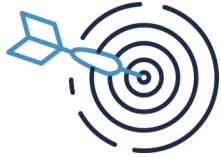


FOCUSED CYBER SECURITY ADVICE AND GUIDANCE DURING COVID-19



The **COVID-19 pandemic** has proven to be an extremely disruptive event, affecting all components of society. The IT world is not immune. The pandemic has forced both public and private sectors to rethink how, when, and where work is performed. Traditional models of office versus home-based work environments have been completely inverted; in many cases, most employees are now working remotely. This inversion has caused IT management, implementers, and clients to scramble to adapt to a new way of working. Unfortunately, this rapid transformation presents both new and unique opportunities for threat actors to take advantage of. The entire IT hierarchy, from management to client, must be made explicitly aware of this fact and take every precaution possible.

The Canadian Centre for Cyber Security (Cyber Centre) has created a valuable collection of advice and guidance products, many of which are now more relevant than ever. To assist you during this disruptive time, we curated a selection of our products and organized them by area of interest. We hope this helps, and, as always, we are here to assist you whenever possible. **You may find our complete list of guidance products at: cyber.gc.ca/**

IT MANAGEMENT GUIDANCE

- [Top 10 IT Security Actions: #6 Provide Tailored Cyber Security Training \(ITSM.10.093\)](#)
- [Cloud Security Risk Management \(ITSM.50.062\)](#)
- [Top 10 IT Security Actions to Protect Internet-Connected Networks and Information \(ITSM.10.189\)](#)



IT IMPLEMENTER GUIDANCE

- [Implementation Guidance: Email Domain Protection \(ITSP.40.065\)](#)
- [Cyber Centre Data Centre Virtualization Report: Best Practices for Data Centre Virtualization \(ITSP.70.010\)](#)
- [Steps to Address Data Spillage in the Cloud \(ITSAP.50.112\)](#)
- [Security Tips for Organizations with Remote Workers \(ITSAP.10.016\)](#)
- [Using Virtual Desktop At-Home and In-Office \(ITSAP.70.111\)](#)
- [Security Considerations for Mobile Device Deployments \(ITSAP.70.002\)](#)
- [Protecting Your Organization Against Denial of Service Attacks \(ITSAP.80.100\)](#)



CLIENT AWARENESS

- [Don't Take the Bait: Recognize and Avoid Phishing Attacks](#)
- [Cyber Hygiene for COVID-19](#)
- [Video Teleconferencing ITSAP.10.216](#)
- [How Updates Secure Your Device \(ITSAP.10.096\)](#)
- [Secure Your Accounts and Devices with Multi-Factor Authentication \(ITSAP.30.030\)](#)
- [Protect Your Organization From Malware \(ITSAP.00.057\)](#)
- [Virtual Private Networks \(ITSAP.80.101\)](#)
- [Ransomware: How to Prevent and Recover \(ITSAP.00.099\)](#)
- [Rethink Your Password Habits to Protect Your Accounts from Hackers \(ITSAP.30.036\)](#)
- [Best Practices for Passphrases and Passwords \(ITSAP.30.032\)](#)
- [Using Bluetooth Technology \(ITSAP.00.011\)](#)
- [Spotting Malicious Email Messages \(ITSAP.00.100\)](#)



ADDITIONAL INFORMATION

- [RSS feed](#)
- [Alerts and Advisories](#)
- [Contracting with Managed Service Providers](#)
- [Canadian Shield—Sharing the Cyber Centre's Threat Intelligence to Protect Canadians During the COVID-19 Pandemic](#)

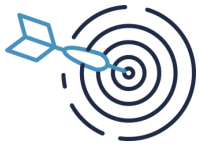


Traditional models of office vs. home-based work environments have been completely inverted.

