



## UTILISATEUR D'UN ORDINATEUR PERSONNEL

### SIGNALEZ-LES !

#### Comment dois-je réagir?

Si vous devenez une victime, ne paniquez pas. Cessez immédiatement d'utiliser votre ordinateur. Appelez un professionnel de la TI digne de confiance qui pourra essayer d'isoler la menace.

Signalez l'incident à votre service de police local. N'oubliez pas qu'il est important de signaler tous les incidents; ils constituent un outil précieux pour les enquêteurs.

Communiquez également avec le **Centre antifraude du Canada (CAFC)** en signalant l'incident en ligne en tout temps à [www.antifraudcentre-centreantifraude.ca](http://www.antifraudcentre-centreantifraude.ca). Cliquez sur l'onglet « Signaler un incident », puis sur le lien menant au « Système de signalement des fraudes » ou appelez le CAFC en composant le 1-888-495-8501, de 8 h 30 à 17 h (HNE), du lundi au vendredi.

Vous pouvez obtenir de **l'aide supplémentaire** sur le site Web No More Ransom, à l'adresse suivante : [www.nomoreransom.org/fr/index.html](http://www.nomoreransom.org/fr/index.html). Ce site est un outil visant à aider les victimes à récupérer leurs données. Il a été créé par des autorités policières et des entreprises spécialisées en sécurité de l'information à l'échelle mondiale.

## UTILISATEUR D'UN ORDINATEUR PROFESSIONNEL

### SIGNALEZ-LES !

#### Comment mon entreprise doit-elle réagir?

Cessez immédiatement d'utiliser votre ordinateur. Si vous y avez accès, consultez votre service de TI ou un spécialiste de la TI.

Les infrastructures essentielles, les entreprises et les gouvernements provinciaux, territoriaux et municipaux doivent immédiatement signaler l'incident auprès du **Centre canadien de réponse aux incidents cybernétiques (CCRIC)** par courriel ([ps.cyberincident-cyberincident.sp@canada.ca](mailto:ps.cyberincident-cyberincident.sp@canada.ca)) ou consulter le site <https://www.publicsafety.gc.ca/cnt/ntnl-scr/cbr-scr/ccirc-ccric-fr.aspx> pour obtenir de plus amples renseignements. Le CCRIC contribue aux mesures d'atténuation et de prévention.

Nous vous encourageons à entamer une enquête criminelle en signalant l'incident au service de police local. Informez-en ensuite le CCRIC. N'oubliez pas qu'il est important de signaler tous les incidents; ils constituent un outil précieux pour les enquêteurs.

Vous pouvez également communiquer avec le **Centre antifraude du Canada (CAFC)** en signalant l'incident en ligne en tout temps à [www.antifraudcentre-centreantifraude.ca](http://www.antifraudcentre-centreantifraude.ca). Cliquez sur l'onglet « Signaler un incident », puis sur le lien menant au « Système de signalement des fraudes » ou appelez le CAFC en composant le 1-888-495-8501, de 8 h 30 à 17 h (HNE), du lundi au vendredi.



### Nous vous encourageons fortement à **NE PAS PAYER LA RANÇON** pour les raisons suivantes :

- Rien ne garantit que vos données soient récupérées.
- Vous risquez d'être à nouveau victime d'extorsion après le paiement de la rançon initiale.
- Vous pouvez faire de vous une cible future.
- L'extorsion par l'entremise d'un rançongiciel est une infraction criminelle. L'argent que vous enverrez à la personne responsable servira à financer des criminels ou des organisations criminelles et les motivera à faire d'autres victimes.

Nous savons qu'il peut y avoir des raisons légitimes de payer la rançon, comme le risque éventuel de ne plus avoir accès à vos données, car vous n'avez pas de sauvegarde. Nous vous encourageons à signaler tous les incidents, même si vous avez payé la rançon exigée par les extorqueurs.

### Lignes directrices supplémentaires :

<https://www.pensezcybersecurite.gc.ca/cnt/prtct-yrslf/index-fr.aspx>

<https://www.cyber.nj.gov/threat-profiles/ransomware/>

### Lignes directrices supplémentaires :

Guide Pensez cybersécurité pour les petites et moyennes entreprises

<https://www.pensezcybersecurite.gc.ca/cnt/rsrscs/pblctns/sml-bns-gd/index-fr.aspx>

Conseils US-CERT

<https://www.us-cert.gov/ncas/tips> (en anglais seulement)

Guide du National Institute of Standards and Technology :

<http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf> (en anglais seulement)

### En consultation avec :



CALGARY  
POLICE  
SERVICE