NPC Smarter Computing™

Couches de sécurité essentielles pour protéger vos données

Que vous travailliez toujours à distance ou que vous retourniez au bureau, il est important de rappeler que votre environnement a une grande incidence sur votre état de préparation en matière de cybersécurité. Il existe des couches de sécurité à considérer quand nous travaillons à distance, qui sont différentes de celles mises en place au bureau, et vice versa. Il faut donc savoir s'adapter les principes de base suivants pour toutes situations. Séparément, chacune de ces couches est importante et améliore la sécurité à sa manière, mais une fois superposées, elles favorisent un environnement sécurisé optimal.

Utiliser un réseau Wi-Fi sécurisé

Au-delà de votre environnement de travail se trouve votre connexion avec le reste du monde. Il est important de sécuriser votre connexion Wi-Fi en changeant le mot de passe par défaut et en vous assurant d'activer au moins une clé avec chiffrement WPA2. Veuillez aussi activer le pare-feu et désactiver les fonctions UPnP et WPS de votre routeur une fois qu'ils sont configurés.

Votre modem, votre routeur et vos appareils de l'Internet des objets (IdO) ont également leurs propres mesures de sécurité; modifiez donc les mots de passe par défaut et effectuez toujours les mises à jour du micrologiciel, car elles peuvent comporter des correctifs de sécurité.

Comme vous ne pouvez pas garantir la sécurité des réseaux Wi-Fi gratuits ou publics, pour minimiser les risques, évitez tout simplement de travailler sur ces réseaux. Quand vous naviguez sur Internet en déplacement, utilisez un ordinateur avec connectivité mobile ou le réseau de votre téléphone pour assurer une connexion chiffrée.

Sécuriser vos appareils informatiques

La couche de sécurité suivante concerne votre ordinateur qui recueille et traite vos données. Si votre ordinateur est compromis, il agira comme passerelle par laquelle d'autres atteintes à la sécurité seront possibles. Les ordinateurs ont leur propre ensemble de mesures de sécurité avec des composants matériels et logiciels qui fonctionnent de manière interdépendante.

Les outils de sécurité obsolètes peuvent ne pas être équipés pour gérer les menaces actuelles; il est donc important d'investir dans des technologies à jour, en particulier des technologies conçues pour la détection des menaces comme une suite de logiciels malveillants. Il est également important d'effectuer les mises à jour logicielles de votre système d'exploitation, de votre BIOS, de vos applications et de tout appareil de l'IdO à mesure qu'elles sont offertes. Ces mises à jour comprennent des correctifs de sécurité qui aident à corriger les failles et à protéger vos appareils contre de nouvelles menaces.

Opter pour la collaboration et le partage de fichiers sécurisés

Plus une couche de cybersécurité se rapproche de vos données, plus il faut exercer une vigilance accrue pour assurer leur sécurité. Étant donné que les activités commerciales se font de plus en plus en ligne, il

est important de savoir que, par défaut, les courriels ne sont pas cryptés, ce qui les rend. L'élimination du courriel comme moyen de transférer des fichiers est une bonne pratique à adopter qui facilitera l'identification des documents malveillants envoyés par des auteurs de menaces.

Utilisez plutôt un service de stockage infonuagique sécurisé et réputé pour accéder à vos fichiers et n'accordez l'accès qu'aux personnes qui en ont besoin. De cette façon, les collègues peuvent facilement collaborer sur des documents et les clients peuvent être invités à les consulter en ligne en toute sécurité. Si moins de personnes s'envoient moins de fichiers en va-et-vient, l'angle d'attaque sera restreint, ce qui vous rendra, vous et vos clients, moins vulnérables.

Rendre les mots de passe longs et forts

Nous avons abordé en détail la sécurité des mots de passe dans notre dernier bulletin, mais nous devons réitérer l'importance des phrases passe longues. Le temps que ça prend pour déchiffrer un mot de passe augmente de façon exponentielle à chaque caractère ajouté, de sorte que nous recommandons des mots de passe d'au moins 14 caractères. Collez plusieurs mots ensemble pour créer une phrase passe qui sera plus facile à retenir et à taper plutôt qu'une chaîne de caractères complexes.

Assurez-vous d'activer l'authentification multifacteur (MFA) dans la mesure du possible pour ajouter une deuxième couche de sécurité à vos comptes. Il s'agit certainement de la meilleure protection contre une atteinte à la sécurité d'un compte en ligne.

Sauvegarder vos données

La sauvegarde est votre meilleure protection en cas d'échec de sécurité, et elle vous aidera à protéger ou à récupérer votre contenu plus facilement si le pire devait se produire. Votre processus de sauvegarde doit être sécurisé et exécuté automatiquement, permettre de stocker les données à distance et de créer des redondances, en plus de pouvoir être facilement restauré en cas de perte, de vol, d'incendie, de défaillance mécanique, d'erreur humaine, de virus, de logiciel malveillant, etc.

Il existe des services infonuagiques conçus pour faciliter la sauvegarde de vos données et la rendre sécurisée, mais assurez-vous de choisir une entreprise digne de confiance avant de leur confier vos données. Soyez au courant des exigences de conformité réglementaire en matière de et veillez à ce qu'elles soient respectées ou surpassées par votre fournisseur de services de sauvegarde.

Voilà quelques exemples de couches de sécurité à mettre en place pour mieux protéger vos données, et elles nécessitent des vérifications régulières pour maintenir leur efficacité. Joignez-vous au prochain webinaire sur les pratiques informatiques sécuritaires de NPC intitulé *Five-Step Checkup for Your Cyber Protection [en anglais seulement]*, pour en apprendre davantage sur les couches de sécurité essentielles et les façons d'adopter des pratiques exemplaires en matière de cybersécurité – inscrivez-vous ici.

NPC

NPC DataGuard, une division de Compugen Inc.
1 855 667-2642
info@npcdataguard.com
www.npcdataguard.com