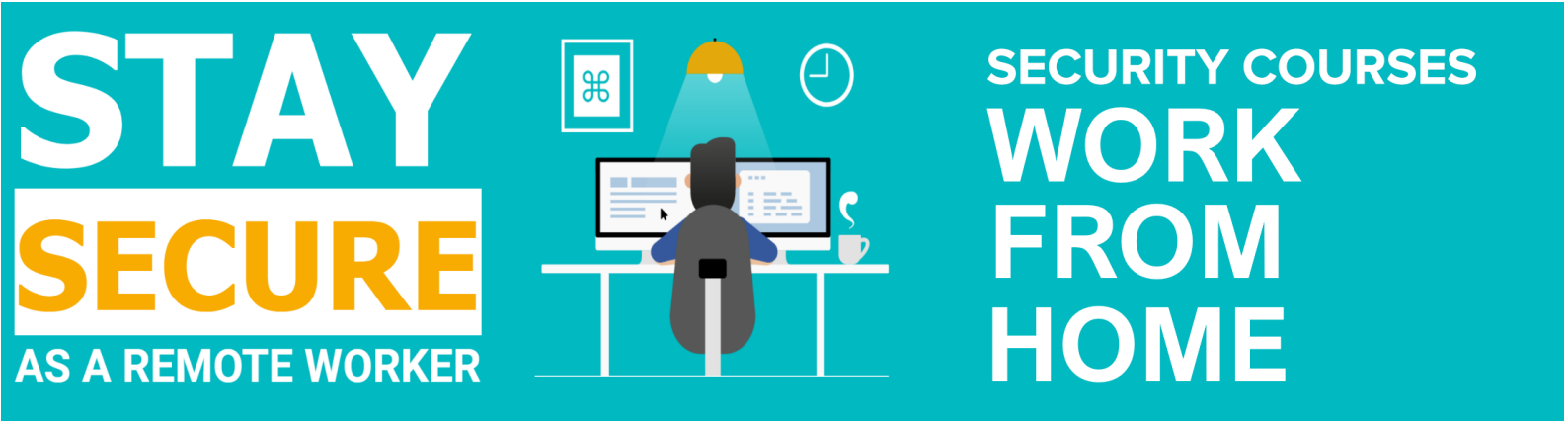


SÉCURISEZ VOTRE PC AVEC CES CONSEILS SUR LA CYBERSÉCURITÉ DE LUCY SECURITY

Que vous utilisiez votre PC principalement pour le travail ou pour votre usage personnel, vous souhaitez que votre ordinateur et son contenu soient sécurisés. Suivez ces mesures pour minimiser les risques que votre ordinateur soit compromis.

✓ CONSEIL 1 : MAINTENEZ TOUS LES LOGICIELS À JOUR

De nombreux problèmes de sécurité proviennent de logiciels qui n'ont pas les dernières mises à jour installées. La plupart des logiciels peuvent installer les mises à jour de manière automatique. Si vous travaillez sur un PC Windows, assurez-vous d'activer la fonction de mise à jour automatique pour que Windows, Microsoft Office et les autres applications Microsoft se maintiennent à jour.

Activez également les mises à jour automatiques pour les applications autres que Microsoft, comme Adobe Acrobat Reader, et les autres programmes que vous utilisez régulièrement.

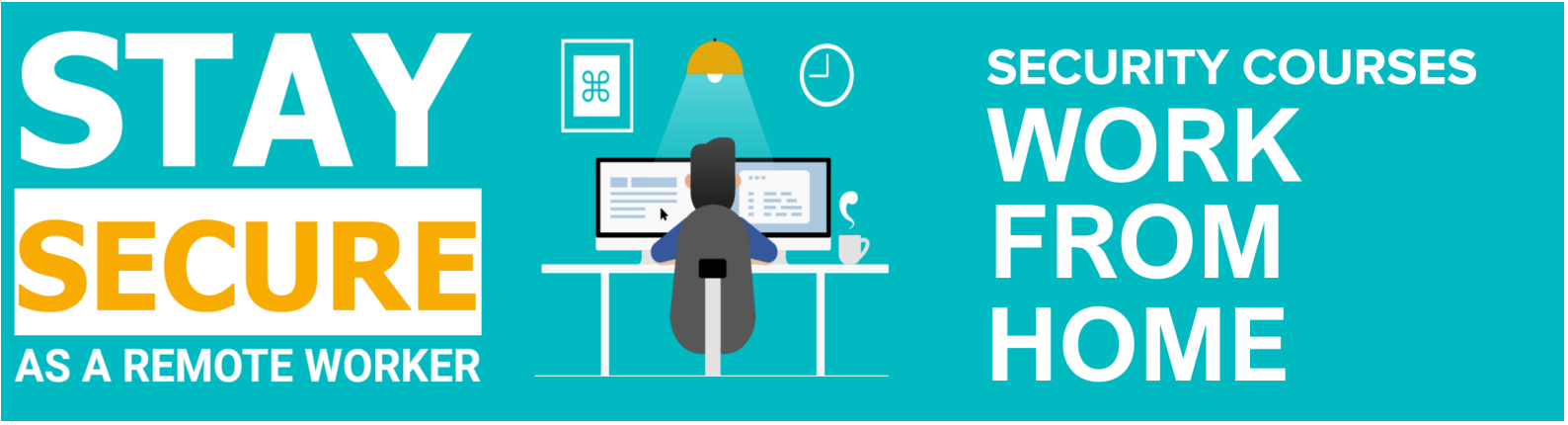
Pour les Macs, utilisez le mécanisme de mise à jour du logiciel qui figure dans les préférences système du menu Apple.

