



PARLONS  
PRÉVENTION

# COMPROMISSION DE COURRIELS D'ENTREPRISE ET PIRATAGE PSYCHOLOGIQUE

Les cybercriminels abusent de la confiance des gens : voici ce que votre entreprise peut faire pour réduire les risques

La compromission des courriels d'entreprise constitue l'une des formes de cyberfraude les plus courantes pour les entreprises de nos jours, et elle peut causer des pertes financières considérables. Dans ce type d'arnaque, les fraudeurs ne font pas que tirer profit des failles techniques. Ils visent à exploiter la confiance des gens, la nature humaine en général et les processus d'affaires, et ce, en usurpant l'identité de personnes de confiance, comme les dirigeants, les fournisseurs, les clients, les avocats ou les comptables. Leur objectif est souvent de détourner des paiements, d'obtenir des renseignements sensibles ou d'accéder aux systèmes de l'entreprise ciblée.

Les autorités canadiennes continuent de signaler des pertes importantes liées à la compromission de courriels d'entreprise et à l'hameçonnage ciblé. Mais, puisque ce ne sont pas toutes les pertes qui sont déclarées, les experts estiment que les pertes réelles pourraient être nettement plus élevées<sup>1</sup>.



### TACTIQUES COURANTES DE COMPROMISSION DES COURRIELS D'ENTREPRISE

Les cybercriminels adaptent sans cesse leurs méthodes, mais les stratagèmes couramment utilisés comprennent les suivants :

- **Usurpation de l'identité d'un dirigeant** : Un fraudeur se fait passer pour un cadre supérieur et demande un paiement ou un virement urgent et confidentiel. Typiquement, le fraudeur cherche à créer un sentiment d'urgence pour dissuader la victime de vérifier l'authenticité de la demande.
- **Détournement du paiement d'un fournisseur** : Un cybercriminel se fait passer pour un fournisseur ou un sous-traitant et fournit de nouvelles coordonnées bancaires ou des instructions « mises à jour » à sa victime pour qu'elle fasse un virement. Il peut ainsi détourner le paiement légitime vers un compte frauduleux.
- **Détournement de la paie** : Un fraudeur se fait passer pour un employé et demande la modification de renseignements relatifs à la paie ou au dépôt automatique du salaire afin de détourner les fonds.

- **Usurpation de l'identité d'un conseiller professionnel** :

Un fraudeur peut aussi prétendre être un avocat, un comptable ou un conseiller en placements afin d'inciter la victime à effectuer un virement non autorisé ou à divulguer des renseignements sensibles.

### Autres techniques de piratage psychologique

Les fraudes par compromission des courriels d'entreprise s'inscrivent souvent dans le cadre de tactiques plus larges de piratage psychologique<sup>2</sup> et peuvent comprendre les techniques suivantes :

- Formes courantes d'hameçonnage, comme l'hameçonnage ciblé, vocal ou par texto
- Fraudes par code QR et par transfert de documents
- Formes plus sophistiquées d'hameçonnage conçues pour récupérer des mots de passe et des données d'authentification
- Fausses demandes de consentement et manipulation de règles de courriels pour dissimuler des activités frauduleuses ou rediriger des communications

### Soyez attentif aux indices

- Demandes impliquant une certaine urgence ou un caractère confidentiel
- Nouvelles instructions bancaires ou de paiement
- Demandes visant à contourner les procédures d'approbation habituelles
- Messages dont la mise en page, le langage, la grammaire ou le ton sont inhabituels
- Demandes reçues tandis qu'une personne est en déplacement ou indisponible, ou encore à un moment où il est difficile de faire des vérifications

### MESURES CONCRÈTES POUR CONTRIBUER À RÉDUIRE LES RISQUES

#### Renforcer les contrôles relatifs aux paiements et à la paie

Des processus internes rigoureux peuvent vous aider à prévenir les pertes liées aux fraudes par compromission de courriels d'entreprise. Pensez, notamment, à :

- Vérifier par téléphone toutes les demandes de changement bancaire ou de paiement en utilisant un numéro de téléphone de confiance déjà enregistré dans vos systèmes
- Exiger une double approbation pour les transactions importantes et les changements apportés aux comptes
- Adopter un processus de vérification par une deuxième personne pour les mises à jour des renseignements sur la paie et les fournisseurs
- Mettre en place des procédures pour les modifications de paiement et les virements bancaires et les consigner

## Utiliser l'authentification multifacteur

L'authentification multifacteur (AMF) demeure l'une des mesures de contrôle les plus efficaces pour réduire les accès non autorisés<sup>3</sup>.

