signalez l'incident à la source du compte ainsi qu'aux autres comptes connexes (p. ex. ouverture de session depuis des sources partenaires).
2. Déterminez quelle est l'information touchée (p. ex. des données financières, un numéro d'assurance sociale).
3. Changez les mots de passe et les questions de sécurité de tous les comptes qui sont associés au compte compromis (p. ex. comptes partenaires, courriels) ou qui utilisent le même mot de passe.
4. Faites appel aux services d'Equifax et de TransUnion pour analyser votre rapport de solvabilité et activer les alertes afin d'être informé de toute demande non autorisée.
5. Signalez l'incident au Centre antifraude du Canada au 1-888-495-8501 ou en ligne.
6. Informez un organisme d'application de la loi de la situation.
7. Signalez tout vol d'identité organisationnelle au Centre pour la cybersécurité (**contact@cyber.gc.ca**).

POUR EN SAVOIR PLUS

Visitez le site Web du Centre canadien pour la cybersécurité (cyber.gc.ca) pour en apprendre plus sur la cybersécurité et les services offerts par l'organisme. Vous y trouverez le catalogue qui contient, notamment, les publications suivantes :

- ITSAP.00.071, *Comment faire des achats en ligne en toute sécurité*;
- ITSAP.00.080, *Utilisation sûre des services bancaires en ligne*;
- ITSAP.80.101, *Les réseaux privés virtuels*;
- ITSAP.00.101, *Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage*;
- ITSAP.30.032, *Pratiques exemplaires de création de phrases de passe et de mots de passe*;
- ITSAP.30.030, *Sécurisez vos comptes et vos appareils avec une authentification multifacteur*;
- ITSAP.80.009, *Utiliser la technologie Wi-Fi dans votre organisation en toute sécurité*.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.