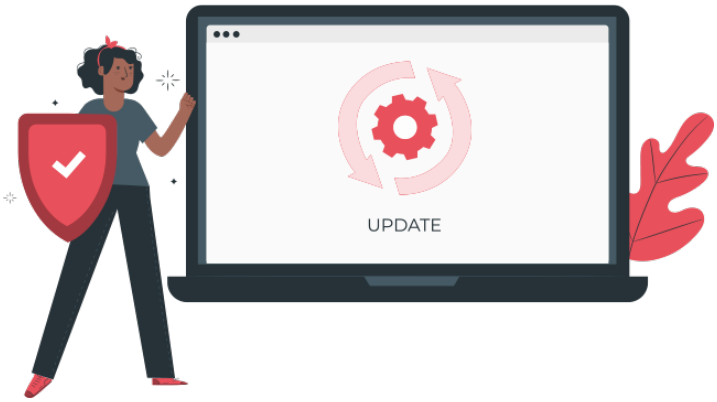
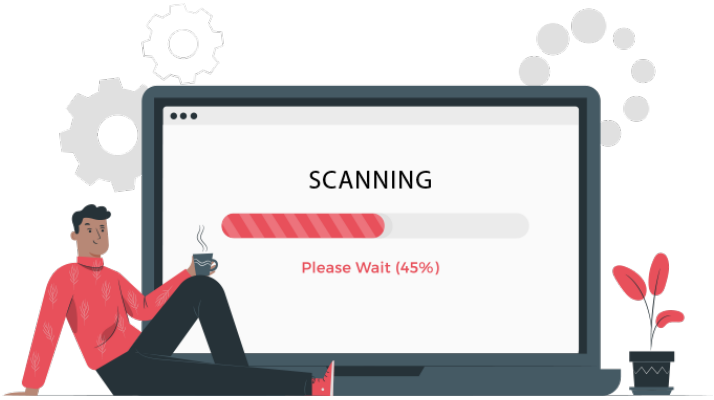
Confidentialité des données

Installez un logiciel antivirus / anti-malveillant. De nombreux ordinateurs personnels ne sont pas protégés contre les virus et les programmes malveillants. Ce type de protection est une première étape indispensable pour protéger votre ordinateur contre les virus.



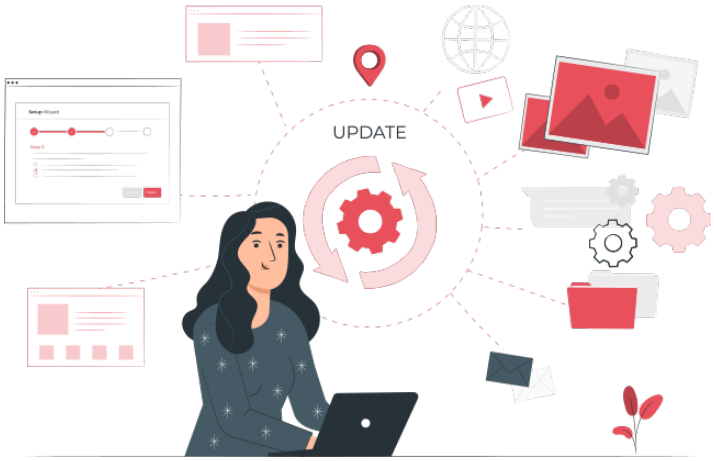
Gardez votre logiciel antivirus à jour. La protection est la première étape; les mises à jour sont le deuxième. Un logiciel antivirus gratuit est mieux que rien, mais n'oubliez pas que ce n'est pas la meilleure solution.

Exécutez des analyses régulièrement avec votre logiciel antivirus. Configurez votre logiciel choisi pour les faire du jour au lendemain si votre ordinateur ne s'éteint pas automatiquement ou ne passe pas en mode hibernation. Une fois par semaine est préférable, mais n'attendez pas plus longtemps entre les analyses.



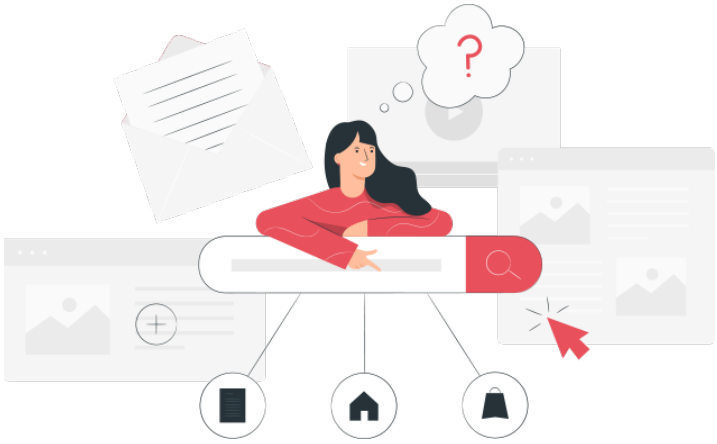
Gardez votre système d'exploitation à jour. Quel que soit le système d'exploitation *(Windows, Mac OS, etc.)*, gardez-le à jour. Les développeurs de systèmes d'exploitation publient fréquemment des correctifs qui corrigent et bouchent les risques de sécurité. Ces correctifs contribuent à sécuriser votre système.

Gardez également vos logiciels à jour. Vous devez non seulement maintenir votre système d'exploitation, mais aussi tous les logiciels exécutés sur votre ordinateur. Les lecteurs de PDF, les applications bureautiques, les éditeurs de photos ont tous des mises à jour de sécurité qui sont envoyées régulièrement. Appliquez-les au fur et à mesure pour sécuriser vos logiciels.