✓ CONSEIL 2 : INSTALLEZ UN LOGICIEL ANTI-VIRUS

Les logiciels anti-virus sont indispensables pour tout le monde, tant pour les utilisateurs de Windows que de Mac. Les applications anti-virus doivent également être mises à jour régulièrement. Si vous utilisez des clés USB ou des disques durs externes, vérifiez toujours qu'ils ne contiennent pas de virus, surtout si le dispositif appartient à un tiers.

✓ CONSEIL 3 : NAVIGUEZ SUR LE WEB EN TOUTE SÉCURITÉ

Évitez de visiter des sites qui offrent un contenu potentiellement illicite. Surtout, ne visitez pas les sites porno (ou tout autre site suspect) ! Car il existe des sites conçus spécialement pour infecter votre ordinateur avec un virus. De nombreux sites porno vous ciblent délibérément. Utilisez un navigateur moderne comme Microsoft Edge ou la dernière version de Chrome, qui peut vous aider à bloquer les sites web malveillants et à empêcher l'exécution de programmes malveillants sur votre ordinateur. En aucun cas, vous ne devez télécharger, installer ou exécuter un logiciel provenant de sources douteuses.



✓ CONSEIL 4 : SÉCURISEZ L'UTILISATION DU COURRIER ÉLECTRONIQUE

Lorsque vous consultez vos e-mails, méfiez-vous des escroqueries qui visent à voler vos informations personnelles ou votre argent. Nombre de ces escroqueries sont connues sous le nom de « escroqueries par hameçonnage ». N'ouvrez pas les pièces jointes suspectes et ne cliquez pas sur les liens inhabituels figurant dans les messages. Ils peuvent apparaître dans des e-mails, des tweets, des posts, des annonces en ligne, des messages ou des pièces jointes, et parfois se dissimulent sous la forme de sources connues et fiables.

✓ CONSEIL 5 : CRÉEZ VOTRE PROPRE COMPTE D'UTILISATEUR AVEC DES DROITS RESTREINTS

Même si vous êtes la seule personne qui utilise votre ordinateur, créez un compte d'utilisateur sans privilèges d'administrateur à partir duquel vous travaillerez. Cela limitera les dommages causés par des logiciels malveillants.

✓ CONSEIL 6 : MAINTENEZ VOTRE MOT DE PASSE SÛR ET DIFFICILE À DEVINER

Utilisez un mot de passe composé d'au moins huit caractères et formé d'une combinaison de chiffres, de lettres majuscules et minuscules. N'utilisez pas de mots ou de combinaisons facilement identifiables comme des anniversaires ou d'autres informations permettant d'établir un lien avec vous. Utilisez également un mot de passe différent pour chaque site web que vous utilisez.

