Conseils pour l'utilisation du Wi-Fi public en toute sécurité

Des mauvaises personnes acteurs peuvent profiter de vous en ligne. Vous trouverez ci-dessous quelques conseils à suivre si vous devez utiliser le Wi-Fi public.

En raison de l'apparition de l'épidémie de coronavirus et de la fermeture d'entreprises et de bibliothèques, beaucoup d'entre nous passent plus de temps en ligne. Par conséquent, il est possible que nous utilisions le Wi-Fi public pour nous connecter à l'internet. Si vous avez besoin d'utiliser le Wi-Fi public, veuillez tenir compte des recommandations suivantes du chef de la protection des renseignements personnels de l'État afin de protéger vos données :

1. Confirmez que vous avez le bon réseau.

Assurez-vous que vous vous connectez au bon réseau. Des mauvaises personnes peuvent créer des réseaux qui semblent inoffensifs d'après leur nom mais qui, en fait, vous invitent à vous connecter à un réseau configuré pour voir votre navigation sur Internet. Cela signifie que si vous saisissez des identifiants de connexion ou des mots de passe sur des sites web, le pirate pourra voler vos informations. Pour se protéger contre ce risque, lisez très attentivement le nom du réseau et, si possible, demandez à un employé ou vérifiez la signalisation de l'entreprise pour vous assurer que le réseau est authentique.

Les réseaux bien connus, comme ceux des chaînes de café, sont probablement moins suspects parce que l'entreprise exploite le réseau comme un service à leur entreprise. Les réseaux connus sont généralement plus sûrs que les réseaux Wi-Fi gratuits et aléatoires qui peuvent apparaître sur votre téléphone dans un lieu public.

2. Désactiver la connexion automatique.

Plusieurs appareils (smartphones, ordinateurs portables et tablettes) ont des paramètres de connectivité automatiques. Ce paramètre permet à vos appareils de se facilement connecter aux réseaux les plus proches. Cela ne pose pas de problème pour les réseaux de confiance, mais il peut aussi connecter vos appareils à des réseaux qui peuvent être dangereux. Vous pouvez désactiver cette fonction grâce à la fonction de paramétrage de votre appareil. Gardez

ces paramètres désactivés, surtout lorsque vous voyagez dans des endroits peu familiers. Par précaution, vous pouvez cocher la case « oublier le réseau » après avoir utilisé le Wi-Fi public.

Vous devez également surveiller votre Bluetooth lorsque vous êtes dans un lieu public. La connectivité Bluetooth permet à divers appareils de communiquer entre eux, et un pirate peut rechercher des signaux Bluetooth ouverts pour accéder à vos appareils. Désactivez cette fonction sur votre téléphone et les autres appareils lorsque vous vous trouvez dans une zone inconnue.

3. Désactivez le partage de fichiers.

Veillez à désactiver l'option de partage de fichiers lorsque vous êtes en Wi-Fi public. Vous pouvez désactiver le partage de fichiers à partir des préférences système ou du panneau de contrôle, selon votre système d'exploitation. AirDrop est un exemple de fonction de partage de fichiers que vous voudrez désactiver. Certains systèmes d'exploitation comme Windows/PC désactiveront le partage de fichiers pour vous en choisissant l'option « public » lors de la première connexion à un nouveau réseau public.

Étapes pour désactiver le partage de fichiers

Sur un PC :

1. Allez au Centre réseau et de partage.
2. Ensuite Modifiez les paramètres de partage avancés.
3. Désactivez le partage de fichiers et d'imprimantes.

Pour les Macs :

1. Allez dans Préférences Système.
2. Choisissez Partager.
3. Décochez tout.
4. Ensuite, dans le Finder, cliquez sur AirDrop, et sélectionnez Allow me to be discovered by : Personne.

Pour l'iOS, il suffit de trouver AirDrop dans le centre de contrôle et de le désactiver.

4. Utilisez un VPN.

Pensez à installer un réseau privé virtuel (VPN) sur votre appareil. Un VPN est l'option la plus sûre pour la confidentialité numérique sur le Wi-Fi public. Il crypte vos données lorsqu'elles

passent par votre appareil et agit comme un « tunnel » de protection afin que vos données ne soient pas visibles lorsqu'elles passent sur un réseau.

5. Avertissement du FBI concernant les sites web cryptés - HTTPS.

Le FBI a lancé une mise en garde contre les sites web dont l'adresse commence par « https ». La présence de « https » et de l'icône du cadenas est censée indiquer que le trafic web est crypté et que les visiteurs peuvent partager des données en toute sécurité. Cependant, les cybercriminels misent désormais sur la confiance du public en attirant les gens vers des sites web malveillants qui intègrent le protocole https et semblent sécurisés alors qu'ils ne le sont pas.

