

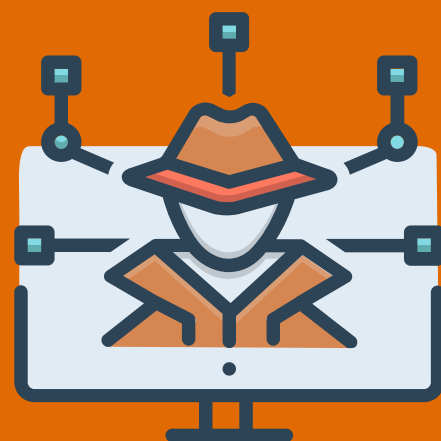
# PRÉVENTION DE LA CYBERCRIMINALITÉ



## Protéger les RPM

### LE RISQUE CROISSANT DE LA CYBERCRIMINALITÉ

- La cybercriminalité est le crime qui connaît la croissance la plus rapide au monde, se classant au 3e rang mondial derrière la corruption gouvernementale et les stupéfiants.
- Le coût global estimé des attaques de cybersécurité en 2015 était de 400 milliards de dollars.
- Le coût prévu en 2019 était estimé à plus de 1 000 milliards de dollars.
- Le vol de propriété intellectuelle représente au moins un quart du coût de la cybercriminalité.



### EXEMPLES COURANTS DE CYBERCRIMINALITÉ



- L'hameçonnage est l'endroit où le fraudeur enverra un e-mail d'apparence légitime tentant d'amener l'employé à fournir des données.
- Le piratage, c'est lorsqu'un criminel utilise la technologie pour accéder à un compte d'individu ou d'entreprise afin d'obtenir un accès non autorisé aux informations et au système à son profit personnel.
- Les attaques de logiciels malveillants sont ciblées pour voler des données à l'entreprise.
- Les attaques de ransomware exigeront un paiement de la part de l'entreprise pour permettre l'accès au système et aux données.

### ZONES À RISQUE DE CYBERCRIMINALITÉ

- Demandes de renseignements personnels.
- Demandes d'informations sur la propriété intellectuelle.
- Informations sur la paie.
- Informations sur les comptes clients et fournisseurs.
- Fraude par fil - Modifications des coordonnées bancaires.
- Modification des détails du client et du fournisseur.
- Changement d'adresse de livraison pour les bons de commande.
- Fraude au bon de commande.



### RÉGIME DE PROTECTION



- Soyez vigilant. Qui est l'expéditeur ?
- Ne répondez pas aux e-mails suspects.
- Utilisez des mots de passe forts.
- Vérifiez toujours les demandes d'informations de manière indépendante.
- Un mot de passe protège les informations sensibles.
- Suivez les contrôles internes conçus pour atténuer les risques.
- Méfiez-vous toujours des e-mails qui demandent une action immédiate.
- Ne cliquez pas sur les liens, ne téléchargez pas ou n'ouvrez pas de pièces jointes provenant d'expéditeurs inconnus.
- Gardez les mises à jour informatiques à jour, contrôlez votre risque de spam.
- Tenez également compte du risque lié aux téléphones portables.
- Communiquez la tentative à la direction.

NOUS SOMMES RPM ET NOTRE SUCCÈS DÉPEND DE CHACUN DE NOUS SUIVANT LA BONNE VOIE ET ADOPTANT NOTRE VALEUR DE 168® POUR PRENDRE LES BONNES DÉCISIONS.

CONTACTEZ-NOUS : [CONFORMITÉ@RPMINC.COM](mailto:CONFORMITÉ@RPMINC.COM)

