CYBER READINESS
INSTITUTE

Les trois choses à faire et à ne pas faire pour les employés à distance

Les criminels informatiques utilisent la pandémie COVID-19 pour abuser des employés travaillant à distance en leur volant leurs informations personnelles et professionnelles. Pour se protéger contre cette menace croissante et la nouvelle réalité en matière de sécurité, veuillez trouver ci-dessous, de simples gestes à faire et à ne pas faire pour être mieux préparer à la sécurité informatique.

Depuis le début de la pandémie, tout le monde a appris à effectuer trois mesures simples pour rester en bonne santé. Lavez-vous les mains pendant 20 secondes. Ne vous touchez pas le visage. Restez à 2 mètre de distance. Bien sûr, il a fallu une certaine adaptation, mais vous vous êtes habitué à ce changement au bout de quelques semaines. Vous devez adopter la même attitude positive en changeant des comportements simples concernant l'utilisation de votre ordinateur, votre tablette et votre smartphone.

La sécurité informatique nécessite un effort communautaire de collaboration, semblable à celui nécessaire afin de lutter contre le coronavirus. Aussi, nous vous invitons à partager ce guide avec vos collègues, votre famille et vos amis.

Faire

- Utilisez des mots de passe/phrases de passe distincts pour le travail et l'usage personnel – idéalement comprenant au moins 16 caractères
- Mettez à jour tous les logiciels sur tous les a ppareils régulièrement – idéalement sur une base hebdomadaire
- Utilisez l'authentification multiples (dans la mesure du possible)

Ne pas faire

- Cliquez sur les liens ou les pièces jointes des courriers électroniques d'expéditeurs dont vous ne pouvez pas vérifiez l'identité
- Envoyez des informations financières ou personnelles par courrier électronique tant que vous n'avez pas appelé pour vérifier la transaction
- Utilisez des clés USB, des ordinateurs ou des Wi-Fi publics (dans la mesure du possible)

Pour plus de conseils et d'outils, consultez la Cyber Readiness Institute (CRI) dans les prochaines semaines. Nous nous sommes engagés à être une ressource clé pour aider les petites et moyennes entreprises (PME) à trouver un équilibre entre le travail à distance et la cybersécurité. Pour accéder à des guides sur la cybersécurité pour le télétravail, veuillez consulter le site **https://www.cyberreadinessinstitute.org/remote-work-resources**

Pour en savoir plus sur notre **programme** gratuit de **préparation à la sécurité informatique** et sur comment devenir un responsable en cybersécurité, consultez le site **www.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.

N'hésitez pas à nous contacter pour toute question, commentaire ou exemple de réussite (**guides@cyberreadinessinstitute.org**).

guide@cyberreadinessinstitute.com