Le télétravail:

Sept mesures simples pour assurer votre sécurité et celle de votre lieu de travail sur Internet

Août 2022

Où que vous soyez dans le monde, vous avez probablement été affecté, d'une manière ou d'une autre, par la COVID-19. La pandémie a renvoyé chez eux les salariés comme les étudiants, a conduit à annuler les événements sociaux tels que les remises de diplôme et les mariages, et a mis en danger un nombre très important de personnes, en particulier les personnes âgées ou immunodéprimées.

Du fait des restrictions imposées dans le cadre de la COVID-19, de nombreux employeurs ont demandé à leurs employés de travailler depuis chez eux. Si vous avez la chance de disposer de cette possibilité, il est important de veiller à ne pas vous exposer, ou exposer votre entreprise, à des risques plus importants sur le plan du numérique. Les attaques par hameçonnage et rançongiciels augmentent avec la propagation de la COVID-19. Cloudfare a indiqué que le nombre de cyberattaques avait bondi de 37 % au Royaume-Uni en mars 2020.

Il ne vous viendrait pas à l'idée de demander à un médecin ou un(e) infirmier/infirmière de travailler sans équipements de protection individuelle. Vous-même ne devriez pas le faire non plus.

Équipez-vous: suivez ces conseils simples pour sécuriser le travail que vous effectuez depuis chez vous sur le réseau de votre domicile.

1. Ne gardez pas vos assistants intelligents dans la pièce où vous travaillez.

Les assistants intelligents sont en permanence à l'écoute, en attendant d'entendre un mot de « réveil ». Par exemple, votre Amazon Echo commencera à prêter attention aux sons s'il entend « Alexa ». De ce fait, les assistants intelligents peuvent accidentellement écouter des conversations relatives à des travaux confidentiels durant une visioconférence ou un appel vocal.

Pour éviter cela, il vous suffit d'éteindre votre assistant intelligent, ou de le ranger dans une autre pièce lors de vos conversations professionnelles. Vous n'aurez de toute façon pas besoin qu'il lance

une chanson, mette à jour votre liste de courses ou réponde à une de vos questions pendant vos appels. Si vous souhaitez tout de même le garder près de vous, assurez-vous de désactiver le mode écoute ou de le débrancher durant vos conversations. Si vous tenez accidentellement une conversation professionnelle à proximité d'un assistant intelligent, vous pourrez peut-être supprimer l'enregistrement manuellement. Par exemple, vous pouvez supprimer les fichiers audio enregistrés de Siri dans les « Paramètres » d'un appareil Apple et supprimer les enregistrements des appareils Google Home. Notez que le fournisseur de services peut toujours conserver une copie des enregistrements même si l'utilisateur les a supprimés de son compte, et cela peut ou non être évident pour l'utilisateur. Ainsi, il est préférable de pécher par excès de prudence et de désactiver les appareils pendant les appels professionnels comme décrit ci-dessus.

2. Utilisez des mots de passe uniques et un gestionnaire de mots de passe.

Il peut sembler pratique d'utiliser le même mot de passe pour tout ce qui touche au travail, mais cela présente, pour votre espace de travail, un plus grand risque de piratage de compte et de vol de données. Si quelqu'un découvre votre mot de passe, il peut facilement accéder à tous vos systèmes de travail, et compromettra à la fois vos données et celles de votre employeur.

Puisqu'il est difficile de retenir des mots de passe uniques pour chaque système lié au travail, un gestionnaire de mots de passe peut s'avérer utile. Ce type de logiciels vous permet d'enregistrer au même endroit tous vos mots de passe uniques, et comprend souvent une fonctionnalité d'entrée automatique de vos mots de passe lorsque vous vous connectez à vos différents comptes. Grâce à cette solution, il vous suffit de vous rappeler du mot de passe global pour pouvoir accéder à tous vos comptes. De nombreux sites et plateformes prodiguent des conseils sur le choix du gestionnaire de mots de passe qui correspond à vos besoins. Vous trouverez quelques ressources ici, ici et ici.

Cryptage de bout en bout (E2E) Ce type de cryptage est très sécurisé, et garantit que seuls l'expéditeur et le destinataire prévu peuvent lire les messages et les informations. Grâce au cryptage E2E, même le service de communication ne peut pas accéder aux informations.

3. Mettez en place une authentification à deux facteurs partout où cela est possible.

Les mots de passe uniques et les gestionnaires de mots de passe sont utiles et importants, mais vous devez aller encore plus loin pour sécuriser vos systèmes de travail. Si vous souhaitez améliorer encore la sécurité de vos mots de passe, cherchez à savoir si vos systèmes de travail permettent l'authentification à deux facteurs.

Il existe plusieurs types d'authentification à deux facteurs. Il est par exemple possible de recevoir un code par SMS ou par courriel lorsque vous vous connectez à votre système de travail. N'oubliez pas que cette méthode n'est pas complètement sécurisée, car les SMS et les courriels ne sont pas toujours cryptés. Si vous n'avez d'autre choix que l'envoi d'un SMS, il est important de protéger votre numéro de téléphone portable contre une attaque par échange de carte SIM. Certains

opérateurs de téléphonie mobile permettent aux utilisateurs d'activer un code PIN ou un mot de passe secret afin d'éviter de telles attaques.

