A+ A-

Cinq conseils pour se prémunir contre les rançongiciels (ransomware)

Par **Bercy Infos < https://economie.gouv.fr/entreprises/bercy-infos-qui-sommes-nous>** , le 03/03/2023 - **Sécurité numérique** LECTURE : 3 MINUTES

Vous avez reçu un message douteux contenant des pièces jointes ? Vous avez retrouvé par hasard une clé USB ? Gare aux rançongiciels (ou « ransomware ») ! Vos données peuvent-être chiffrées et prises en otage contre rançon. Voici cinq conseils pour minimiser les risques.

~~Qu'est ce qu'un rançongiciel ?~~

D'après le site **cybermalveillance.gouv.fr < https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares>** , un rançongiciel (*ransomware* en anglais) est un logiciel malveillant qui bloque l'accès à l'ordinateur ou aux fichiers des victimes et qui leur réclame le paiement d'une rançon pour en obtenir à nouveau l'accès.

Conseil n°1 : effectuez des sauvegardes régulières de vos données

Pensez à régulièrement sauvegarder vos données et de votre système ! Vous pourrez ainsi récupérer les récupérer en cas d'attaque.

Rendez-vous sur le site cybermalveillance.gouv.fr < https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes> pour tout savoir sur les bonnes pratiques en matière de sauvegarde.

Conseil n°2 : n'ouvrez pas les messages dont la provenance ou la forme est douteuse

Ne vous laissez pas tromper par un simple logo. Pire, le hacker peut avoir récupéré certaines de vos données préalablement (les noms de vos clients par exemple) et créé des adresses de messagerie ressemblant à un détail près à celles de vos interlocuteurs habituels.

Restez donc très vigilants ! Certains messages paraissent tout à fait authentiques.

Apprenez à identifier les courriels piégés (ou autres formes de récupération de vos données) sur le site de l'**Agence nationale de la sécurité des systèmes d'information < http://www.ssi.gouv.fr/entreprise/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel/>** (ANSSI).

Vous avez un doute ? Contactez l'expéditeur par un autre canal de communication.

Conseil n°3 : apprenez à identifier les extensions douteuses des fichiers

Vous recevez habituellement des fichiers en .doc ou .mp4 (par exemple) et le fichier du message dont vous avez un doute se finit par un autre type d'extension ? Ne les ouvrez surtout pas !

Voici quelques exemples d'extensions douteuses : .pif, .com, .bat, .exe, .vbs, .lnk, etc.

Attention à l'ouverture de pièces jointes de type .scr ou .cab. Comme le rappelle l'**Agence nationale de la sécurité des systèmes d'information (ANSSI) < https://www.ssi.gouv.fr/actualite/alerte-campagne-de-rancongiciel/>** , il s'agit des extensions de compression des campagnes CTB-Locker sévissant chez les particuliers, les PME ou les mairies.

Conseil n° 4 : mettez à jour vos principaux outils

On ne vous le dira jamais assez : traitement de texte, lecteur PDF, navigateur mais aussi antivirus… Veillez à mettre à jour vos outils régulièrement.

Si possible, désactivez les macros des solutions de bureautique qui permettent d'effectuer des tâches de manière automatisée. Cette règle évitera en effet la propagation des rançongiciels via les vulnérabilités des applications.

Considérez que, d'une manière générale, les systèmes d'exploitation en fin de vie, qui ne sont plus mis à jour, donnent aux attaquants un moyen d'accès plus facile à vos systèmes.

Conseil n° 5 : utilisez un compte « utilisateur » plutôt qu'un compte « administrateur »

Évitez de naviguer depuis un compte administrateur. L'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés de votre ordinateur.

Préférez l'utilisation d'un compte utilisateur. Cela ralentira, voire dissuadera le voleur dans ses actions malveillantes.

À savoir

L'Agence nationale de la sécurité des systèmes d'information (**ANSSI < https://www.ssi.gouv.fr/>**) a publié, en partenariat avec la Direction générale des Entreprises (**DGE < https://www.entreprises.gouv.fr/fr>**), la Confédération des petites et moyennes entreprises (**CPME < https://www.cpme.fr/>**) et **France Num < https://www.francenum.gouv.fr/>** , **un nouveau guide destiné aux TPE et aux PME**. Réalisée avec le soutien du dispositif **Cybermalveillance.gouv.fr < https://www.cybermalveillance.gouv.fr/>** , cette publication propose des **réponses accessibles à treize questions essentielles pour la sécurité de ces entreprises**
Consultez le guide La cybersécurité pour les TPE/PME en treize questions < https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-treize-questions/>

Ces contenus peuvent aussi vous intéresser

- **Sécurité de vos données : quelles sont les méthodes de piratage les plus courantes ?**
- **Entreprises : quelles règles de cybersécurité appliquer ?**
- **Piratage : bénéficiez d'un accompagnement sur-mesure avec cybermalveillance.gouv.fr**
- **Dix règles pour vous prémunir contre le piratage de vos données personnelles**

Tout savoir sur les attaques par rançonlogiciel

- **Cybersécurité : attention aux rançongiciels < https://www.interieur.gouv.fr/actualites/actu-du-ministere/cybersecurite-attention-aux-rancongiciels>** *sur le site du ministère de l'Intérieur*
- **Rançongiciel ou ransomware, que faire ? < https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares>** *sur le site cybermalveillance.gouv.fr*
- **5 réflexes à avoir lors de la réception d'un courriel < https://www.ssi.gouv.fr/particulier/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel/>** *sur le site de l'ANSSI*
- **État de la menace rançongiciels à l'encontre des entreprises et institutions < https://www.bercynumerique.finances.gouv.fr/etat-de-la-menace-rancongiciels-lencontre-des-entreprises-et-institutions>** *sur Bercy Numérique*

Thématiques : **Sécurité numérique**

Ce sujet vous intéresse ? Chaque jeudi avec la lettre Bercy infos Entreprises, recevez les toutes les dernières actus fiscales, comptables RH et financières… utiles à la gestion de votre activité.

Partager la page