FEDIL

Publication

TÉLÉTRAVAIL: LA SÉCURITÉ ET LA CYBERSÉCURITÉ PEUVENT ALLER DE PAIR

Le travail à domicile sera le seul moyen de travailler pour de nombreuses personnes. La
sécurité d'abord! Mais la cybersécurité ne doit pas être oubliée...
Dans cette situation très particulière, le travail à distance sera le seul moyen de travailler
pour de nombreuses personnes et un choix très judicieux pour de nombreuses autres. La
sécurité est la priorité absolue pour le moment. Mais la cybersécurité ne doit pas être
oubliée si nous ne voulons pas ajouter le chaos numérique au chaos «physique». Nous vous
donnons quelques conseils de base pour vous protéger et protéger vos informations en ces
temps difficiles.

Dispositifs

• Faites particulièrement attention à ce que les appareils tels que les clés USB, les
téléphones, les ordinateurs portables ou les tablettes ne soient pas perdus ou égarés.
• Assurez-vous que chaque appareil dispose des mises à jour nécessaires, telles que les
mises à jour du système d'exploitation (comme iOS ou Android) et les mises à jour
logicielles / antivirus.
• Assurez-vous que votre ordinateur, ordinateur portable ou appareil est utilisé dans
un endroit sûr, par exemple où vous pouvez le voir et minimiser qui d'autre peut voir
l'écran (en particulier si vous travaillez avec des données personnelles sensibles).
• Verrouillez votre appareil si vous devez le laisser sans surveillance pour une raison
quelconque.
• Assurez-vous que vos appareils sont éteints, verrouillés ou stockés avec soin lorsqu'ils ne sont pas utilisés.
• Utilisez des contrôles d'accès efficaces (tels que l'authentification multi

facteur et
des mots de passe forts) et, le cas échéant, le cryptage pour restreindre l'accès à l'appareil et pour réduire le risque si un appareil est volé ou égaré.
• Lorsqu'un appareil est perdu ou volé, vous devez prendre des mesures immédiates
pour assurer un effacement de la mémoire à distance, si possible.

Emails

• Utilisez des comptes de messagerie professionnels plutôt que des comptes personnels pour les e-mails liés au travail impliquant des données personnelles. Si
vous devez utiliser un e-mail personnel, assurez-vous que le contenu et les pièces
jointes sont cryptés et évitez d'utiliser des données personnelles ou confidentielles
dans les lignes d'objet.
• Avant d'envoyer un e-mail, assurez-vous de l'envoyer au bon destinataire, en particulier pour les e-mails impliquant de grandes quantités de données personnelles ou des données personnelles sensibles.
• Si possible, préférez envoyer des e-mails chiffrés à chaque fois.
Accès au cloud et au réseau
• Ne vous connectez à aucun réseau public, inconnu ou non contrôlé
o Connectez-vous aux réseaux 3G ou 4G si vous n'avez pas accès à une connexion Wi-Fi sécurisée
o Utilisez un VPN
• Dans la mesure du possible, utilisez uniquement les réseaux ou services de confiance
de votre organisation et respectez toutes les règles et procédures organisationnelles
concernant l'accès au cloud ou au réseau, la connexion et le partage de données.
• Si vous travaillez sans accès au cloud ou au réseau, assurez-vous que toutes les
données stockées localement sont correctement sauvegardées en toute sécurité.
• Les logiciels d'accès à distance (comme Teamviewer) doivent être utilisés très soigneusement et uniquement par des employés autorisés. Il doit toujours être mis à
jour et utilisé uniquement en cas de nécessité absolue.

Spécial pour RSSI

Assurez-vous que chaque appareil mobile utilisé par les employés est sûr et que vous avez la
possibilité de les essuyer en cas de vol ou de perte.
Utilisez la gestion des appareils mobiles pour sécuriser les appareils utilisés par les employés

Communiqué par SECURITYMADEIN.LU