Hygiène de cybersécurité pendant la pandémie de COVID-19

Ce qu'il faut faire et ne pas faire : un guide à partager avec vos employés

La menace

Comme si la situation actuelle n'était pas assez difficile, les auteurs de cybermenaces profitent de la pandémie actuelle de COVID-19 en exploitant les craintes et les incertitudes des gens. Tous les centres de sécurité des gouvernements et de l'industrie constatent une hausse importante des activités malicieuses liées à la pandémie de COVID-19.

Plusieurs de ces activités sont des attaques d'hameçonnage où des sites illicites imitent des sites officiels. Les courriels malicieux peuvent utiliser des adresses de courriel d'expéditeur frauduleuses qui pastichent des adresses légitimes et comprendre des liens qui semblent vous diriger vers des sources faisant autorité (US Center for Disease Control, Mayo Clinic, Organisation mondiale de la santé, etc.).

Si un utilisateur imprudent clique sur ces liens ou ouvre une pièce jointe contenant un logiciel malveillant (vers, chevaux de Troie, « rootkits », enregistreurs de frappe, logiciels de rançon, etc.), l'infection peut se produire rapidement.

CIRCONSTANCES POUR LES UTILISATEURS

De nombreuses organisations demandent à leurs employés de faire du télétravail. Cela peut intensifier le risque étant donné que les systèmes de sécurité d'entreprise ne sont pas toujours mis à la disposition des télétravailleurs. Certains télétravailleurs pourraient même avoir à utiliser des systèmes personnels qui n'ont pas le même niveau de protection que les systèmes d'extrémité du bureau.

Trucs pour les utilisateurs

Quelles que soient les circonstances dans lesquelles vous travaillez, vous devez être particulièrement vigilants à l'égard des attaques malicieuses qui tentent d'exploiter la pandémie et les craintes qu'elle suscite chez les gens. Cela s'applique que vous travailliez au bureau ou à domicile.

DES SIGNES À SURVEILLER

Il n'y a pas de signes sûrs qui permettent aux utilisateurs (sauf peut-être les analystes en sécurité) de détecter toutes les attaques. Portez cependant attention aux éléments suivants qui devraient être considérés comme suspects :

- **courriels inattendus ou non sollicités :** méfiez-vous des courriels que vous **ne vous attendiez pas à recevoir**, même s'ils proviennent d'un ami (son adresse de courriel pourrait avoir été prise dans les médias sociaux et pastichée) ou d'un organisme qui semble faire autorité;
- **courriels qui créent un sentiment d'urgence**, tout spécialement ceux qui annoncent de nouvelles informations sur la pandémie et qui vous demandent de cliquer sur un lien ou de fournir des renseignements personnels pour ne rien manquer de soi-disant prochaines annonces;
- **courriels qui commencent par une salutation bizarre ou inhabituelle** par exemple Cher Monsieur/Madame;
- **adresses de courriel étranges** qui ne semblent pas assez « professionnelles » ou qui contiennent des fautes. On a déjà vu par exemple un courriel qui prétendait venir d'une agence fédérale américaine, mais qui utilisait une adresse aol.com;
- **fautes d'orthographe ou erreurs grammaticales;** méfiez-vous si le texte est bizarrement formulé;
- **pièces jointes :** la règle est simple : **n'ouvrez pas** une pièce jointe que vous ne vous attendiez pas à recevoir. Dans le doute, si l'expéditeur est un ami ou un collègue, communiquez avec lui pour vous assurer que la pièce jointe vous est bel et bien destinée **avant de l'ouvrir**;
- **liens intégrés :** méfiez-vous des liens. Faites passer votre souris sur le lien pour voir si l'adresse « annoncée » correspond au lien fourni. Mieux encore : rendez-vous sur le site Web officiel de l'organisme mentionné sans cliquer sur le lien fourni dans le courriel. Certains sites malicieux affichent des messages du genre « ERREUR 404 – SITE WEB INTROUVABLE » lorsque les utilisateurs cliquent sur un lien intégré; méfiez-vous, malgré ce message apparemment rassurant, votre sécurité pourrait quand même être déjà compromise.