Need help or have questions? Want to stay up to date and find out more on all things cyber security? Visit the Cyber Centre website at cyber.gc.ca



CONSEILS CIBLÉS SUR LA CYBERSÉCURITÉ APPLICABLES DURANT LA PANDÉMIE DE COVID-19



La pandémie de COVID-19 est un événement extrêmement perturbateur qui touche toutes les composantes de la société. Et le monde des TI n'est pas immunisé. La pandémie a contraint les secteurs public et privé à repenser comment, quand, et où le travail est effectué. Les modèles traditionnels des environnements de travail au bureau et à domicile ont été complètement inversés; dans de nombreux cas, une majorité d'employés font du télétravail. Cette inversion force les membres de la direction, les responsables de la mise en œuvre et les clients des TI à s'adapter à une nouvelle façon de travailler. Malheureusement, cette transformation rapide présente de nouvelles possibilités pour les auteurs de cybermenaces qui tentent par tous les moyens d'en profiter. Il est impératif que l'ensemble de la chaîne hiérarchique des TI, de la direction aux clients, soit sensibilisée à ce sujet et que l'on prenne toutes les précautions possibles.

Le Centre canadien pour la cybersécurité (ou Centre pour la cybersécurité) a compilé et organisé par domaines d'intérêt une vaste gamme d'avis et de conseils qui sont plus pertinents que jamais. Nous espérons que cela vous prètera main-forte et, comme toujours, nous sommes là pour vous aider si vous avez besoin de nous. **Une liste complète des documents de conseils et d'orientation se trouve à l'adresse suivante : cyber.gc.ca.**

CONSEILS POUR LES MEMBRES DE LA DIRECTION DES TI



- [Les 10 mesures de sécurité des TI : NO 6, Miser sur une formation sur mesure en matière de cybersécurité \(ITSM.10.093\)](#)
- [Gestion des risques liés à la sécurité infonuagique \(ITSM.50.062\)](#)
- [Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information \(ITSM.10.189\)](#)

CONSEILS POUR LES RESPONSABLES DE LA MISE EN ŒUVRE DES TI



- [Directives de mise en œuvre - protection du domaine de courrier \(ITSP.40.065\)](#)
- [Rapport du centre pour la cybersécurité sur la virtualisation des centres de données : pratiques exemplaires en matière de virtualisation des centres de données \(ITSP.70.010\)](#)
- [Étapes pour gérer les fuites de données dans le nuage \(ITSAP.50.112\)](#)
- [Conseils de sécurité pour les organisations dont les employés travaillent à distance \(ITSAP.10.016\)](#)
- [Utiliser un poste de travail virtuel à la maison et au bureau \(ITSAP.70.111\)](#)
- [Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles \(ITSAP.70.002\)](#)
- [Protéger son organisation contre les attaques par déni de service \(ITSAP.80.100\)](#)

SENSIBILISATION DE LA CLIENTÈLE



- [Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage](#)
- [Pratiques exemplaires en cybersécurité pour la COVID-19](#)
- [Vidéoconférence \(ITSAP.10.216\)](#)
- [Application des mises à jour sur les dispositifs \(ITSAP.10.096\)](#)
- [Sécurisez vos comptes et vos appareils avec une authentification multifacteur \(ITSAP.30.030\)](#)
- [Protéger l'organisme contre les maliciels \(ITSAP.00.057\)](#)
- [Les réseaux privés virtuels \(ITSAP.80.101\)](#)
- [Rançongiciels : Comment les prévenir et s'en remettre \(ITSAP.00.099\)](#)
- [Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques \(ITSAP.30.036\)](#)
- [Pratiques exemplaires de création de phrases de passe et de mots de passe \(ITSAP.30.032\)](#)
- [Utiliser la technologie Bluetooth \(ITSAP.00.011\)](#)
- [Reconnaître les courriels malveillants \(ITSAP.00.100\)](#)

RENSEIGNEMENTS SUPPLÉMENTAIRES



- [Fils RSS](#)
- [Alertes et avis](#)
- [Passation de marché avec des fournisseurs de services gérés](#)
- [Bouclier canadien—Le Centre pour la cybersécurité fournit du renseignement sur les menaces afin de protéger les Canadiens pendant la pandémie de COVID-19](#)



Les modèles traditionnels des environnements de travail au bureau et à domicile ont été complètement inversés.

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

