# AIDE-MÉMOIRE

# SE PROTÉGER CONTRE LES RANÇONGICIELS

## Objectif du document

L'objectif de ce document est de fournir des conseils et des outils pour se protéger contre les rançongiciels.

Les cybercriminels savent que les entreprises sont plus susceptibles de payer la rançon, car les données sont vitales pour la survie de l'organisation.

## Les types de rançongiciels

- **Rançongiciel chiffrant**. Il chiffre les fichiers et les répertoires personnels.
- **Rançongiciel bloquant**. Il bloque l'écran de l'ordinateur et réclame une rançon.
- **Rançongiciel Master Boot Record (MBR**). Il modifie une portion du disque dure du système d'exploitation pour interrompre le processus de démarrage.
- **Rançongiciel ciblant les serveurs web**. Il chiffre des fichiers sur leur espace de stockage en exploitant une vulnérabilité dans le gestionnaire de contenu (CMS).
- **Rançongiciel mobile**. Il bloque le téléphone en se faisant passer pour des applications connues.

## Mesures préventives

1. **Sauvegarder**. Avoir un système de restauration en place afin d'empêcher qu'un rançongiciel détruise vos données personnelles pour toujours. Il est recommandé de faire deux copies de sauvegarde ; une dans un service d'infonuagique et une autre sur un support physique (ex. : disque dur, clé USB, ordinateur secondaire)
2. **Utiliser un antivirus.**
3. **Maintenir à jour les logiciels et l'OS de votre ordinateur.**
4. **Soyez vigilants.** Ne jamais ouvrir la pièce jointe d'un courriel d'une personne que vous ne connaissez pas. Ne cliquez pas sur des hyperliens dans les courriels si vous n'êtes pas sûrs.
5. **Vérifier l'extension du fichier avant de l'ouvrir.** Restez vigilants ses extensions du type .exe, .vbs, js, hta, docx, docm, doc, chm, jar, com, ocx, bat, cmd, pdf, cpl, et .scr.
6. En cas de comportement inconnu sur votre ordinateur**, déconnectez-le d'Internet ou de tout autre connexion réseau** afin d'empêcher l'infection de se propager.

## En cas d’affetion

Il est fortement recommandé de ne pas payer la rançon, même s’il plus coûteux de restaurer les sauvegardes que de payer le montant de la rançon. En envoyant de l’argent aux criminels, non seulement vous confirmez que les rançongiciels fonctionnent, mais vous avez aucune garanti que la clé de déchiffrement vous sera communiquée.

1. Identifier le type de rançongiciel qui affecte votre système à l’aide du Crtypto Sheriff (gratuit) - https://www.nomoreransom.org/fr/crypto-sheriff.php

2. Restaurer votre poste avec une copie de sauvegarde qui ne contient pas le logiciel malveillant.

Pour les premières générations de rançongiciels, il est possible de déchiffrer vos fichiers avec les outils disponibles sur le site No More Ransomware: https://www.nomoreransom.org/fr/decryption-tools.html

## Compléments d’information

Le site No More Ransomware : https://www.nomoreransom.org/fr/prevention-advice.html