CYBER READINESS INSTITUTE

Préparer vos employés au télétravail

Bien que la technologie permette aux gens de travailler à distance, elle ouvre également la porte à de nouveaux risques en matière de cybersécurité et de protection des données

Aujourd'hui plus que jamais, chaque organisation doit désigner un responsable de la préparation au télétravail, c'est-à-dire une personne qui guidera vos employés. Pour en savoir plus sur notre programme gratuit de préparation au télétravail et le rôle de responsable Cyber, veuillez consulter notre site web (www.cyberreadinessinstitute.org).

Voici trois domaines clés que les responsables doivent prendre en considération préparer leurs employés à la sécurité en ligne :

- Quels dispositifs utilisera le personnel pour se connecter et accéder l'information ?
- Comment se connectera-il pour accéder à l'information ?
- Comment va-il accéder, gérer et protéger le l'information ?

Dispositifs

Si les employés utilisent un appareil fourni par l'entreprise depuis leur domicile :

- Rappelez aux employés de respecter votre politique de mise à jour des logiciels et de mots de passe/ phrases de passe

Si les employés utilisent des appareils personnels :

- Aillez des mots de passe/phrases de passe différents pour le travail et l'usage personnel
- Installez et exécutez un logiciel de détection de virus
- Mettez à jour tous les logiciels avant de vous connecter au réseau de l'organisation
- Activez les mise à jour automatique pour tous les logiciels
- Activez l'authentification multifactorielle chaque fois qu'elle est offerte

Si les employés utilisent des appareils personnels partagés (avec un conjoint, des enfants, etc.) :

- Fermez et quittez toutes les applications à la fin de chaque session de travail
- Déconnectez-vous, fermez et quittez les bases de données ou les navigateurs web
- Ne notez pas les mots de passe/phrases de passe sur ou à proximité de l'ordinateur
- Ne stockez pas les mots de passe/ phrases de passe dans l'appareil et n'utilisez l'identification automatique

Si les employés utilisent des ordinateurs publics (comme un parc, des bibliothèques, des cafés, etc. - s'ils sont ouverts)

- Cette utilisation doit être fortement découragée et ne doit se faire que si elle est essentielle
- Quittez et rouvrez toute applications qui étaient déjà ouvertes
- Utilisez la navigation privée sur le navigateur web si possible
- Fermez et quittez toutes les applications, y compris celles des navigateurs, à la fin de chaque session de travail
- Ne jamais enregistrer de documents sur l'ordinateur public
- Si vous utilisez une clé USB, ce qui est fortement déconseillé, ne jamais la mettre dans un ordinateur public

Connexions

Si les employés utilisent une connexion Wi-Fi personnelle depuis leur domicile :

- Modifier le mot de passe/la phrase de passe Wi-Fi existant avant de commencer le télétravail

Si les employés utilisent une borne Wi-Fi personnel ou fournie par l'entreprise

- Utilisez toujours la borne Wi-Fi plutôt que le Wi-Fi public

Si les employés utilisent un Wi-Fi public :

- En général, les employés doivent éviter d'utiliser des Wi-Fi public à moins que votre organisation ne dispose d'un réseau privé virtuel (VPN) que les employés savent utiliser

Accès et Gestion des données

Indiquez les systèmes et les données auxquels chaque employé peut accéder dans le cadre de ses activités normales.

Faudra-t-il modifier ce à quoi ils peuvent accéder lorsqu'ils travaillent à distance ?

En ce qui concerne l'utilisation des clés USB, il est préférable de les interdire et de prévoir le partage de fichiers par un cloud pour transférer, partager et stocker des données :

- Si votre organisation a une politique de "non USB", rappelez et soulignez l'importance de suivre cette politique tout en travaillant à distance
- Si votre organisation autorise l'utilisation de clés USB (ce n'est pas une bonne idée), fournissez à chaque employé une clé USB ayant été analysé pour détecter les logiciels malveillants. Dites à vos employés qu'ils peuvent l'utiliser uniquement sur l'ordinateur qu'ils utiliseront pour travailler à distance ET de s'assurer qu'ils disposent d'un anti-virus sur l'ordinateur AVANT d'insérer la clé USB

Le partage et la sauvegarde du travail pour les travailleurs à distance peuvent soulever de nouveaux défis.

- Si votre organisation a utilisé un partage de fichiers centralisé (OneDrive, Google Drive, i-Cloud, Box, Drop Box, etc.), les employés seront habitués à gérer la façon dont ils collaborent pour travailler sur des documents
- Si ce n'est pas le cas, vous devez établir des lignes directrices sur la manière dont vos employés gèrent et partagent les documents :
  - Idéalement, vous devriez créer un site de partage de fichiers
  - En attendant, demandez à vos employés d'envoyer leur documents par courriel en tant que pièces jointes cryptées. De nombreuses applications de courrier électronique (Outlook, Gmail, Apple Mail, etc.) permettent de crypter les pièces jointes. Il existe des programmes complémentaires qui fournissent l'encryptage des courriers électroniques et des pièces jointes (Virtu, Tutanota, VMware Boxer, Symantec Bureau, etc.)
  - Vos conseils doivent porter sur la dénomination des documents ainsi que les bases du contrôle des versions. Si les employés enregistrent des documents de travail sur un dispositif personnel, vous avez besoin d'un moyen d'éviter d'avoir plusieurs versions du même document

Nous nous sommes engagés à être une ressource clé pour aider les PME à trouver un équilibre entre le travail à distance et la cybersécurité. N'hésitez pas à nous contacter pour des questions, des commentaires ou des exemples de réussite (support@cyberreadinessinstitute.org).

À propos du Cyber Readiness Institute

Le Cyber Readiness Institute est une initiative à but non lucratif qui réunit des chefs d'entreprise de tous les secteurs et de toutes les régions géographiques afin de partager des ressources et des connaissances au sujet du développement d'outils de cybersécurité gratuits pour les petites et moyennes entreprises (PME).

Le programme autodidacte Cyber Readiness est disponible en ligne en chinois, anglais, français, espagnol, portugais, arabe et japonais.

Pour en savoir plus, consultez le site visit www.becyberready.com.