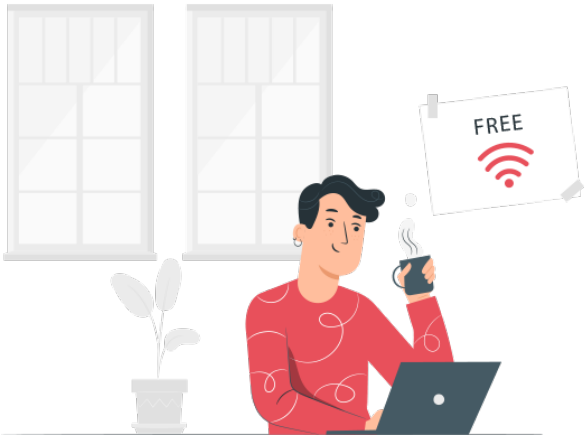
Sécurisez votre réseau domestique. Assurez-vous que votre Wi-Fi nécessite un mot de passe fort pour y accéder. Ne diffusez jamais une connexion Wi-Fi ouverte. Utilisez le cryptage WPA ou WPA2. Ne diffusez pas le nom SSID de Wi-Fi; ajouter plutôt le SSID et le mot de passe manuellement sur chaque appareil autorisé. Si vous avez des invités qui utilisent votre Internet, fournissez un SSID d'invité qui utilise un mot de passe différent.

Pensez avant de cliquer. Évitez les sites Web qui fournissent du matériel piraté. N'ouvrez pas les pièces jointes provenant de quelqu'un ou d'une entreprise que vous ne connaissez pas. Ne cliquez pas sur les liens dans les e-mail non sollicité. Survolez toujours les liens *(en particulier ceux avec un raccourcisseur d'URL)* avant de cliquer pour voir où le lien vous mène réellement.



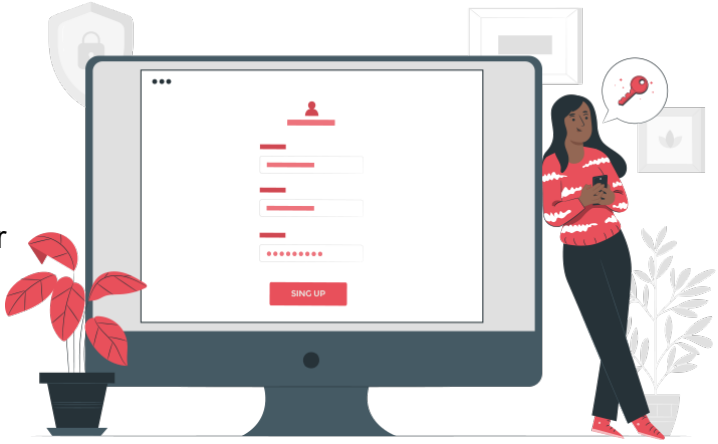
Gardez vos informations personnelles en sécurité. C'est probablement la chose la plus difficile à faire sur Internet. De nombreux pirates accèdent à vos fichiers non pas par la force brute, mais par l'ingénierie sociale. Ils obtiendront suffisamment de vos informations pour accéder à vos comptes en ligne et glaneront plus de vos données personnelles. Ils continueront de compte en compte jusqu'à ce qu'ils aient suffisamment d'informations pour pouvoir accéder à vos données bancaires ou tout simplement voler votre identité. Soyez prudent sur les babillards électroniques et les médias sociaux. Verrouillez tous vos paramètres de confidentialité et évitez d'utiliser votre vrai nom ou votre identité sur les forums de discussion.

N’utilisez pas de Wi-Fi ouvert. Que vous soyez dans un café local, une bibliothèque, et en particulier à l’aéroport, n’utilisez pas le Wi-Fi ouvert “gratuit” *(sans mot de passe, non crypté)*. Pensez-y. Si vous pouvez y accéder sans problème, que pourrait faire un individu malveillant formé?



Faites des sauvegardes de vos fichiers. La meilleure chose que vous puissiez faire est de sauvegarder tous vos fichiers. Idéalement, vous pourrez conserver des copies de vos fichiers et de vos données au moins a trois endroits: où vous travaillez dessus, sur un périphérique de stockage séparé et aussi hors site. Conservez vos fichiers sur votre ordinateur, sauvegardez-les sur un disque dur externe. Sauvegardez-les aussi dans un emplacement différent. Vous pouvez utiliser un service de sauvegarde ou simplement obtenir deux disques durs externes et en garder un au travail, chez un ami, chez un membre de la famille ou dans un coffre-fort.

Utilisez plusieurs mots de passe forts. N’utilisez jamais le même mot de passe, surtout sur votre compte bancaire. Très souvent, nous utilisons la même adresse e-mail ou le même nom d’utilisateur pour tous nos comptes. Ceux-ci sont faciles à voir et à voler. Si vous utilisez le même mot de passe sur tous les systèmes ou à de nombreux endroits et qu’il est découvert, il ne faut que quelques secondes pour pirater vos comptes. Utilisez un mot de passe fort avec des minuscules, des majuscules, des chiffres et des symboles. Choisissez quelque chose qui est facile à retenir mais difficile à deviner. N’utilisez pas de dates ou de noms d’animaux.



Utilisez un bloqueur de fenêtres publicitaires. Les navigateurs Web ont la possibilité d’arrêter l’ouverture de fenêtres contextuelles indésirables et vous permettent de définir la sécurité pour accepter les fenêtres contextuelles souhaitées. Soyez prudent et réfléchissez avant de cliquer sur les liens dans les fenêtres publicitaires. Ne cliquez jamais sur une fenêtre contextuelle qui vous invite à télécharger des logiciels.