TÉLÉTRAVAIL

Plusieurs personnes doivent travailler de leur domicile, ce qui comporte de nouveaux risques comme nous l'avons vu précédemment. Voici quelques conseils d'« hygiène » pour réduire ces risques :

- **utilisez préférablement l'ordinateur portable fourni par votre employeur :** il est probablement doté de systèmes de sécurité plus robustes que votre ordinateur personnel;
- si possible, **utilisez un accès à distance sécurisé et approuvé** pour vous connecter à votre environnement de travail : la plupart de ces connexions comprennent une session RPV (réseau privé virtuel) point à point chiffrée;
- **assurez-vous que votre ordinateur est à jour :** assurez-vous que toutes les mises à jour logicielles et de sécurité et tous les correctifs ont été appliqués et que votre système de protection contre les programmes malveillants est à jour et contient les plus récents fichiers DAT;
- **ne désactivez pas les systèmes de sécurité** comme les systèmes de protection contre les programmes malveillants et les coupe-feu qui protègent les points d'extrémité;

- **Ne naviguez pas sur le Web pour des motifs personnels** lorsque votre session d'accès à distance est ouverte : si vous visitez un site Web malicieux lorsque votre connexion d'accès à distance est ouverte, votre ordinateur pourrait être utilisé comme un pont pour infecter le réseau de votre organisation;
- **ordinateurs laissés sans surveillance :** si vous devez vous éloigner de votre ordinateur, fermez la connexion d'accès à distance, puis éteignez ou verrouillez votre écran au moyen d'un mot de passe;
- **évitez d'utiliser un Wi-Fi public** ou de travailler dans des **lieux publics**.

UTILISEZ DES SITES DE CONFIANCE

Plusieurs sites Internet propagent des informations erronées ou trompeuses au sujet de la COVID-19. Nous vous recommandons fortement de ne vous fier qu'aux informations des organismes suivants en consultant leurs sites officiels :

- Organisation mondiale de la santé : www.who.int/fr ou www.who.int
- Santé Canada : https://www.canada.ca/fr/sante-canada.html ou https://www.canada.ca/en/health-canada.html
- Votre autorité provinciale en matière de santé
- Votre autorité municipale ou régionale en matière de santé

SIGNES DE COMPROMISSION

Si le pirate est doué, il ne laissera aucune trace de son passage. Voici cependant des symptômes courants que vous pourriez observer :

- des fenêtres contextuelles s'ouvrent dans votre système alors qu'il n'y en avait pas avant;
- la page d'accueil de votre navigateur n'est plus la même;
- le système et des applications ne fonctionnent pas comme d'habitude (p. ex., une page, une application ou un système plante);
- votre ordinateur est plus lent;
- des programmes inconnus sont en fonction dans votre système;
- le système de protection contre les programmes malveillants est désactivé;
- certains de vos mots de passe ont été changés ou vous recevez des demandes non sollicitées de changement ou de validation de mot de passe.

ACTIONS IMMÉDIATES EN CAS DE COMPROMISSION

Si vous croyez que votre ordinateur est compromis, prenez **immédiatement** les mesures suivantes :

- mettez fin à toute session d'accès à distance;
- déconnectez votre ordinateur de toute connexion par câble ou Wi-Fi;
- éteignez votre ordinateur;
- communiquez avec le centre d'assistance en sécurité de votre organisation et suivez ses directives.

CONCLUSION

Un effet secondaire de la pandémie de COVID-19, surtout pour les télétravailleurs, est l'augmentation des menaces de cybersécurité. Vous pouvez réduire cette menace en étant conscient de la situation et mettant en application les lignes directrices présentées dans ce guide. Pour en savoir davantage concernant la menace pour la cybersécurité que représente la pandémie de COVID-19, consultez le site Web officiel du Centre canadien pour la cybersécurité.

Pour toute question concernant la cybersécurité, écrivez à **globalcybersecurity@cgi.com.**