Empreinte numérique

Février 2024

ITSAP.00.133

Votre organisation utilise Internet pour mener des activités opérationnelles, fournir des capacités de télétravail aux employées et employés et offrir des services à la clientèle. À la lumière des activités que réalisent vos employées et employés ainsi que partenaires sur différentes plateformes et applications en ligne, vous devriez songer à l'empreinte numérique qu'ils laissent derrière eux et prendre les mesures de sécurité appropriées pour la protéger. Les empreintes numériques contiennent de l'information sensible dont peuvent tirer profit les auteures et auteurs de menace. À l'aide de techniques de suivi et de surveillance, les auteures et auteurs de menace peuvent accéder à cette information sensible et l'exfiltrer, compromettant ainsi sa confidentialité et sa sécurité.

À propos des empreintes numériques

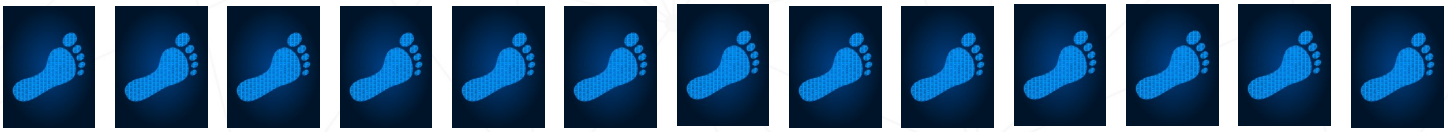
Une empreinte numérique désigne la trace de données que vous créez lorsque vous utilisez Internet. Cette trace de données est issue des sites Web que vous consultez, des courriels que vous envoyez et de l'information que vous soumettez ou téléchargez en ligne. Vous contribuez à votre empreinte de façon active et passive.

- **Empreinte numérique active :** Données laissées à la suite d'activités intentionnelles, telles que l'affichage de contenu sur les médias sociaux, le remplissage de formulaires en ligne ou l'acceptation des témoins de navigateur.
- **Empreinte numérique passive :** Données laissées involontairement ou sans le savoir. Ces données sont souvent recueillies par la surveillance de votre adresse IP. Les sites Web et les applications peuvent installer des témoins sur les dispositifs sans vous en aviser, utiliser le suivi de la location ou consigner vos activités.

Comprendre les risques

Votre organisation est tenue de protéger l'information sensible qu'elle recueille, comme les noms des clientes et clients, les données financières et l'information d'identification personnelle. Les auteures et auteurs de menace sont à la recherche de vulnérabilités qu'ils peuvent exploiter pour accéder à de l'information sensible.

La protection de l'information sensible de vos clientes et clients est extrêmement importante. Les empreintes numériques compromises peuvent entraîner un vol d'identité, des problèmes liés à la vérification des antécédents et porter atteinte à la réputation. Mettez en place les mesures préventives nécessaires afin de protéger la confidentialité et l'intégrité de votre information sensible. Tout défaut de protéger cette information peut nuire à la réputation de votre organisation.



Connaître les menaces

Les auteures et auteurs de menace tentent d'exploiter les vulnérabilités et d'accéder à de l'information sensible au moyen de techniques de collecte de données par l'entremise des empreintes actives et passives. Les techniques les plus courantes comprennent les attaques par hameçonnage et la mystification de sites Web. En cliquant sur un lien, en téléchargeant une pièce jointe ou en échangeant de l'information sensible, vous facilitez l'accès des auteures et auteurs malveillants à votre empreinte numérique.

Les algorithmes d'intelligence artificielle (IA) peuvent aussi poser une menace pour votre empreinte numérique. Ils peuvent analyser vos empreintes numériques pour faire un suivi de vos comportements en ligne. Une ou un auteur de menace peut avoir recours à ces données pour voler votre identité.

Les programmes « prenez votre appareil personnel (PAP) », les appareils intelligents et les réseaux Wi-Fi non sécurisés sont des vecteurs que peuvent employer les auteures et auteurs de menace pour recueillir des données. Compte tenu du grand nombre de personnes qui font du télétravail, des données sensibles sont susceptibles d'être transmises sur des appareils et des réseaux qui ne sont pas protégés par les mesures de sécurité appropriées.

Si votre entreprise gère des commandes en ligne, vous devez prendre en compte des considérations supplémentaires relatives à la protection des données sensibles. Pour obtenir plus de détails sur le chiffrement et la navigation sécurisée, lisez Utiliser le chiffrement pour assurer la sécurité des données sensibles (ITSAP.40.016).

