Comment vous protéger du vol d'identité en ligne

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mai 2024 | ITSAP.00.033

Par identité numérique, on entend l'information concernant une personne ou une organisation qui identifie de façon unique cette 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 cette identité. Votre identité numérique établit votre réputation et votre crédibilité lorsque vous échangez avec d'autres personnes ou lorsque vous utilisez des produits ou des services en ligne.

L'information nominative est une cible de grande valeur pour les auteures et auteurs de cybermenace qui cherchent à vendre cette information ou à l'utiliser à des fins frauduleuses. Les auteures et 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'auteure ou 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, par exemple :

- votre date de naissance;
- votre numéro d'assurance sociale;
- vos renseignements médicaux;
- votre numéro de téléphone;
- vos justificatifs d'ouverture de session.

Ces données sont recueillies et transmises lorsque vous utilisez vos comptes en ligne, notamment vos comptes de médias sociaux, vos abonnements en ligne, vos comptes financiers et autres. Vos données sont aussi recueillies lorsque vous utilisez des navigateurs Web, des services infonuagiques et des bases de données en ligne, comme des plateformes de santé ou d'enseignement. L'ensemble des attributs de votre identité numérique augmente à mesure que vous utilisez de nouveaux services et que les organisations avec lesquelles vous interagissez dans le monde réel mettent plus de données en ligne.

Les menaces qui pèsent sur votre identité numérique

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

Une fraudeuse ou un fraudeur vous appelle, vous envoie un texte ou un courriel, ou utilise les médias sociaux pour vous inciter à :

- cliquer sur un lien malveillant;
- télécharger un maliciel;
- transmettre de l'information sensible.

Lecture complémentaire: Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101), et Qu'est-ce que l'hameçonnage vocal (ITSAP.00.102)

Piratage psychologique

Une fraudeuse ou un fraudeur mène 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.

Lecture supplémentaire: Piratage psychologique (ITSAP.00.166) et Reconnaître les courriels malveillants (ITSAP.00.100)

Atteintes à la protection des données d'une tierce partie

Une atteinte à la protection des données d'une tierce partie se produit lorsqu'une auteure ou un auteur de menace compromet le réseau et les données sensibles de votre fournisseur. Les réseaux et l'information externes, comme les données et les justificatifs d'identité des clientes et clients, gérés par le fournisseur compromis sont à risque. Les auteures et auteurs de menace peuvent se servir de justificatifs d'identité compromis pour accéder à d'autres comptes et étendre la portée de l'attaque.

Lecture complémentaire: Apprenez à protéger votre information et vos données lorsque vous utilisez des applications (ITSAP.40.200)

Hypertrucages

Une auteure ou un auteur de menace utilise des supports synthétiques, tels que des vidéos, des extraits audio et des photos, afin d'usurper votre identité ou celle de votre organisation. Il peut également employer ce support aux fins d'authentification ou de falsification en vue de voler de l'information sensible ou de répandre de la mésinformation.

Lecture supplémentaire: Repérer les cas de mésinformation, désinformation et malinformation (ITSAP.00.300), L'intelligence artificielle générative (ITSAP.00.014) et Biométrie (ITSAP.00.019)

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

No de cat. D97-1/00-033-2024F-PDF
ISBN 978-0-660-72035-7

Canada

Comment vous protéger du vol d'identité en ligne

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
Mai 2024 | ITSAP.00.033

Protéger votre identité numérique

Pour protéger votre identité numérique, vous devriez mettre en œuvre des pratiques exemplaires de base en matière de cybersécurité.

Utilisez un réseau Wi-Fi sécurisé

Sécurisez votre réseau Wi-Fi en modifiant le nom par défaut du réseau, soit l'identifiant de l'ensemble de services (SSID pour *Service Set Identifier*), et le mot de passe par défaut qui ont été fournis avec votre routeur et votre compte de service. Évitez d'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, servez-vous d'un réseau privé virtuel pour protéger votre information sensible.

Utilisez des outils et des logiciels de sécurité

Installez un pare-feu pour protéger votre réseau des menaces externes. Un pare-feu filtre et bloque le trafic malveillant. Installez un logiciel antivirus pour analyser vos appareils et détecter les maliciels, et un logiciel antihameçonnage 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 une authentification multifacteur (AMF) résistante à l'hameçonnage pour sécuriser tous les comptes. L'AMF ajoute une couche de sécurité additionnelle et protège votre compte advenant la compromission de votre mot de passe.

Gardez vos comptes personnels de médias sociaux privés pour limiter le nombre de personnes qui peuvent voir le contenu que vous partagez en ligne. Cette mesure peut réduire les risques d'hypertrucage. Dans le cas des comptes de médias sociaux d'entreprise, rappelez aux membres du personnel qui gèrent les comptes de faire preuve de prudence quant à l'information qu'ils publient en ligne.

Choisissez judicieusement les renseignements personnels que vous communiquez

Avant de vous inscrire à un service ou à un compte, vous devriez effectuer des recherches sur l'entité à laquelle vous confierez vos données. Passez en revue les politiques de l'entreprise en matière de protection de la vie privée pour savoir comment les tierces parties traitent votre information personnelle.

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 au moyen des coordonnées publiées sur le site Web officiel.

Gérez et surveillez vos comptes

Vérifiez vos comptes régulièrement et surveillez vos comptes financiers afin de détecter toute activité suspecte. Si vous n'utilisez plus un compte, assurez-vous de retirer l'information personnelle qu'il contient, puis de supprimer le compte.

Intervenir à un vol d'identité numérique

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

- Signalez l'incident à la source du compte ainsi qu'aux autres comptes connexes.
- Déterminez quelle est l'information touchée, comme des données financières ou un numéro d'assurance sociale.
- Changez les mots de passe et les questions de sécurité de tous les comptes qui sont associés au compte compromis, notamment les comptes partenaires et les courriels d'ouverture de session, ou qui utilisent le même mot de passe.
- Faites appel aux services d'Equifax et de TransUnion pour analyser votre rapport de solvabilité et activer les alertes afin d'être informée ou informé de toute demande non autorisée.
- Signalez l'incident au Centre antifraude du Canada au 1-888-495-8501 ou en ligne.
- Informez un organisme d'application de la loi de la situation.
- Communiquez avec le Centre pour la cybersécurité pour signaler tout vol d'identité organisationnelle.

Pour en savoir plus

- Comment faire des achats en ligne en toute sécurité (ITSAP.00.071)
- Utilisation sûre des services bancaires en ligne (ITSAP.00.080)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Utiliser le Wi-Fi sans compromettre la sécurité de votre organisation (ITSAP.80.009)
- Empreinte numérique (ITSAP.00.133)
- Étapes à suivre pour déployer efficacement l'authentification multifacteur (AMF) (ITSAP.00.105)
- Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) (ITSAP.30.018)
- Facteurs à considérer lors de l'utilisation des médias sociaux dans votre organisation (ITSM.10.066)