

Fiche de la première heure : incident de cybersécurité

Quoi faire, qui appeler et à quoi ne pas toucher dans la première heure d'un rançongiciel, d'une fraude par courriel ou de la perte d'un portable.

[PDF à imprimer](#)[Lecture de 8 minutes](#)[Mis à jour en octobre 2026](#)

Imprimez-la. Affichez un exemplaire près de la salle des serveurs et rangez-en un dans le bureau de la personne responsable de l'administration. Remplissez la section des contacts aujourd'hui, pas pendant l'incident.

PARTIE 1 : QUOI FAIRE DANS LA PREMIÈRE HEURE

Si de l'argent est sorti par virement ou par TEF dans les 72 dernières heures : appelez maintenant la ligne antifraude de votre banque, puis revenez ici.

Avant toute chose (2 minutes)

- 1 Désignez une seule personne responsable de l'incident.** Une personne décide, toutes les autres lui rendent compte. Quand deux personnes donnent des consignes différentes aux TI, vous perdez un temps que vous n'avez pas.
- 2 Commencez un journal papier.** Notez l'heure, ce que vous avez constaté et qui a fait quoi. Utilisez du papier ou un téléphone qui n'est pas sur le réseau de l'entreprise. Votre assureur, votre avocat et l'organisme de réglementation vous demanderont tous cette chronologie, et c'est à partir d'elle qu'on jugera si vous avez agi « avec diligence ».
- 3 Cessez d'utiliser le courriel de l'entreprise et Teams/Slack pour en parler.** Dans bien des cas de rançongiciel et de fraude par courriel, l'attaquant peut lire la boîte de courriel. Passez par le téléphone, ou par un groupe Signal/WhatsApp sur des téléphones personnels.

Qu'avez-vous devant vous?

VOUS CONSTATEZ...	IL S'AGIT PROBABLEMENT DE...	ALLEZ À
Des fichiers renommés avec une extension inhabituelle, une demande de rançon, des serveurs ou des lecteurs partagés soudainement inaccessibles	Rançongiciel	A

VOUS CONSTATEZ...	IL S'AGIT PROBABLEMENT DE...	ALLEZ À
Un client ou un fournisseur dit avoir reçu de vous un courriel avec de nouvelles coordonnées bancaires; un paiement est parti dans le mauvais compte; des règles de boîte de réception étranges; des demandes d'authentification multifacteur que personne n'a faites	Prise de contrôle d'un compte de courriel / fraude au paiement (compromission de courriel d'affaires)	B
Un portable, un téléphone ou une clé USB perdu ou volé	Appareil perdu	C
Une alerte de connexion inhabituelle, une fenêtre de l'antivirus, une impression que « quelque chose cloche »	Traitez-le comme B jusqu'à preuve du contraire	B

A. Rançongiciel

À faire

- ✓ **Débranchez le câble réseau et coupez le Wi-Fi des appareils touchés. Laissez-les allumés.** La mémoire contient des preuves (processus en cours, parfois des clés) qui disparaissent à l'arrêt.
Exception : si un serveur de fichiers est visiblement en train de chiffrer et que vous ne pouvez pas couper son réseau, l'éteindre est le moindre mal. Notez que vous l'avez fait, et à quelle heure.
- ✓ **Déconnectez les sauvegardes dès maintenant.** Débranchez les disques de sauvegarde USB ou NAS. Changez le mot de passe et l'authentification multifacteur de la console de sauvegarde à partir d'un appareil sain (un téléphone, un ordinateur à la maison), jamais à partir d'un poste du réseau touché. Les attaquants s'en prennent aux sauvegardes très tôt.
- ✓ **Appelez la ligne d'urgence de votre assureur avant d'embaucher qui que ce soit ou de dépenser de l'argent.** Bien des polices exigent le consentement préalable de l'assureur et le recours à ses fournisseurs attitrés; les frais engagés avant risquent de ne pas être remboursés. N'attendez pas son rappel pour contenir l'attaque : isoler des appareils est toujours permis.