Vous devriez songer à activer l'authentification multifacteur pour les éléments suivants :

- Les comptes de courriel
- Les applications bancaires
- Les services infonuagiques
- Les réseaux privés virtuels et les outils d'accès à distance
- Les comptes administratifs

Les employés des Finances, les dirigeants et les administrateurs des TI peuvent avoir intérêt à adopter des méthodes d'authentification multifacteur plus robustes et offrant une meilleure résistance à l'hameçonnage que la norme habituelle, lorsque possible<sup>3</sup>.

## Renforcer la sécurité des courriels

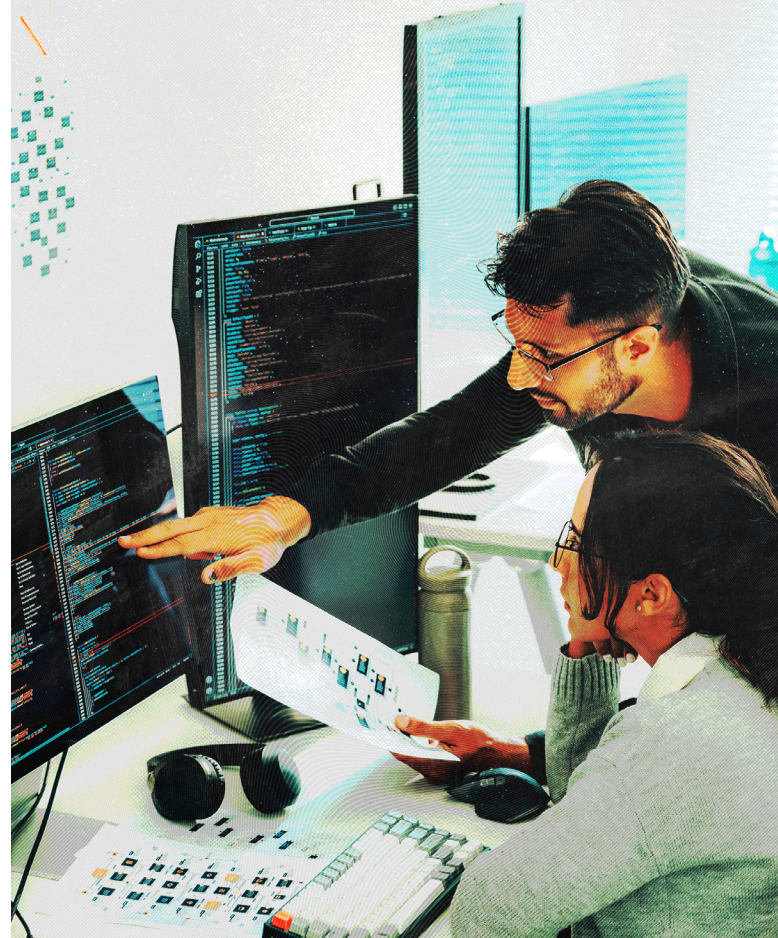
Comme la compromission des courriels d'entreprise commence souvent par la compromission d'un compte de messagerie, pensez à revoir les contrôles de sécurité des courriels. Voici quelques importantes mesures à prendre :

- Pour vérifier l'authenticité des expéditeurs et réduire les risques d'hameçonnage et d'usurpation d'adresses de courriel, mettre en œuvre des contrôles d'authentification des courriels : Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC), etc.
- Revoir régulièrement les règles de transfert, les accès délégués aux boîtes de courriels et les paramètres de sécurité des courriels
- Surveiller les anomalies concernant les comptes de courriel, les comportements des usagers et les connexions, surtout lorsque les heures, les endroits ou les appareils sont inhabituels

