Important

Pour mieux protéger vos appareils contre tout ransomware tel que WannaCrypt, sauvegardez régulièrement vos données, assurez-vous que les mises à jour automatiques sont activées et que vos appareils sont à jour.

- Dans Windows 10, accédez à **Paramètres** > **Mise à jour et sécurité**. Vous pouvez alors vérifier l'tat de mise à jour de votre appareil.
- Dans Windows 8.1, accédez à **Paramètres** > **Modifier les paramètres du PC** > **Mise à jour et récupération**.
- Dans Windows 7, accédez à **Panneau de configuration** > **Windows Update**.

Si l'état de mise à jour de votre appareil indique que ce dernier est à jour, vous n'avez rien à faire. Si tel n'est pas le cas, Microsoft vous recommande d'installer immédiatement le Bulletin de sécurité Microsoft MS17-010.

Find out more about the WannaCrypt ransomware virus.

Un ransomware est un programme malveillant qui restreint l'accès à votre PC (voire même vous empêche de l'utiliser) ou chiffre vos fichiers. Il vous oblige ensuite à verser de l'argent (une rançon) pour retrouver l'accès à ces derniers.
Vous pouvez être infecté par un ransomware de l'une des façons suivantes :

- En visitant les sites web dangereux, suspects ou frauduleux
- En ouvrant des e-mails et des pièces jointes que vous n'attendiez pas ou provenant de personnes que vous ne connaissez pas
- En ouvrant des liens malveillants ou corrompus dans les e-mails, Facebook, Twitter et d'autres publication de réseaux sociaux, ou dans des sessions de conversation instantanée, comme dans Skype

Vous pouvez souvent reconnaître un e-mail ou une page Web frauduleux, car ils contiennent des fautes d'orthographe ou ont un aspect inhabituel. Cherchez une façon étrange d'orthographier les noms de société (comme « PayePal » au lieu de « PayPal ») ou des espaces, symboles ou ponctuation inhabituels (comme le « ServiceiTunesCustomer » au lieu de « Service iTunes Customer »).
Un ransomware peut cibler n'importe quel PC, qu'il s'agisse d'un ordinateur personnel, d'un PC sur un réseau d'entreprise ou de serveurs utilisés par un organisme public.

Comment puis-je protéger mon PC ?

Si vous venez d'acheter un nouveau PC ou si vous utilisez le même depuis longtemps, il existe différentes façons de renforcer sa sécurité :

- Assurez-vous que votre PC est à jour avec la dernière version de Windows. En savoir plus sur Windows Update.
- Activez l'Antivirus Windows Defender pour vous protéger contre les virus et programmes malveillants.
- Activez l'historique des fichiers si celui-ci n'a pas déjà été activé par le fabricant de votre PC. En savoir plus sur l'historique des fichiers.
- Sauvegardez le contenu sur votre PC régulièrement. En savoir plus sur la sauvegarde de vos fichiers.
- Tirez parti de l'espace de stockage pour conserver deux copies des données de votre PC. En savoir plus sur l'espace de stockage.

Si vous pensez avoir été infecté

Utilisez des logiciels anti-programme malveillant, comme Antivirus Windows Defender, chaque fois que vous craignez que votre PC risque d'être infecté (par exemple, si vous entendez parler d'un nouveau logiciel malveillant dans les actualités ou si vous constatez un fonctionnement inhabituel de votre PC). En savoir plus sur Antivirus Windows Defender.

Si vous êtes infecté par un ransomware

Malheureusement, une infection par un ransomware ne se détecte que lorsqu'une notification apparaît, soit dans une fenêtre, une application ou un message plein écran, vous demandant de l'argent pour récupérer l'accès à votre PC ou à vos fichiers. Ces messages s'affichent souvent après chiffrement de vos fichiers.
Essayez de nettoyer complètement votre PC avec Windows Defender hors ligne. Vous devez effectuer cette opération avant d'essayer de récupérer vos fichiers. Consultez également Sauvegarde et restauration dans Windows 10 pour obtenir de l'aide sur la sauvegarde et la récupération de fichiers pour votre version de Windows.

Ne payez rien pour récupérer vos fichiers. Même si vous payez la rançon, il n'existe aucune garantie que vous pourrez accéder de nouveau à votre PC ou à vos fichiers.

Que faire si vous avez déjà payé ?

Si vous avez déjà payé la rançon, contactez immédiatement votre banque et les autorités locales. Si vous avez payé avec une carte de crédit, votre banque peut être en mesure de bloquer la transaction et de vous rembourser.

Vous pouvez également consulter les sites web gouvernementaux suivants de signalement des fraudes et des escroqueries :

- En Australie, consultez le site web SCAMwatch.
- Au Canada, consultez le site web du Centre antifraude du Canada.
- En France, consultez le site web de l'Agence nationale de la sécurité des systèmes d'information.
- En Allemagne, consultez le site web Bundesamt für Sicherheit in der Informationstechnik.
- En Irlande, consultez le site web An Garda Síochána.
- En Nouvelle-Zélande, consultez le site web Consumer Affairs Scams.
- Au Royaume-Uni, consultez le site web Action Fraud.
- Aux États-Unis, consultez le site web On Guard Online.

Si votre pays ou région n'est pas répertorié ici, Microsoft vous recommande de contacter la police nationale ou l'autorité en charge des communications de votre pays ou région.

Pour obtenir une vue d'ensemble illustrée des ransomware et découvrir ce que vous pouvez faire pour vous protéger, visitez la page The 5Ws and 1H of ransomware.

Si vous êtes dans une entreprise, consultez le site du Centre de protection Microsoft contre les programmes malveillants pour obtenir des informations détaillées sur les ransomware.

Propriétés

ID d'article : 4013550 - Dernière mise à jour : 30 mai 2017 - Révision : 4

Les informations contenues dans cet article s'appliquent au(x) produit(s) suivant(s):

Windows 10, Windows 7, Windows 8.1