Les recommandations du FBI :

- Ne vous contentez pas de faire confiance au nom figurant sur un courriel : remettez en question l'intention du contenu du courriel.
- Si vous recevez un courriel suspect avec un lien provenant d'un contact connu, confirmez que le message est légitime en appelant ou en envoyant un courriel au contact. Ne répondez pas directement à un courriel suspect.
- Vérifiez s'il y a des fautes d'orthographe ou des domaines erronés dans un lien (par exemple, si une adresse qui devrait se terminer par « .gov » se termine plutôt par « .com »).
- Ne faites pas confiance à un site web simplement parce qu'il comporte une icône de verrouillage ou « https » dans la barre d'adresse du navigateur.

6. L'accès aux informations sensibles n'est pas recommandé.

Même si vous disposez d'un VPN, il n'est toujours pas recommandé d'accéder à des comptes bancaires personnels, ou à des données personnelles sensibles similaires comme les numéros de sécurité sociale sur des réseaux publics non sécurisés. Les réseaux publics sécurisés peuvent eux aussi être risqués. Faites preuve de discernement si vous devez accéder à ces comptes sur le réseau Wi-Fi public. Pour les transactions financières, il peut être préférable d'utiliser plutôt la fonction « hotspot » de votre smartphone.

7. Sécurisé contre non sécurisé.

Il existe essentiellement deux types de réseaux Wi-Fi publics : Sécurisés et non sécurisés.

Dans la mesure du possible, connectez-vous à des réseaux publics sécurisés. Il est possible de se connecter à un réseau non sécurisé sans aucun type de dispositif de sécurité comme un mot

de passe ou un identifiant. Un réseau sécurisé exige généralement que l'utilisateur accepte les conditions générales, enregistre un compte ou saisisse un mot de passe avant de se connecter au réseau.

8. Gardez votre pare-feu activé.

Si vous utilisez un ordinateur portable, laissez votre pare-feu activé lorsque vous êtes en Wi-Fi public. Un pare-feu agit comme une barrière qui protège votre appareil contre les menaces de logiciels malveillants. Les utilisateurs peuvent désactiver le pare-feu de Windows à cause des pop-ups et des notifications, puis oublier de le réactiver. Si vous voulez le redémarrer sur un PC, allez dans le panneau de configuration, « Système et sécurité » et sélectionnez « Pare-feu Windows ». Si vous êtes un utilisateur Mac, allez dans « Préférences système », puis « Sécurité et confidentialité », puis l'onglet « Pare-feu » pour activer la fonction.

9. Utilisez un antivirus.

Veillez également à installer la dernière version d'un programme antivirus sur votre ordinateur portable. Les programmes antivirus peuvent vous aider à vous protéger lorsque vous utilisez le Wi-Fi public en détectant les logiciels malveillants qui pourraient s'introduire dans votre système lors de l'utilisation du réseau partagé. Une alerte vous avertira si des virus connus sont chargés sur votre appareil ou s'il y a une activité suspecte, une attaque, ou si un logiciel malveillant s'introduit dans votre système.

10. Utilisez une authentification à deux facteurs ou à plusieurs facteurs.

Utilisez l'authentification multifactorielle (MFA) lorsque vous vous connectez à des sites web avec vos informations personnelles. Cela signifie que vous disposez d'un deuxième code de vérification (envoyé par SMS sur votre téléphone ou fourni par une application ou une clé physique) qui vous protège davantage. Ainsi, même si un pirate informatique obtient votre nom d'utilisateur et votre mot de passe, il ne peut pas accéder à vos comptes sans un code d'authentification.

11. Surveillez vos appareils personnels.

Ne laissez pas votre ordinateur portable, tablette ou smartphone sans surveillance dans un lieu ou un véhicule public. Même si vous prenez des précautions sur un réseau Wi-Fi, cela

n'empêchera pas quelqu'un de s'emparer de votre bien ou de fouiller dans vos informations. Soyez conscient de votre environnement et de celui des personnes qui vous entourent.

12. Autres conseils de sécurité en ligne.

Voici quelques conseils pour naviguer en toute sécurité, surtout si vous utilisez une connexion Wi-Fi publique :

- Utilisez des mots de passe complexes.
- Cryptez vos appareils.
- Attention aux e-mails de phishing.
- Faites attention à ce que vous publiez sur les réseaux sociaux. Les pirates informatiques peuvent deviner les mots de passe en raison du trop grand nombre de détails personnels.
- Supprimez les anciennes informations inutiles.
- Si un réseau vous demande d'installer un logiciel supplémentaire ou des extensions de navigateur, ne vous connectez pas.
- Assurez-vous que les derniers patchs et mises à jour de logicielles sont installés sur vos appareils afin de vous protéger contre les problèmes rencontrés.