## Sensibiliser les employés

De nombreuses fraudes par compromission de courriels d'entreprise aboutissent parce qu'elles semblent légitimes. Une formation de sensibilisation pourrait aider vos employés à reconnaître les activités suspectes et à y réagir. La formation devrait porter sur :

- Les stratagèmes de fraude concernant les paiements
- Les détournements de la paie
- Les tentatives d'hameçonnage
- Les attaques par demande d'authentification répétée
- Les tactiques d'usurpation d'identité
- Les pièces jointes et les liens suspects



## Maintenez une bonne cyberhygiène

Des pratiques rigoureuses en matière de cyberhygiène peuvent contribuer à réduire l'exposition à toute une série de risques de cyberfraudes, comme les attaques par rançongiciel et la compromission des courriels. Parmi les pratiques clés figurent les suivantes :

- Utiliser des phrases de passe fortes et uniques
- Maintenir à jour les systèmes d'exploitation et les logiciels
- Déployer des antivirus ou des systèmes de protection évolutive des points de terminaison (PEPT)
- Limiter les privilèges administratifs
- Effectuer régulièrement des analyses de vulnérabilité
- Chiffrer les données sensibles
- Faire des copies de sauvegarde sécurisées et les tester régulièrement pour protéger les données essentielles et en faciliter la récupération en cas de cyberincident. Les copies peuvent inclure des sauvegardes non modifiables et non supprimables (à moins d'avoir les autorisations requises) stockées sur le nuage ou hors ligne. Ces copies peuvent accélérer la remise sur pied à la suite d'une attaque par rançongiciel
- Tester régulièrement les procédures de restauration des sauvegardes

## Si vous soupçonnez une fraude, agissez rapidement

Une intervention rapide peut contribuer à réduire l'impact d'un cyberincident et les pertes financières. Pensez à :

1. Contacter immédiatement votre institution financière pour qu'elle suspende ou annule toute transaction problématique
2. Réinitialiser les paramètres d'authentification multifacteur et les identifiants qui pourraient avoir été compromis
3. Revoir vos comptes de courriel pour vérifier s'il y a des règles de transfert ou des accès non autorisés
4. Signaler l'incident aux autorités compétentes, notamment au Centre antifraude du Canada et au Centre national de coordination en cybercriminalité
5. Vérifier les renseignements relatifs à vos fournisseurs et à vos paiements avant de recommencer à effectuer des transactions

## COMMENT NOUS POUVONS VOUS AIDER

Northbridge Assurance propose des solutions d'assurance des cyberrisques et offre les services Assistance Cyberrisques, qui sont conçus pour aider les entreprises à **renforcer leur cyberrésilience et à se préparer à faire face à d'éventuels incidents**. Les clients admissibles ont également accès à des outils tels que des analyses de vulnérabilité, des autoévaluations et des simulations d'incidents.

Pour savoir comment mieux protéger votre entreprise, communiquez avec le Service de prévention au **1.833.692.4111** ou rendez-vous sur notre site [www.northbridgeassurance.ca](http://www.northbridgeassurance.ca).

[5066-001-ed04F | 10.2026]

Northbridge Assurance, le logo Northbridge Assurance et *Parlons prévention* sont des marques de commerce utilisées par la **Société d'assurance générale Northbridge** (émettrice des polices Northbridge Assurance) avec l'autorisation de la Corporation financière Northbridge. Nous ne faisons aucune assertion et n'offrons aucune garantie relativement à l'exactitude ou à l'intégralité des renseignements contenus dans le présent document. Nous ne pourrions en aucun cas être tenus responsables des pertes pouvant découler de l'utilisation de ces renseignements.

<sup>1</sup> Gendarmerie royale du Canada (GRC), 2025.

<sup>2</sup> Centre canadien pour la cybersécurité, gouvernement du Canada, 2024-2025.

<sup>3</sup> Centre canadien de lutte contre la fraude, gouvernement du Canada, 2025.

