LA CYBERSÉCURITÉ À LA MAISON ET AU BUREAU – SÉCURISER VOS DISPOSITIFS, VOS ORDINATEURS ET VOS RÉSEAUX

OCTOBRE 2020 | ITSAP.00.007

Avec la popularité grandissante du télétravail, nous dépendons d'un plus grand nombre de dispositifs et devons être en mesure de nous connecter à Internet à des fins professionnelles et personnelles. Les auteurs de cybermenace tirent avantage de notre dépendance à la technologie. Protégez-vous en faisant l'inventaire de tous les produits de technologie que vous utilisez, y compris vos dispositifs mobiles et intelligents, vos ordinateurs et vos réseaux sans fil. En sachant ce que vous avez, vous pourrez prioriser vos efforts en matière de sécurité et mettre en place les mesures de protection appropriées. Vous ne savez pas par où commencer? Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) a les conseils et les orientations dont vous avez besoin et a regroupé ci-dessous une série de ces produits d'information.

Vous trouverez l'ensemble de notre catalogue de produits et services sur notre site Web (**cyber.gc.ca**).

DISPOSITIFS MOBILES ET INTELLIGENTS

Nos dispositifs sont essentiels à tous les aspects de notre vie. Nous les utilisons dès notre réveil et jusqu'au moment où nous allons au lit. Nos électroménagers, nos montres, et même nos thermostats et nos systèmes de sécurité, sont connectés à Internet. Avec une telle dépendance à nos téléphones, il n'est pas surprenant que les auteurs de menace les considèrent comme des cibles de choix pour obtenir des renseignements personnels en vue de commettre des crimes, comme le vol d'identité. Heureusement, vous pouvez contrer les tentatives des auteurs de menace en prenant quelques mesures simples pour améliorer votre sécurité.

Dans un monde où tout semble pouvoir être stocké ou exécuté sur un dispositif intelligent, comment pouvons-nous nous assurer que notre information personnelle demeure, comment dire, personnelle? Les auteurs de menace arrivent à s'introduire dans ces dispositifs, car ils sont nombreux, ils sont connectés à Internet et souvent, ils ne sont pas adéquatement sécurisés. Certains de vos dispositifs n'ont pas la même puissance de calcul qu'un ordinateur de bureau ou un portable, ce qui les rend plus vulnérables aux auteurs de menace. Pour vous défendre contre d'éventuelles cyberattaques, il convient de vous familiariser avec les paramètres de confidentialité de vos dispositifs, de veiller à utiliser des phrases de passe ou des mots de passe uniques et complexes et d'utiliser l'authentification multifacteur pour vos comptes.

CONSEILS SUR L'UTILISATION DE VOS DISPOSITIFS

- *Utiliser son dispositif mobile en toute sécurité (ITSAP.00.001)*
- *Dispositifs mobiles et voyages d'affaires (ITSAP.00.087)*
- *Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles (ITSAP.70.002)*
- *Sécurité de l'internet des objets pour les petites et moyennes organisations (ITSAP.00.012)*
- *Utiliser la technologie Bluetooth (ITSAP.00.011)*
- *Messagerie instantanée (ITSAP.00.266)*

CONSEILS SUR LA FAÇON DE SÉCURISER VOS DISPOSITIFS

- *Application des mises à jour sur les dispositifs (ITSAP.10.096)*
- *Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)*
- *Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)*
- *Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques (ITSAP.30.036)*
- *Conseils de sécurité sur les gestionnaires de mots de passe (ITSAP.30.025)*
- *Êtes-vous victime de piratage? (ITSAP.00.015)*
- *Conseils de sécurité pour les organisations dont les employés travaillent à distance (ITSAP.10.016)*

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

ORDINATEURS

Nous nous servons de nos portables et de nos PC pour effectuer des opérations que nos dispositifs intelligents ne peuvent faire aussi efficacement. Pour veiller à ce que vos dispositifs fonctionnent correctement et éviter de compromettre votre information, assurez-vous de mettre en place les mesures de sécurité nécessaires pour les protéger des cybermenaces, ainsi que l'information qu'ils contiennent.

RÉSEAUTAGE

Les dispositifs réseau, comme les routeurs et les modems, sont le fondement de tout accès à Internet et de l'utilisation de vos appareils. On oublie facilement les services qu'ils offrent, jusqu'à ce qu'Internet tombe en panne. Les dispositifs réseau sont les gardiens des appareils qui y sont connectés et doivent, à ce titre, être sécurisés.

CONSEILS SUR LA FAÇON DE RECONNAITRE LES CYBERMENACES

- *Protéger l'organisme contre les maliciels (ITSAP.00.057)*
- *Rançongiciels : comment les prévenir et s'en remettre (ITSAP.00.099)*
- *Reconnaître les courriels malveillants (ITSAP.00.100)*
- *Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)*
- *Protection d'un organisme contre les macros malveillantes (ITSAP.00.200)*

CONSEILS SUR LA FAÇON DE SÉCURISER VOTRE RÉSEAU

- *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.189)*
- *Conseils de cybersécurité pour le télétravail (ITSAP.10.116)*
- *Protéger son organisation contre les attaques par déni de service (ITSAP.80.100)*
- *Rapport du centre pour la cybersécurité sur la virtualisation des centres de données : pratiques exemplaires en matière de virtualisation des centres de données (ITSP.70.010)*

CONSEILS SUR LA FAÇON DE TRAVAILLER EN TOUTE SÉCURITÉ

- *Utiliser un poste de travail virtuel à la maison et au bureau (ITSAP.70.111)*
- *Vidéoconférence (ITSAP.10.216)*
- *Considérations liées à la sécurité dans le cadre de l'utilisation de logiciels libres (ITSAP.10.059)*
- *Protection de l'information de grande valeur : Conseils pour les petites et moyennes organisations (ITSAP.40.001)*
- *Sécurité des TI : difficultés observées chez les employés (ITSAP.00.005)*
- *Sauvegarder et récupérer vos données (ITSAP.40.002)*

CONSEILS SUR L'UTILISATION DE SERVICES FONDÉS SUR L'INFONUAGIQUE

- *Qu'est-ce que l'infonuagique? (ITSAP.50.110)*
- *Avantages et risques liés à l'adoption des services fondés sur l'infonuagique par votre organisation (ITSE.50.060)*
- *Modèles de l'infonuagique (ITSAP.50.111)*
- *Gestion des risques liés à la sécurité infonuagique (ITSM.50.062)*
- *Guide sur la défense en profondeur pour les services fondés sur l'infonuagique (ITSP.50.104)*
- *Guide sur l'évaluation et l'autorisation de la sécurité infonuagique (ITSP.50.105)*