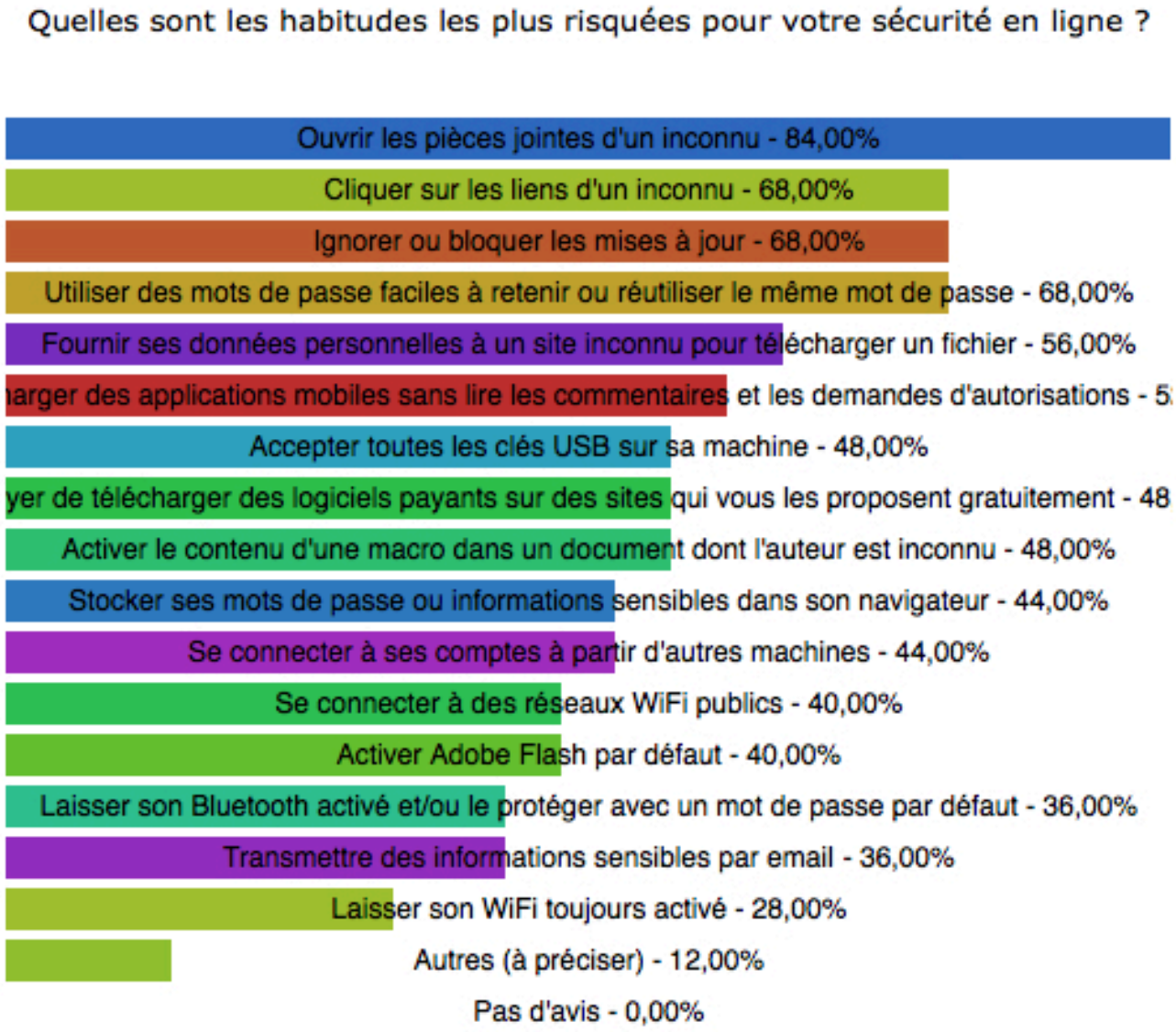
Seize petites habitudes à bannir pour éviter d'être exposé à des risques de sécurité énormes

Lesquelles sont les plus risquées ?

