ProtÃ©ger sa Maison des Attaques NumÃ©riques : 10 Astuces
Internet
PostÃ© par : JulieM
PubliÃ©e le : 19/10/2017 13:00:00

Les maisons modernes connectÃ©es engendrent des risques â les rÃ©seaux wi-fi non protÃ©gÃ©s peuvent Ãªtre piratÃ©s et les consÃ©quences sont lourdes. Le danger est d'autant plus important lorsque que la maison est Ã©quipÃ©e avec de nombreux appareils IdO (Internet des Objets).

En piratant un seul de ces objets, un hacker peut avoir accÃ¨s au rÃ©seau entier et contrÃ´ler Ã distance les autres objets connectÃ©s. Un voleur d'identitÃ© peut Ã©galement voler vos comptes bancaires, votre numÃ©ro de sÃ©curitÃ© sociale ou d'autres informations confidentielles sensibles.



Certaines mÃ©thodes de diagnostic et de rÃ©paration des rÃ©seaux peuvent se convertir en appareils de piratage puissants et faciles d'utilisation lorsqu'ils tombent entre les mains de criminels.

Le Â« sniffing Â», par exemple, est une mÃ©thode qui permet d'afficher les donnÃ©es prÃ©sentes sur le rÃ©seau d'un utilisateur en configurant prÃ©alablement le rÃ©seau pour que les informations transitent via l'ordinateur d'un hacker.

Â« Il n'est pas impossible que les nouveaux appareils connectÃ©s rencontrent davantage de problÃ¨mes que les ordinateurs, puisque ces derniers sont mieux contrÃ´lÃ©s en matiÃ¨re de sÃ©curitÃ©.

Les fabricants continuent de produire beaucoup d'objets connectÃ©s, sans toujours prendre le

temps d'utiliser les technologies les plus fiables Â», a dÃ©clarÃ© Marty P. Kamden, CMO de NordVPN (RÃ©seau PrivÃ© Virtuel). Â« Votre appareil le plus vulnÃ©rable pourrait tout Ã fait Ãªtre une camÃ©ra ou une imprimante connectÃ©e au rÃ©seau.

Un seul appareil peut compromettre la sÃ©curitÃ© de tout le rÃ©seau. Les objets connectÃ©s IdO comportant les risques les plus sÃ©rieux sont les voitures sans conducteur et les appareils mÃ©dicaux. Â»

NordVPN vous offre ses conseils de sÃ©curitÃ© fondamentaux pour protÃ©ger le rÃ©seau de toutes les maisons.

1. Utilisez des logiciels antivirus. Avant toute chose, pensez Ã utilisez un antivirus fiable. Malheureusement, les avis des experts divergent sur la question : il revient donc aux utilisateurs de chercher un antivirus efficace, en lequel ils ont confiance. Tous les antivirus ne sont pas sÃ»rs, comme le prouve l'incident rÃ©cent avec l'antivirus russe Kaspersky Lab, que des hackers russes ont utilisÃ© pour obtenir des fichiers de la NSA.

2. Utilisez un pare-feu. Le routeur doit contenir un logiciel de pare-feu Ã jour pour se prÃ©munir contre de nouveaux malwares qui pourraient Ãªtre installÃ©s Ã distance par des hackers. Ces logiciels malveillants sont notamment Ã mÃªme de voler vos donnÃ©es personnelles.

3. ParamÃ©trez la double authentification sur vos comptes en ligne. Lorsque vous avez activÃ© la double authentification sur vos comptes en ligne, il devient plus difficile pour les fraudeurs de voler vos informations personnelles. Bien que cette solution ne constitue pas une solution dÃ©finitive contre les pirates, il vaut tout de mÃªme mieux s'enregistrer avec une double authentification que sans.

4. Utilisez des portefeuilles Ã©lectroniques pour effectuer des achats en ligne. Les portefeuilles Ã©lectroniques sont rÃ©putÃ©s pour faciliter et sÃ©curiser les achats en ligne. Les gestionnaires de paiement tels que Apple Pay, PayPal, Google Wallet et d'autres encore commencent Ã implÃ©menter cette mÃ©thode de paiement en un clic dans leurs services.

5. Installez un VPN. Les VPNs sont une des mÃ©thodes les plus efficaces pour sÃ©curiser vos rÃ©seaux privÃ©s et les retirer Ã la vue des regards indiscrets, en chiffrant les donnÃ©es qui transitent entre Internet et le serveur VPN. NordVPN utilise des protocoles de chiffrement avancÃ©s, offre une couverture mondiale et bÃ©nÃ©ficie d'une politique anti-log.

6. Changez les informations de connexion par dÃ©faut de votre routeur. Il est trÃ¨s facile de modifier les nom d'utilisateur et mot-de-passe par dÃ©faut d'un routeur â□□ et cela rend la tÃ¢che plus complexe pour les hackers. AprÃ¨s toute modification, pensez Ã vous dÃ©connecter.

7. Ne cliquez pas sur les mails suspects. Tous les mails de hameÃ§onnage contiennent des piÃ¨ces jointes et paraissent provenir de vos connaissances. Il suffit d'un clic sur un lien prÃ©sent dans un mail d'apparence fiable pour exposer le rÃ©seau du foyer tout entier Ã la menace d'un hack.

8. Faites systÃ©matiquement les mises Ã jour de sÃ©curitÃ© sur vos appareils connectÃ©s. Les systÃ¨mes d'exploitation de vos ordinateurs personnels, tablettes, smartphones et autres appareils doivent Ãªtre Ã jour.

9. VÃ©rifiez bien les paramÃ¨tres de sÃ©curitÃ© de tous les appareils que vous connectez chez vous. De nouveaux appareils tels qu'un appareil photo ou une imprimante ont beau fonctionner efficacement et Ãªtre performants, il est important d'Ãªtre attentif Ã leurs paramÃ¨tres de sÃ©curitÃ©. Il est gÃ©nÃ©ralement conseillÃ© d'Ã©teindre leurs interfaces web.

10. CrÃ©ez un nouveau rÃ©seau. CrÃ©ez un autre rÃ©seau â la plupart des routeurs offrent la possibilitÃ© de paramÃ©trer un rÃ©seau invitÃ©. Bannissez les objets connectÃ©s IdO les moins fiables du nouveau rÃ©seau.

Â