SÉRIE SENSIBILISATION

No de cat. D97-1/00-133-2024F-PDF
ISBN 978-0-660-69845-8

Protection de la vie privée

La protection de la vie privée est importante. Afin de réduire les risques d'exploitation des données sensibles, veuillez envisager l'adoption des mesures suivantes.

Formez et sensibilisez vos employés. Vos employées et employés doivent être au fait des enjeux relatifs à la cybersécurité et à la protection de la vie privée. La formation devrait comprendre un volet sur les mesures appropriées de protection et de traitement de l'information ainsi qu'un volet sur les pratiques exemplaires en matière de cybersécurité.

Lisez les politiques de confidentialité et les conditions d'utilisation. Avant de télécharger une application ou d'utiliser un service, il est important de lire et de bien comprendre les types d'information recueillie, les façons dont cette information peut être utilisée et les mesures de sécurité en place pour protéger les renseignements personnels.

Désactivez les témoins, dans la mesure du possible. Même si vous ne partagez pas activement de l'information sur les applications et sites Web, vos données font l'objet d'un suivi par l'entremise de votre appareil, de votre adresse IP et de votre réseau.

Configurez les paramètres par défaut. Les paramètres de certaines applications sont réglés par défaut à « accès public ». Configurez plutôt vos paramètres de sécurité et de protection de la vie privée au mode le plus sécurisé et restrictif possible.

Désactivez les paramètres de surveillance. Évitez d'utiliser les applications non nécessaires qui exigent l'accès à votre emplacement, à votre calendrier ou à vos contacts. Désactivez les paramètres qui analysent et surveillent vos activités dans le but de vous présenter de la publicité ciblée.

Restez au fait des changements apportés aux conditions d'utilisation, aux mises à jour et aux paramètres de protection de la vie privée des applications

Autres considérations liées à la cybersécurité

Pour veiller à ce que vos activités en ligne soient à l'abri des auteures et auteurs de cybermenace, envisagez de mettre en œuvre les mesures préventives suivantes :

- installez un antivirus et un pare-feu pour réduire les risques de partage passif des données;
- appliquez l'authentification multifacteur (AMF) et imposez la création de mots de passe ou de phrases de passe robustes et uniques pour tous les comptes et dispositifs;
- évitez de vous connecter à un Wi-Fi public, utilisez plutôt des réseaux sécurisés et un réseau privé virtuel (RPV);
- déployez un système de gestion des appareils ou des applications mobiles afin de surveiller les programmes PAP;
- limitez la navigation de sites Web non chiffrés;
- installez des extensions de navigateur Web qui renforcent la protection de la vie privée (comme des bloqueurs de publicité);
- mettez en œuvre des listes d'applications ou bloquez les adresses IP, les noms de domaine et les types de fichiers reconnus pour être malveillants;
- retirez les comptes et les privilèges d'accès aux employées et employés qui n'en ont plus besoin;
- accordez l'accès aux utilisatrices et utilisateurs selon le principe du besoin de connaître et classifiez les données en fonction du niveau de sensibilité;
- créez une politique relative à l'utilisation des médias sociaux pour clarifier les attentes relatives au contenu pouvant être partagé sur les comptes organisationnels;
- etirez les métadonnées des photos avant de les partager et de les afficher en ligne,
    - car ces informations sont stockées dans le fichier image et peuvent exposer des renseignements personnels tels que votre emplacement géographique.

Pour en savoir plus

Pour plus d'information, consultez les ressources

- Sécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations (ITSAP.00.070)
- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- Sécurité de l'Internet des objets (ITSAP.00.012)
- Est-ce que votre appareil intelligent vous écoute? (ITSAP.70.013)
- Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles (ITSAP.70.002)
- Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093)
- Comment vous protéger du vol d'identité en ligne (ITSAP.00.033)
- Comment protéger votre organisation contre les menaces internes (ITSAP.10.003)
- Les réseaux privés virtuels (ITSAP.80.101)
- Liste d'applications autorisées (ITSAP.10.095)
- Système d'adressage par domaine de protection (ITSAP.40.019)
- Utilisation de comptes personnels de médias sociaux au travail (ITSAP.00.066)
- Intelligence artificielle (ITSAP.00.040)
- Étapes à suivre pour déployer efficacement l'authentification multifacteur (ITSAP.00.105)
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)

Le Carrefour de l'apprentissage offre également des cours de formation

- Cours 110 – La cybersécurité dans le GC et la visibilité en ligne (1/2 journée)
- Cours 108 – Les pratiques exemplaires en matière de cybersécurité (1 journée)

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**.