Le 20 décembre 2016, par Michael Guilloux, Chroniqueur Actualités



Avec la sophistication des attaques des pirates informatiques, avoir le minimum de sécurité est aujourd'hui un luxe, mais que tout le monde peut s'offrir, à condition d'avoir du bon sens et adopter de bonnes pratiques. De nombreux rapports sur les menaces qui guettent les utilisateurs montrent en effet que ces derniers sont très souvent sollicités, d'une manière ou d'une autre, par les pirates pour exécuter leurs attaques. Ce qui signifie que le comportement de l'utilisateur lui-même peut aider ou bloquer les cybercriminels dans la mise en œuvre de leurs attaques. Quelles sont donc les petites habitudes à bannir pour éviter d'être exposé à des risques de sécurité énormes ? La liste n'est certainement pas exhaustive, mais on peut citer les éléments suivants :

1. Activer Adobe Flash par défaut. Les problèmes de sécurité de Flash ne sont plus à rappeler. Les éditeurs de navigateurs invitent les utilisateurs à fuir Flash comme la peste. Il est donc recommandé de ne pas l'activer sauf si c'est vraiment nécessaire.

2. Utiliser des mots de passe faciles à retenir ou réutiliser le même mot de passe. Traditionnellement, le choix d'un mot de passe résulte d'un arbitrage entre un niveau de complexité acceptable et un mot de passe facile à retenir. Très souvent, les utilisateurs préfèrent un mot de passe facile à retenir, qui peuvent être également faciles à devenir par quelqu'un d'autre. À défaut d'utiliser des mots de passe faciles à retenir, d'autres préfèrent un mot de passe complexe, mais utilisé pour tous leurs comptes, dans le même but de pouvoir s'en souvenir plus facilement. Le risque est que les pirates sont conscients de ce comportement chez les utilisateurs. Quand ils réussissent à trouver un mot de passe pour un compte donné, ils le testent donc sur les différents comptes de l'utilisateur.

3. Stocker ses mots de passe ou informations de carte de crédit dans son navigateur web pour éviter de les saisir à chaque fois. Les navigateurs offrent la possibilité d'enregistrer vos informations dans les formulaires des sites web. Mais pour vos informations sensibles ou mots de passe, il est préférable de ne pas les enregistrer dans le navigateur. D'ailleurs, cela vous permet de les retenir de sorte que si vous utilisez un autre navigateur ou une autre machine, vous n'ayez pas de difficulté à vous connecter à vos comptes.

4. Ignorer ou bloquer les mises à jour, parce qu'elles arrivent toujours au moment où vous avez un travail urgent à terminer. En agissant ainsi, vous laissez vos appareils vulnérables. Les mises à jour ne viennent pas toujours pour ajouter de nouvelles fonctionnalités dont vous n'avez pas nécessairement besoin. La plupart du temps, elles viennent pour offrir plus de protection à votre appareil.

5. Ouvrir les pièces jointes de personnes que vous ne connaissez pas. Personne ne sait ce qui se cache derrière une pièce jointe. Il peut s'agir d'une menace soigneusement conçue pour infecter votre machine. Il faut donc éviter de les ouvrir quand vous ne connaissez pas les expéditeurs. D'ailleurs, même les pièces jointes qui viennent de vos amis ne vous offrent pas de garantie de sécurité à 100 %.

6. Cliquer sur les liens de personnes que vous ne connaissez pas. Les liens sont également l'une des manières les fréquentes de déguiser une menace. Ils peuvent vous rediriger vers des sites compromis où un malware sera téléchargé silencieusement sur votre machine.

7. Transmettre des informations sensibles comme des données de cartes de crédit par email. Aucun service de messagerie n'est sécurisé, même si certains le sont plus que d'autres. Il faut donc avoir en tête que minimiser la quantité d'informations sensibles et de données dans les courriels est nécessaire pour éviter que ces données se retrouvent dans les mains de la mauvaise personne.

8. Activer le contenu d'une macro dans un document MS Word ou Excel dont vous ne connaissez pas l'auteur. Les macros ont été et continuent d'être d'importants vecteurs d'attaques. C'est pour cela qu'un avertissement est donné à l'utilisateur à l'ouverture d'un document qui les contient. Si ne vous ne connaissez pas l'auteur du document, vous devrez donc éviter autant que vous le pouvez d'activer le contenu.