À ne pas faire

- ✗ **N'ouvrez pas le lien de la demande de rançon et ne communiquez pas avec les attaquants.** Tout contact leur apprend que vous les avez repérés et peut accélérer la fuite de données. Payer ne garantit pas que vous récupérerez vos données, et pourrait être illégal au regard des lois sur le terrorisme, le recyclage des produits de la criminalité ou les sanctions (Centre canadien pour la cybersécurité). Toute négociation relève de spécialistes, en coordination avec votre assureur et votre avocat.
- ✗ **Ne restaurez pas tout de suite dans le même réseau.** Si vous restaurez avant d'avoir fermé la porte d'entrée, vous restaurez dans un réseau que l'attaquant contrôle encore, et vous écrasez les preuves de ce qu'il a pris. La porte d'entrée est habituellement un RPV ou un pare-feu sans authentification multifacteur, un bureau à distance exposé ou un mot de passe volé. Restaurez une fois ce problème réglé, ou dans un environnement isolé et reconstruit, avec votre firme d'intervention en cas d'incident.
- ✗ **Ne réinstallez pas, n'effacez rien et ne lancez pas d'outil de « nettoyage ».** Vous détruiriez les preuves que votre assureur, votre avocat et l'organisme de protection des renseignements personnels vous demanderont.

- ✓ **Pour les TI :** exportez les journaux du pare-feu, du RPV et de l'EDR vers un support hors ligne avant que quiconque fasse le « ménage ». Notez quels journaux s'écrasent, et à quel moment.

- ✗ **Ne tenez pas pour acquis qu'« ils ont seulement chiffré, ils n'ont rien volé ».** La plupart des groupes de rançongiciel copient maintenant les données avant de les chiffrer. Tant que l'enquête forensique n'a pas démontré le contraire, planifiez comme si des renseignements personnels avaient été pris.

B. Prise de contrôle d'un courriel / fraude au paiement (compromission de courriel d'affaires)

À faire

- ✓ **Si de l'argent est sorti : appelez la ligne antifraude de votre banque dans l'heure et demandez le rappel du virement.** Les chances de récupérer les fonds baissent d'heure en heure, à mesure qu'ils sont transférés ailleurs. Portez ensuite plainte à la police : la banque et l'assureur vous demanderont le numéro de dossier.
- ✓ **Bloquez le compte, puis coupez les sessions.** Réinitialiser le mot de passe ne déconnecte pas un attaquant qui détient déjà un jeton de session. Dans Microsoft 365 : Centre d'administration Microsoft Entra → Utilisateurs → l'utilisateur → *Révoquer les sessions*. Bloquez aussi la connexion pendant l'enquête, car les jetons déjà émis peuvent rester valides jusqu'à environ une heure. Supprimez ensuite les méthodes d'authentification multifacteur et faites-les réinscrire (les attaquants ajoutent souvent leur propre application d'authentification). Dans Google Workspace : réinitialisez les témoins de connexion et vérifiez les appareils inscrits à la validation en deux étapes.
- ✓ **Prenez des photos avant de supprimer quoi que ce soit :** les règles de boîte de réception (transfert, suppression automatique, déplacement des messages vers « Flux RSS » ou « Archive »), le transfert de la boîte aux lettres, les applications autorisées (consentements OAuth), les appareils d'authentification multifacteur récemment ajoutés.

À ne pas faire

- ✗ **Ne supprimez ni le courriel d'hameçonnage ni les règles malveillantes.** Ils montrent ce que l'attaquant a lu. C'est ce qui détermine si des renseignements personnels ont été consultés, et donc vos obligations en vertu de la Loi 25 et de la LPRPDE.
- ✗ **Ne répondez pas au fil frauduleux** pour « avertir » l'autre partie. L'attaquant contrôle ce fil.

- ✓ **Exportez les journaux aujourd'hui.** Les journaux de connexion et d'audit de Microsoft Entra sont conservés **7 jours** avec la version gratuite et **30 jours** avec Entra ID P1/P2. Le journal d'audit unifié de Microsoft 365 (Audit Standard) est conservé 180 jours. Les journaux non exportés risquent d'avoir disparu avant le début de l'enquête forensique.
- ✓ **Téléphonez à vos principaux clients et fournisseurs** (avec les numéros de vos propres dossiers, pas ceux du courriel) pour les avertir que toute modification bancaire « venant de nous » est frauduleuse. L'attaquant a souvent écrit à tout votre carnet d'adresses.

