

# Comment protéger vos données contre les attaques de rançongiciel

Les rançongiciels (ransomware) peuvent prendre différentes formes. Qu'il s'agisse d'un courriel d'hameçonnage, d'une clé USB contenant des fichiers malveillants ou de fichiers téléchargés sur Internet, un rançongiciel prend le contrôle de votre ordinateur et garde vos données en otage. Voici quelques trucs pour protéger vos données des attaques d'hameçonnage.



1

## INSPECTER L'URL DU SITE WEB

Les sites Web ou les courriels d'hameçonnage qui ciblent les utilisateurs avec des fichiers de rançongiciel proviennent d'adresses qui contiennent des éléments suspects, comme des caractères changés ou ajoutés, ou des fautes d'orthographe intentionnelles dans des mots communs.

## NE JAMAIS CLIQUER SUR DES LIENS NON VÉRIFIÉS OU SUSPECTS

Évitez de cliquer sur des liens qui proviennent d'un expéditeur inconnu ou qui mènent vers un site Web inconnu. Les téléchargements qui débutent après avoir cliqué sur un lien peuvent contaminer votre appareil.

2

3

## NE PAS OUVRIR LES PIÈCES JOINTES DOUTEUSES

N'ouvrez jamais les pièces jointes provenant d'expéditeurs suspects. Évitez d'activer des macros dans des logiciels de productivité ou des programmes actifs s'ils ne proviennent pas d'une source fiable.

## VISITER SEULEMENT DES SITES DE CONFIANCE

Évitez de visiter ou de télécharger des fichiers provenant de sites Web non vérifiés ou non sécurisés. Téléchargez seulement des fichiers ou des programmes provenant de sites Web officiels. Recherchez les lettres « https » ou un symbole de bouclier ou de cadenas au début de la barre d'adresse pour vous assurer que le site visité est considéré sécuritaire.

4

5

## ÉVITER D'UTILISER DES PÉRIPHÉRIQUES DE STOCKAGE INCONNUS OU NON AUTORISÉS

Les supports de stockage physiques, comme les clés USB à mémoire flash ou les disques durs de sauvegarde automatique, peuvent également contaminer votre appareil si vous ne connaissez pas leur provenance. Les cybercriminels peuvent placer des supports de stockage dans des endroits publics pour vous inciter à les utiliser.

## EFFECTUER RÉGULIÈREMENT UN BALAYAGE ET UNE MISE À JOUR DU LOGICIEL SYSTÈME

En effectuant régulièrement des balayages antivirus et en gardant votre logiciel système à jour, vous contribuerez à protéger vos données des rançongiciels. Il est plus difficile pour les cybercriminels d'exploiter les failles du système lorsque les correctifs de sécurité sont installés.

6

7

## PROTÉGER LES FICHIERS

Enregistrez vos fichiers à des endroits qui font régulièrement l'objet d'une sauvegarde automatique afin d'assurer leur récupération en cas de contamination par un rançongiciel. Ne payez jamais de rançon pour récupérer vos fichiers et communiquez toujours avec votre service de soutien TI en cas d'infection.