Cybersecurity at Work Meeting Kit – French

QUELS SONT LES ENJEUX?

Un seul clic sur un lien malveillant peut coûter des millions à votre entreprise. Des rançongiciels aux courriels d'hameçonnage, les cyberattaques ne visent pas seulement les services informatiques – elles visent les personnes. Cela veut dire vous. Si vous gérez des courriels, ouvrez une session dans des systèmes, accédez à des données clients ou utilisez le Wi-Fi au travail, vous faites partie de la première ligne de défense. Les cybermenaces peuvent paralyser les opérations, divulguer des renseignements confidentiels et ruiner la réputation d'une organisation. Et elles ne représentent pas qu'un risque d'affaires – elles peuvent aussi mettre en péril votre emploi, votre identité et la sécurité de vos collègues. Rester vigilant sur le plan numérique n'est pas optionnel. C'est une responsabilité quotidienne.

QUELS SONT LES DANGERS?

Les menaces de cybersécurité ne ressemblent pas toujours à des menaces. Elles se présentent souvent sous forme de courriels inoffensifs, de fenêtres pop-up amicales ou d'écrans de connexion habituels. Mais derrière ces apparences se cache un danger réel – et une seule erreur peut suffire.

Hameçonnage et courriels frauduleux – Déguisés et dangereux

Les courriels d'hameçonnage sont conçus pour vous tromper. Ils semblent provenir de votre patron, de votre banque ou d'un fournisseur de confiance – mais contiennent des liens ou pièces jointes qui, une fois ouverts, permettent aux pirates de voler des données ou d'installer des logiciels malveillants.

- Certains courriels imitent des contacts internes et demandent des transferts urgents ou des mots de passe.
- D'autres incluent de fausses factures ou notifications d'expédition contenant des fichiers infectés.

Mots de passe faibles et réutilisés – Une cible facile

Utiliser le même mot de passe pour plusieurs systèmes, ou choisir des options simples comme « 123456 » ou le nom de son animal, facilite le travail des pirates. Une fois un système compromis, ils peuvent souvent accéder à d'autres – surtout si l'authentification multifacteur n'est pas activée.

Logiciels malveillants et rançongiciels – Mode verrouillage

Les rançongiciels peuvent bloquer entièrement votre système – fichiers, réseaux et même systèmes de sécurité. Vous pourriez voir un écran exigeant un paiement en

cryptomonnaie pour récupérer vos données. Ces attaques commencent souvent par un seul fichier ou lien infecté.

Appareils et réseaux non sécurisés – La menace silencieuse

Travaillez-vous à distance ou utilisez-vous vos appareils personnels pour le travail? S'ils ne sont pas sécurisés ou mis à jour, ils deviennent une porte d'entrée facile pour les cybercriminels.

- Se connecter à un Wi-Fi public sans VPN peut exposer des données sensibles.
- Les violations de données qui en découlent ont des conséquences bien réelles.

COMMENT SE PROTÉGER

La cybersécurité n'a pas besoin d'être compliquée – mais elle exige de la vigilance. La plupart des attaques ne viennent pas d'un « super pirate » franchissant un pare-feu, mais d'une personne qui clique sur un mauvais lien, réutilise un mot de passe ou ignore une mise à jour. La bonne nouvelle? Quelques habitudes solides peuvent faire toute la différence.

Réfléchissez avant de cliquer

C'est souvent là que tout commence – et que tout peut être évité. Les pirates envoient des courriels qui semblent légitimes. Peut-être que cela vient des « RH », ou de « l'informatique » qui vous demande de « mettre à jour votre mot de passe maintenant ». Ils comptent sur votre empressement. Ralentissez. Observez. Si quelque chose vous semble suspect, faites confiance à votre instinct. Mieux vaut transférer le message à votre équipe TI que de tomber dans le piège.

Utilisez des mots de passe forts et uniques

C'est l'une des mesures les plus simples – et les plus négligées. Considérez votre mot de passe comme la serrure de votre maison : utiliseriez-vous la même clé pour tout?

- Créez des mots de passe combinant lettres, chiffres et caractères spéciaux.
- Évitez les dates d'anniversaire, les noms d'animaux ou « 123456 ».
- Utilisez un gestionnaire de mots de passe – la plupart des entreprises en recommandent un.
- Changez régulièrement vos mots de passe et ne les partagez jamais – même pas avec un collègue.

Gardez vos appareils à jour

Oui, ces rappels de mise à jour sont agaçants – mais les ignorer, c'est laisser la porte ouverte aux menaces. Les mises à jour ne servent pas qu'à ajouter des fonctions; elles corrigent des failles de sécurité connues des pirates. Qu'il s'agisse de votre ordinateur portable, de votre poste de travail ou de votre téléphone, maintenez-les à jour. Plus vous attendez, plus le risque augmente.

Sécurisez le travail à distance et l'accès mobile

Le télétravail et la mobilité sont pratiques – jusqu'à ce que vos données tombent entre de mauvaises mains. Ne vous connectez jamais à un Wi-Fi public sans VPN et verrouillez toujours votre écran lorsque vous vous éloignez. Si votre entreprise vous fournit des outils de sécurité, utilisez-les – ce n'est pas optionnel. Et si vous utilisez vos appareils personnels, assurez-vous qu'ils soient protégés aussi.

Protégez les données de l'entreprise

Tout comme vous ne laisseriez pas des documents confidentiels dans la salle de pause, ne laissez pas non plus vos fichiers numériques sans protection. Faites attention à

la façon dont vous accédez, partagez et stockez les informations.

- Ne sauvegardez pas de fichiers professionnels sur des clés USB personnelles.
- Ne vous envoyez jamais de documents confidentiels à votre adresse personnelle.
- Utilisez uniquement les applications et plateformes approuvées pour l’entreposage et le partage de fichiers.

MOT DE LA FIN

La cybersécurité n’est pas seulement l’affaire du service informatique – c’est la responsabilité de tous. Un seul clic, un mot de passe réutilisé ou une mise à jour ignorée peuvent ouvrir la porte à une violation de données qui touche toute l’organisation.