C. Appareil perdu ou volé

À faire

- ✓ **Établissez d'abord un seul fait : l'appareil était-il chiffré (BitLocker, FileVault, code d'accès du téléphone) et verrouillé?** C'est en grande partie ce qui détermine si vous faites face à un incident de confidentialité à déclarer. Demandez une preuve aux TI, comme le rapport de conformité de la gestion des appareils mobiles (MDM) ou la clé de récupération BitLocker conservée sous séquestre. « Je pense que oui » n'est pas une preuve.
- ✓ **Verrouillez ou effacez l'appareil à distance par la MDM** (Intune, Jamf, gestion des points de terminaison de Google). Notez l'heure et la confirmation.
- ✓ **Révoquez les sessions de l'utilisateur et changez tous les mots de passe enregistrés dans le navigateur** (courriel, banque, applications d'affaires).
- ✓ **Portez plainte à la police s'il s'agit d'un vol.** L'assureur et les organismes de réglementation vous demanderont le numéro de dossier.

À ne pas faire

- ✗ **N'omettez pas l'inscription au registre sous prétexte que l'appareil était chiffré.** En vertu de la Loi 25, tout incident de confidentialité doit être consigné au registre, y compris la perte d'un appareil contenant des renseignements personnels. Consignez-le et notez pourquoi vous avez jugé le risque faible (chiffré, verrouillé, effacé à 14 h 32).

Appelez dans cet ordre

- 1 **La ligne antifraude de la banque en premier** si de l'argent a bougé dans les 72 dernières heures.
- 2 **La personne responsable de l'incident à l'interne** (elle décide; une seule voix).
- 3 **La ligne d'urgence de l'assureur**, *avant* d'embaucher des fournisseurs ou de dépenser de l'argent. L'assureur désigne habituellement un avocat coordonnateur (*breach coach*) et une firme d'enquête forensique. **Pas d'assurance?** Appelez directement une firme d'intervention en cas d'incident et un avocat.
- 4 **L'avocat coordonnateur ou votre avocat.** Mener l'enquête par l'intermédiaire d'un avocat peut aider à protéger le secret professionnel. Posez-lui la question; ne le tenez pas pour acquis.
- 5 **Votre fournisseur TI ou fournisseur de services gérés.** Dites-lui : contenir, ne rien effacer. Si son outil de gestion à distance a pu servir de porte d'entrée à l'attaquant, il fait partie de l'enquête, pas seulement de la solution.
- 6 **La police et le Centre antifraude du Canada** en cas de fraude ou d'extorsion : 1-888-495-8501, signalementcyberetfraude.canada.ca. Le **Centre canadien pour la cybersécurité** reçoit aussi les signalements : 1-833-CYBER-88 (1-833-292-3788), Mon cyberportail.
- 7 **Les organismes de protection des renseignements personnels** : une fois les faits établis, avec votre avocat (voir les délais ci-dessous).
- 8 **Le personnel, les clients, les partenaires** : une seule fois, à partir d'un texte préparé. Ne laissez pas les rumeurs circuler avant vous.

Preuves à conserver (ne rien supprimer, ne pas faire de « ménage »)

- Votre journal papier (avec l'heure de chaque entrée).
- Des photos des demandes de rançon, des messages d'erreur et des courriels suspects (écran complet, avec l'heure visible).
- Les courriels suspects eux-mêmes, exportés avec les en-têtes complets (.eml/.msg), et non transférés.
- Les journaux du pare-feu, du RPV, de l'EDR ou de l'antivirus, ainsi que les journaux de connexion et d'audit de Microsoft 365 ou Google Workspace, exportés vers un support hors ligne.
- Les appareils touchés : allumés et débranchés du réseau, ou éteints et étiquetés avec le nom des personnes qui les ont manipulés et l'heure.
- Les confirmations bancaires, les détails du virement, la fausse facture.
- La liste de toutes les personnes qui ont touché à un système touché, avec les heures.

Délais réglementaires

Au Canada, les lois sur la protection des renseignements personnels ne fixent **pas de nombre d'heures**, contrairement aux 72 heures européennes. « Avec diligence » et « le plus tôt possible » s'évaluent après coup, et c'est votre journal qui vous permet de le démontrer. Les secteurs réglementés font exception (voir le tableau).