✓ CONSEIL 7 : VÉRIFIEZ VOTRE PARE-FEU

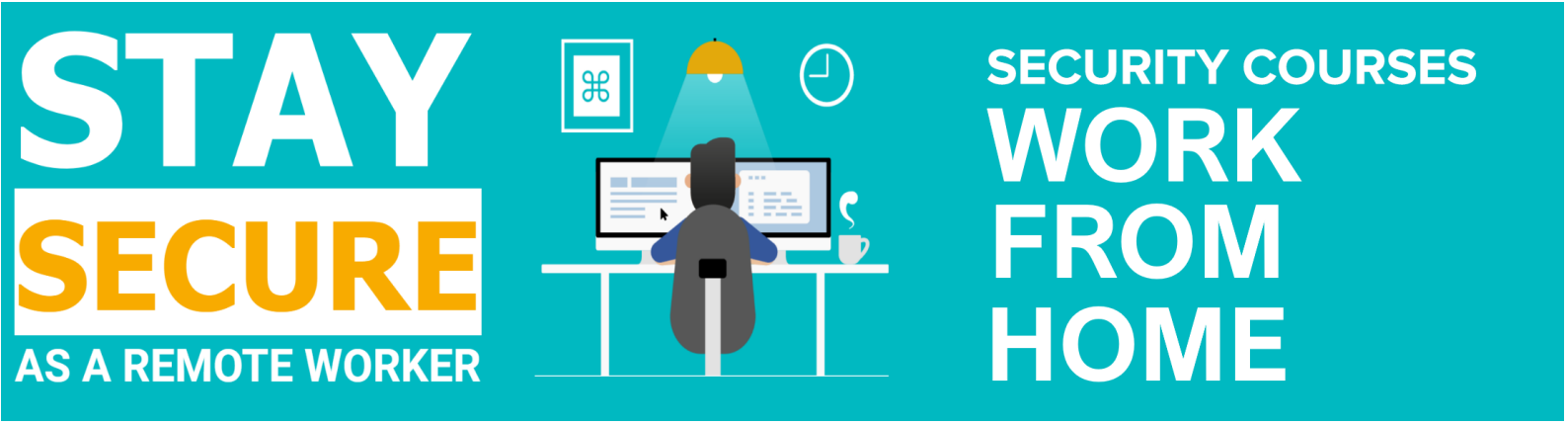
Un pare-feu agit comme une barrière entre votre ordinateur ou votre réseau et Internet. La vérification de votre pare-feu peut paraître compliquée, mais ce n'est pas le cas. Si vous possédez un système basé sur Windows, il vous suffit d'aller dans le panneau de configuration et de taper "pare-feu" dans le champ de recherche. Si votre pare-feu est "activé" ou "connecté", tout va bien.

Si vous possédez un Mac, cliquez sur l'icône Apple de la barre d'outils, allez dans « Préférences système », puis « Sécurité et confidentialité » et enfin « Coupe-feu ».

✓ CONSEIL 8 : ÉVITEZ LES PÉRIPHÉRIQUES À RISQUE

Les clés USB et autres supports de stockage peuvent être truffés de logiciels malveillants. Si vous n'êtes pas propriétaire d'une clé USB ou d'un autre dispositif externe, ne l'utilisez pas.

Pour éviter toute infection par des logiciels malveillants et des virus, assurez-vous que tous les dispositifs externes vous appartiennent ou proviennent d'une source fiable.



✓ CONSEIL 9 : DÉCONNECTEZ-VOUS D'INTERNET LORSQUE VOUS NE L'UTILISEZ PAS

Éteignez votre ordinateur la nuit ou lorsque vous ne l'utilisez pas pour une période prolongée. Le fait d'être toujours allumé fait de votre ordinateur une cible plus visible pour les pirates informatiques. Le fait de l'éteindre interrompt la connexion qu'un pirate informatique aurait pu établir avec votre réseau et empêche tout éventuel acte de malveillance.

✓ CONSEIL 10 : SÉPAREZ LES ACTIVITÉS PROFESSIONNELLES DES ACTIVITÉS PERSONNELLES SUR VOTRE PC

Lorsque les ordinateurs sont utilisés à des fins personnelles plutôt que professionnelles, le risque que surviennent des infections et autres incidents de sécurité augmente - les films, les jeux, la musique et toute autre application personnelle comportent tous des risques inhérents. Si vous ne possédez qu'un seul PC et que vous souhaitez séparer vos activités professionnelles et personnelles, prenez le temps de créer différents comptes d'utilisateur - un pour votre travail et un pour votre usage personnel.

✓ CONSEIL 11 : SÉCURISEZ VOTRE RÉSEAU DOMESTIQUE

Il est important de sécuriser le Wi-Fi de votre domicile. Assurez-vous que la sécurité de votre Wi-Fi domestique est activée et que vous avez changé le mot de passe administratif de votre routeur. La plupart des routeurs vous permettent également de « cacher » votre Wi-Fi, ce qui signifie que les gens doivent connaître à la fois l'identifiant Wi-Fi et le mot de passe pour pouvoir se connecter.

Vous connaissez maintenant les mesures importantes que vous devez prendre pour sécuriser vos informations personnelles et celles de votre entreprise lorsque vous travaillez sur votre PC personnel. Restez en sécurité !