La protection des données

Trajet aller 7 h - 9 h

Ouverture des e-mails
Consulter des e-mails sur votre téléphone peut parfois être source de problèmes, d'autant que l'intégralité des informations de l'expéditeur peut ne pas être visible. Si vous ne connaissez pas l'origine d'un e-mail, ne l'ouvrez pas. S'il vous semble suspect (e-mail de phishing, par exemple), informez l'équipe informatique à votre arrivée au bureau ou signalez-le en cliquant sur le bouton Report Phishing de votre messagerie.

Conversations
Faites attention à ce que vous dites et veillez à ne pas parler trop fort. Les personnes autour de vous pourraient entendre des informations confidentielles considérées comme des « données à caractère personnel ».

Gestion des e-mails sur votre appareil mobile
Sur les appareils mobiles, vérifier l'exactitude des adresses électroniques, du contenu et des pièces jointes avant envoi n'est pas chose facile. Si vous le pouvez, attendez d'arriver au bureau. Sinon, assurez-vous d'utiliser le système de messagerie de votre entreprise.

Au bureau 9 h - 17 h

Téléchargements
Au bureau, vous pourriez être tenté de vous inscrire ou de télécharger une application, un navigateur ou un système informatique tiers en vue d'améliorer un processus commercial. Pour éviter l'introduction de programmes malveillants ou toute autre complication, tous les besoins logiciels (installations ou applications web) doivent être initialement approuvés par votre équipe informatique.

Envoi des e-mails sécurisés au bureau
Utilisez uniquement le système de messagerie officiel de votre entreprise pour garantir l'affichage et l'envoi sécurisés des e-mails et éviter l'omission accidentelle de certains contrôles supplémentaires (comme la détection de virus, le dépistage de programmes malveillants et l'analyse des activités). Suivez les politiques de sécurité informatique de votre entreprise en matière de verrouillage d'écran, de protection par mot de passe et de chiffrement de stockage.

Accès à des données à caractère personnel ou sensible
Si vous avez accès à des données à caractère personnel ou sensible, assurez-vous qu'elles soient sécurisées. En l'absence d'une raison commerciale valable, ne les partagez pas.

Transfert de données à caractère personnel
Avant d'envoyer des données à un tiers, vérifiez si votre entreprise a signé un contrat ou un accord de confidentialité avec ce tiers. Si vous envoyez des fichiers contenant des informations sensibles à un tiers autorisé, utilisez une solution sécurisée de transfert de fichiers.

Suppression et archivage des fichiers obsolètes
Si vous avez des fichiers ou des documents dont vous n'avez plus l'utilité, archivez-les ou supprimez-les selon les cas. Renseignez-vous auprès de votre équipe informatique sur les processus locaux approuvés, notamment les politiques de conservation, de classification et de destruction des documents.

Trajet retour 17 h - 19 h

Informations sans surveillance
Veillez à ne pas laisser votre ordinateur portable ouvert ou l'écran de votre PC visible. Pensez à verrouiller les écrans de vos systèmes lorsque vous les laissez sans surveillance au bureau et arrêtez-les complètement à la fin de la journée avant de rentrer chez vous.

Traitement des données hors du bureau
Vous pourriez être amené à travailler sur des données hors du bureau, à domicile ou lorsque vous partez en déplacement, surtout si elles se trouvent sur votre ordinateur portable. Faites preuve de vigilance, peu importe le support utilisé pour traiter ces données. Qu'elles se trouvent sur une clé USB ou dans un dossier, vous devez les traiter conformément aux processus habituels de votre entreprise.

Elimination de données confidentielles
Ne laissez pas traîner de documents confidentiels ou sensibles (dans le train ou ailleurs). Mettez-les sous clé ou, si vous n'en avez plus besoin, détruisez-les ou placez-les dans un bac de déchiquetage verrouillé et sécurisé.

Connexions
Sur le trajet du retour, réfléchissez à deux fois avant de vous connecter à des réseaux WiFi non sécurisés. Si vous prévoyez d'accéder à des données à caractère personnel, utilisez toujours un réseau privé virtuel (RPV) qui chiffre les données, même si elles sont transmises sur un réseau qui est probablement sécurisé.

#JeProtègelesDonnées