SI VOUS...	OBLIGATION	DÉLAI
Exercez des activités au Québec (Loi 25, loi sur le secteur privé)	Consigner tous les incidents de confidentialité au registre, graves ou non. Conserver chaque inscription au moins 5 ans après la date où vous avez pris connaissance de l'incident. Prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents se produisent.	Registre : dès maintenant.
	Évaluer le risque avec votre responsable de la protection des renseignements personnels . S'il existe un risque qu'un préjudice sérieux soit causé , aviser la Commission d'accès à l'information (formulaire <i>Déclaration d'un incident de confidentialité</i>) et les personnes concernées. Facteurs à considérer : la sensibilité des renseignements, les conséquences appréhendées de leur utilisation, la probabilité qu'ils soient utilisés à des fins préjudiciables. L'avis aux personnes peut être reporté tant qu'il risquerait d'entraver une enquête. Vous pouvez aussi aviser toute personne en mesure de diminuer le risque, en ne communiquant que les renseignements nécessaires.	Avec diligence.
Êtes assujetti à la LPRPDE (loi fédérale; s'applique souvent en parallèle avec la Loi 25 lorsque des renseignements franchissent une frontière provinciale ou nationale)	Si l'atteinte présente un risque réel de préjudice grave : déclarer l'atteinte au Commissariat à la protection de la vie privée du Canada (formulaire en ligne), aviser les personnes touchées et aviser les organisations qui peuvent réduire le préjudice (p. ex. les banques). Tenir un registre de toutes les atteintes pendant 24 mois .	Le plus tôt possible après avoir conclu qu'une atteinte a eu lieu.
Exercez des activités en Alberta	La PIPA exige une déclaration distincte au Commissariat à l'information et à la protection de la vie privée de l'Alberta lorsqu'une personne raisonnable conclurait à un risque réel de préjudice important.	Sans délai déraisonnable.
Êtes une institution financière réglementée (Autorité des marchés financiers au Québec, BSIF au fédéral)	Déclarer les incidents de sécurité de l'information à votre organisme de réglementation. AMF : mises à jour tous les 3 jours, rapport final dans les 30 jours suivant la résolution.	Dans les 24 heures (règlement de l'AMF en vigueur depuis avril 2025; préavis du BSIF).
Avez une assurance cyber	Clause d'avis de sinistre de votre police. Un avis tardif est une cause classique de réclamation contestée.	Selon votre police : inscrivez-le ci-dessous.

SI VOUS...	OBLIGATION	DÉLAI
Avez des contrats clients ou des ententes de traitement des données	Bien des contrats exigent d'aviser le client dans un délai fixe (souvent de 24 à 72 heures).	Selon le contrat : inscrivez le plus strict ci-dessous.

Cette fiche ne constitue pas un avis juridique. C'est votre avocat coordonnateur qui décide quoi déclarer, et quand.

À remplir aujourd'hui

RÔLE	NOM	TÉLÉPHONE (24/7)	PERSONNE DE RELÈVE
Responsable de l'incident			
Substitut (si le responsable est injoignable)			
Fournisseur TI / services gérés			
Ligne d'urgence de l'assureur			
Numéro de police		Délai d'avis prévu à la police :	
Avocat coordonnateur / avocat			
Ligne antifraude de la banque		Directeur de compte :	
Firme d'intervention en cas d'incident (si vous n'êtes pas assuré, ou une fois approuvée par votre assureur)			
Responsable de la protection des renseignements personnels (Loi 25)			
Clause d'avis client la plus stricte	Client :	Heures :	

Si vous êtes assuré, demandez dès maintenant à votre assureur quelles firmes d'intervention il approuve, pour éviter tout litige le jour J.

Où se trouvent les copies hors ligne : identifiants administrateur des sauvegardes : ____ · compte administrateur d'urgence (bris de glace) : ____ · la présente fiche (copie numérique, hors des systèmes de l'entreprise) : ____

Dernière révision : __ / __ / __ par : ____

Besoin d'un deuxième regard?

Parlez directement à l'expert qui dirigerait le mandat.



PRIVATEER
C Y B E R S E C U R I T Y

privateer.ca · info@privateer.ca