CYBER READINESS
INSTITUTE

Sécuriser la main-d'œuvre à distance

Les prochains mois offriront des défis à partout dans le monde car les routines sont perturbées par le coronavirus. Les enfants et les enseignants devront collaborer à distance, les travailleurs feront leur travail depuis leur domicile et les propriétaires d'entreprises dirigeront leur société depuis leur salon, plutôt que depuis la salle du conseil.

Nous avons la chance que les technologies d'aujourd'hui permettent à nombre d'entre nous de poursuivre notre travail avec peu de perturbations. La disponibilité d'une puissance de calcul peu coûteuse, l'accès aux services cloud et des connexions Internet à haut débit font du télétravail une alternative viable qui pourrait contribuer à ralentir cette crise sanitaire.

Mais alors que de plus en plus de personnes font du télétravail, nous devons être conscients que nous sommes exposés à d'autres risques. Alors que de nombreux emplois vont s'exercer à distance, nous devons tous faire preuve d'une grande vigilance en matière de bonnes pratiques de cyber-hygiène.

Voici quelques mesures essentielles que nous pouvons tous prendre pour protéger notre sécurité en ligne.

Alors que de nombreux emplois vont s'exercer à distance, **nous devons tous faire preuve d'une grande vigilance en matière de bonnes pratiques de cyber-hygiène.**

L'essentiel

Mots de passe

Les mots de passe restent la première ligne défense pour accéder aux données et aux applications critiques. Le télétravail augmente la complexité car il faut se fier à la sécurité du réseau domestique de chaque employé.

- Veillez à ce que le mot de passe du routeur domestique ne soit pas facile à deviner et ne comprenne pas votre adresse ou vos noms personnels.
- Dès que possible, activer l'authentification multiple (mot de passe + une autre exigence telle qu'un message textuel), y compris pour l'accès aux données critiques dans les applications de cloud utilisées pour le partage de données et de documents.

Correctifs de sécurité

Les correctifs de sécurité du système d'exploitation doivent être acceptés et rester à jour.

- Exiger des employés que leurs systèmes d'exploitation soient réglés sur une mise à jour automatique.
- Rappelez aux employés - chaque semaine - d'accepter tous les correctifs de sécurité pertinents.

Hameçonnage

Plus nous serons nombreux à être en ligne dans les semaines à venir, plus nous pouvons nous attendre à une augmentation des escroqueries en ligne, le piratage psychologique et les attaques d'hameçonnage (*phishing* en anglais). Les pirates et les criminels ne manqueront pas d'utiliser les inquiétudes concernant la propagation du virus et le désir insatiable d'obtenir des informations pour tromper les gens. .

- Passez toujours la "souris" sur le nom de l'expéditeur du courriel pour déterminer la véritable origine de l'expéditeur. Assurez-vous que le nom de l'expéditeur ne soit pas frauduleux
- La plupart des courriels de demande de rançon individuelle sont des faux. Si vous le pouvez, assurez-vous de vérifier ces courriels par un professionnel de la sécurité avant de répondre.
- Chaque entreprise doit identifier un point de contact au sein de l'entreprise que chaque employé doit contacter lorsqu'il reçoit un courriel d'hameçonnage ou un logiciel de rançon individuel. Cette sensibilisation et cette communication permettront d'informer les employés au sujet des tactiques actuelles des acteurs malveillants.

La distanciation sociale

La distanciation sociale fonctionne aussi en ligne.

- Limiter la quantité de données personnelles que vous partagez sur les médias sociaux afin de réduire vos failles de protection.
- Partager toutes les données via des applications de cloud en ligne sécurisées. Les clé USB ne doivent pas être utilisées pour partager des données car elles peuvent propager des logiciels malveillants.