9. Se connecter à des réseaux WiFi publics. On ne peut pas savoir qui peut se trouver sur un réseau public, peut-être un malfaiteur attendant de trouver une proie. Il faut donc éviter autant que possible de se connecter aux réseaux WiFi publics.

10. Accepter toutes les clés USB sur sa machine. La clé USB est un moyen traditionnel pour transférer des fichiers d'une machine à une autre. Mais ce n'est pas seulement les fichiers qui peuvent être transférés, il y aussi les menaces.

11. Laisser son Bluetooth activé et/ou le protéger avec un mot de passe par défaut. Le Bluetooth peut être très facilement piraté. La nature même du média de communication (ondes hertziennes) implique un certain nombre de menaces génériques telles que les écoutes et analyses passives, mais aussi les attaques Man-in-the-middle, qui consistent à intercepter des communications afin de capturer les flux de données entre deux personnes. Il existe également plusieurs failles sur le Bluetooth qui permettent en plus de mener certaines attaques spécifiques. Il est donc nécessaire de n'utiliser le protocole Bluetooth que si nécessaire ; ne pas le laisser activé sans raison ; ne pas laisser son équipement en mode visible ; rejeter toute sollicitation inattendue, mais aussi changer le mot de passe de connexion par défaut.

12. Laisser son WiFi toujours activé, même quand vous ne l'utilisez pas. Les risques ici sont pratiquement les mêmes que ceux auxquels fait face un utilisateur qui laisse son Bluetooth activé alors qu'il ne n'utilise pas. Si le Sniffing permet de rechercher des réseaux disponibles, aujourd'hui, pour de nombreux pirates, cela permet surtout de trouver des réseaux WiFi qu'ils pourront pénétrer de force pour mettre en oeuvre leur attaque. Pour ne pas être piégé par un sniffeur de WiFi, la solution la plus simple est de désactiver son WiFi, donc de ne pas le laisser allumé quand vous ne l'utilisez pas.

13. Se connecter à ses comptes à partir d'autres machines. Votre machine est certainement celle à laquelle vous pouvez faire le plus confiance, puisque vous avez plus ou moins le contrôle de ce que vous y installez. Sur une autre machine, ne sachant pas par exemple si un logiciel espion est installé, il faut éviter de se connecter à des sites où vous fournissez des informations personnelles ou données sensibles.

14. Télécharger des applications mobiles sans lire les commentaires et les demandes d'autorisations. Lire les commentaires, mais également les demandes d'autorisation peuvent dans certains cas vous éviter l'installation d'un logiciel malveillant ou espion sur votre appareil mobile. Par exemple, une application de torche qui demande un accès à vos contacts. Il n'est pas nécessaire d'être assez futé pour savoir qu'il y a quelque chose qui ne tourne pas rond.

15. Fournir ses données personnelles (email, contact, etc.) à un site inconnu pour pouvoir télécharger un super fichier. Certains sites exigent aux internautes de fournir des informations personnelles pour télécharger des fichiers. L'utilisateur peut être tenté de le faire si le fichier lui semble intéressant. Dans la plupart des cas, les sites demandent ces informations à des fins marketing, mais des pirates peuvent également avoir recours à cette technique pour récolter des informations pour leurs futures attaques.

16. Essayer de télécharger des logiciels payants sur des sites qui vous les proposent gratuitement. Il peut être plus rentable de dépenser pour un logiciel que de le télécharger gratuitement. En effet, certains sites sont conçus uniquement pour piéger les utilisateurs à la recherche de logiciels payants au coût zéro, en les proposant ces produits gratuitement au téléchargement. Dans de nombreux cas, cela peut s'accompagner du téléchargement d'un logiciel malveillant, et souvent, sans avoir le produit lui-même. Cela veut dire que les internautes devraient éviter de visiter les sites torrent. Si certains membres peuvent être animés par la volonté d'aider les autres, ce n'est certainement pas le cas pour tout le monde.