Mieux vaudrait utiliser une application d'authentification, qui peut vous autoriser à ouvrir l'application pour prouver que c'est bien vous qui vous connectez, ou générer des codes différents pour vous, que vous devrez entrer à chacune de vos connexions au système. Ces codes ont souvent une durée limitée, afin que, même si un attaquant y accédait depuis vos courriels ou vos SMS, il ne puisse pas les réutiliser par la suite.

Il existe une option encore plus sûre: l'utilisation d'un jeton d'authentification physique (ex.: Yubikey). Il s'agit d'une petite clé USB, que vous pouvez accrocher à votre porte-clés, et que vous utilisez pour vous connecter à un service prenant cette option en charge.

4. Choisissez des services en ligne offrant un cryptage robuste.

Le cryptage est la meilleure façon d'assurer la sécurité de vos données si vous télétravaillez. Il s'agit de l'un des outils les plus robustes dont disposent les systèmes connectés pour protéger les informations sur l'utilisateur, les données et les systèmes informatiques. Si vous utilisez des systèmes qui ne sont pas protégés par un cryptage robuste, vos propres données, de même que les informations de votre employeur, sont davantage exposées à un risque de piratage.

> Les systèmes à cryptage robuste rendent plus difficile l'accès par des tiers à vos communications, veillent à ce que vos données ne soient pas lisibles, même si quelqu'un parvient à y accéder, et contribuent à empêcher la modification des informations par un attaquant.

Consultez les déclarations relatives à la confidentialité et à la sécurité (c'est-à-dire les « politiques ») de vos systèmes de travail, anciens comme nouveaux, pour savoir lesquels d'entre eux disposent d'un système automatique de cryptage des communications et données. Vous pouvez également effectuer une simple recherche sur Internet pour savoir si des services spécifiques utilisent le cryptage et ce qu'ils cryptent, mais, comme pour toute recherche, assurez-vous que vous consultez des ressources fiables et à jour. Le cryptage de bout en bout offre le meilleur niveau de sécurité pour les communications, et vous devez donc vous assurer qu'il est mis en place avant d'utiliser un nouveau logiciel. Parfois, les applications n'activent pas automatiquement le cryptage, vous devez donc veiller à pouvoir l'activer vous-même. Assurez-vous que votre smartphone, votre tablette, votre ordinateur portable et tout autre objet connecté que vous utilisez sont cryptés et protégés par un mot de passe robuste dès que cela est possible.

5. Utilisez un VPN, même pour votre réseau domestique.

Lorsque vous vous connectez au réseau de votre employeur depuis votre bureau, vous ne pensez pas forcément à vous assurer que la connexion est sécurisée. Il est possible que votre entreprise fasse une partie de ce travail pour vous, grâce à un Intranet accessible depuis un portail sécurisé. Mais, lorsque vous travaillez à distance, assurez-vous que vous protégez bien la totalité de votre trafic. Un réseau privé virtuel (VPN) peut être un outil approprié.

Certains employeurs peuvent intégrer automatiquement un VPN aux ordinateurs de travail que les employés amènent chez eux. Si vous travaillez sur un ordinateur personnel ou un ordinateur de votre entreprise qui ne dispose pas encore d'un VPN, renseignez-vous sur la meilleure façon d'en choisir et d'en télécharger un pour sécuriser vos activités sur Internet sur vos systèmes de travail. Mais méfiez-vous des VPN « gratuits »: s'ils ne facturent pas leurs utilisateurs, il est possible qu'ils gagnent leur argent en vendant vos données personnelles - qui peuvent inclure votre historique de navigation.

6. Mettez vos logiciels à jour.

Il est facile de cliquer sur « Me le rappeler plus tard » lorsqu'un logiciel vous envoie une notification de mise à jour requise, mais, bien souvent, les mises à jour ne sont pas uniquement constituées de nouvelles fonctionnalités. Elles comportent également des correctifs pour des bugs et des failles de sécurité. Vous pouvez améliorer de manière substantielle la sécurité de votre ordinateur et de vos données en effectuant les mises à jour de logiciel. Cela améliorera également la sécurité du réseau de votre employeur.

Il est souvent plus facile de mettre vos logiciels à jour en télétravaillant. Vous pouvez ainsi mettre à jour vos logiciels en vous préparant le matin, ou pendant votre pause déjeuner, ou à la fin de votre journée de travail.

7. Sauvegardez vos fichiers.

Tout le monde peut être victime d'une attaque par ransomware. Lors d'une attaque de ce type, un criminel bloque l'accès aux données, systèmes et informations enregistrées, et prend ces informations en otage jusqu'au versement d'une rançon par la victime. Même si votre lieu de travail devrait toujours sauvegarder les fichiers, vous devez être très vigilant à la sécurisation de vos fichiers lorsque vous travaillez de chez vous.

Commencez par demander à votre employeur des informations sur la façon de sauvegarder vos fichiers en télétravail. Cela peut être effectué avec un service de cloud et/ou un support de stockage externe. Veillez à bien déconnecter le support qui contient vos fichiers de sauvegarde lorsqu'il ne sert pas, afin de pouvoir y accéder même si vos fichiers d'origine sont compromis. La sauvegarde devrait être cryptée et protégée par un mot de passe.

Vous trouverez plus d'informations sur la sécurisation de votre espace de travail en consultant notre Fiche d'information avec Next Century Cities.

Pour plus d'informations sur le rôle critique que joue le cryptage dans la sécurisation de nos activités quotidiennes, rendez-vous sur https://www.internetsociety.org/fr/action-plan/2022/encryption/