CRÉER UNE ORGANISATION DE TRAVAIL À DISTANCE SÉCURISÉE

Alors qu'un tiers des décideurs informatiques ont admis que leur organisation avait subi une violation des données en raison du travail à distance[1], comment vous assurez-vous que les données de votre entreprise restent protégées pendant cette période d'activité aussi inhabituelle ?

01.

Sécurisez votre stratégie de télétravail

Un réseau de bureau à domicile est **3,5 fois plus susceptible** d'être infecté par des programmes malveillants qu'un réseau d'entreprise[2]

Les cybercriminels **savent** si vous êtes un utilisateur à domicile ou un utilisateur professionnel travaillant à domicile

Protégez vos collaborateurs avec une **politique de télétravail sécurisée** et évitez la perte potentielle de données ou le vol de vos propres fichiers avec restitution contre rançon

02.

Méfiez-vous des attaques par phishing

Les e-mails de phishing liés à la pandémie de Covid-19 représentent désormais la méthode d'**attaque** la plus utilisée[3]

Les fraudes ont augmenté de plus de **400 %** rien qu'au Royaume-Uni en février et mars[4], les victimes ayant perdu collectivement plus de 1,6 million de livres sterling[5]

Assurez-vous que vos collaborateurs **connaissent l'identité de l'expéditeur avant d'ouvrir un e-mail**. Ils devraient également y réfléchir à deux fois avant de cliquer sur des liens inconnus

03.

N'oubliez pas la sécurité des appareils domestiques

Votre équipe utilisera l'imprimante ou le scanner dont elle dispose à domicile

Ces appareils **ne disposent probablement pas des fonctions de sécurité standard** fournies par l'équipement de votre réseau d'entreprise

Avec plus de **25 %** de tous les appareils disposant d'un ou plusieurs services exposés sur Internet6, ils sont plus vulnérables aux attaques

Pour protéger les données critiques de votre entreprise, aidez vos employés à s'assurer que leur réseau est privé et accessible uniquement à l'aide d'un mot de passe **sécurisé,** autre que celui par défaut

04.

Et les documents confidentiels

Assurez-vous que vos télétravailleurs traitent les documents de l'entreprise avec le même soin que leurs propres relevés bancaires, en vous assurant qu'ils **détruisent ou stockent en toute sécurité** tout document confidentiel jusqu'à leur retour au bureau

05.

La meilleure politique est d'en avoir une

Travailler de chez soi **ne signifie pas** que les politiques de l'entreprise peuvent être assoupies

Rappelez à votre équipe d'utiliser exclusivement les applications, réseaux et sites Cloud **fournis par l'entreprise**

Les outils gratuits de collaboration et de stockage dans le Cloud qu'ils peuvent être tentés d'utiliser **ne seront peut-être pas sécurisés** si vous ne les avez pas approuvés

Si certains de vos collaborateurs travaillent à distance, vous devez vérifier qu'ils ont parfaitement compris comment assurer le même niveau de sécurité professionnelle, qu'ils soient au bureau ou sur leur canapé.

Contactez Canon pour savoir comment vous pouvez non seulement survivre, mais également prospérer dans une période d'activité aussi inhabituelle.

Canon

Élargissez vos perspectives

1 https://www.techrepublic.com/article/security-of-remote-workers/
2 https://www.techrepublic.com/article/security-of-remote-workers/
3 https://www.ncsc.gov.uk/news/phishing-attacks-exploiting-fear-of-covid-19
4 https://www.ncsc.gov.uk/news/phishing-attacks-exploiting-fear-of-covid-19
5 https://www.ukfinance.org.uk/news/press-releases/fraudsters-exploit-coronavirus-pandemic-to-target-vulnerable-people
6 https://www.ncsc.gov.uk/guidance/bring-your-own-device-for-home-and-small-offices-guidance