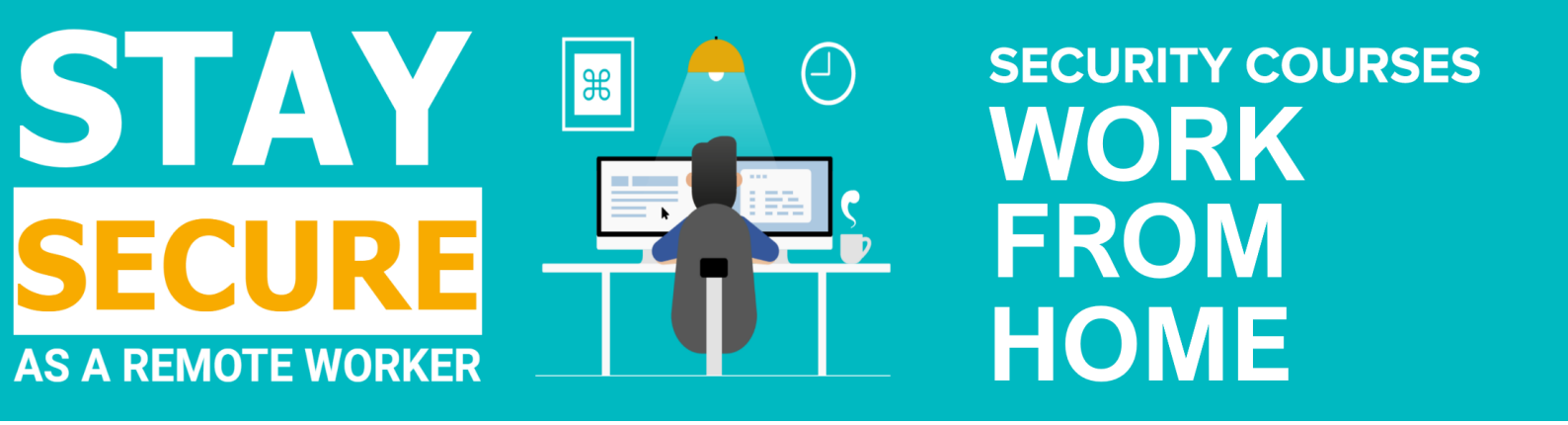


Formation Sécurité pour le travail à domicile

Il existe de nombreux avantages à travailler à distance ou de chez soi. Ceux-ci incluent un gain de temps dans les transports, de productivité, des horaires et temps de travail plus souples qui permettent aux télétravailleurs une meilleure organisation, un gain en autonomie et en responsabilité et donc un accroissement en efficacité. Néanmoins, quand vous travaillez à distance, soit chez vous, soit ailleurs dans un lieu public, Vous êtes le seul responsable de votre propre sécurité, celle de vos outils informatiques, et de l'information que vous pouvez véhiculer ou échanger.

Vous ne pouvez avoir un niveau de sécurité similaire à celui de votre entreprise. Vous devez donc vous préparer pour ce télétravail. Si vous ne le faites pas, vous risquez d'être la cible facile de personnes ou organisations malveillantes, de criminels, voir de concurrents peu scrupuleux qui auront un moyen simple de voler de l'information (personnelle ou entreprise). Une bonne préparation peut cependant réduire considérablement les risques et rendre votre expérience de travail à domicile nettement plus confortable et productive.

A quels risques de sécurité devrez-vous faire face en travaillant à distance ?

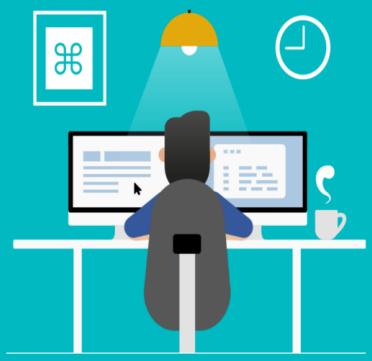
De nombreux facteurs peuvent compromettre la sécurité des travailleurs à distance et des données manipulées de manière journalière. Pour cette formation nous avons regroupé ces risques en 4 catégories : Le vol ou la perte physique, le manque de sensibilisation et de connaissance, la connexion publique non sécurisée et l'accès sans limite ni contrôle au système d'information de l'entreprise.

PERTE OU VOL PHYSIQUE

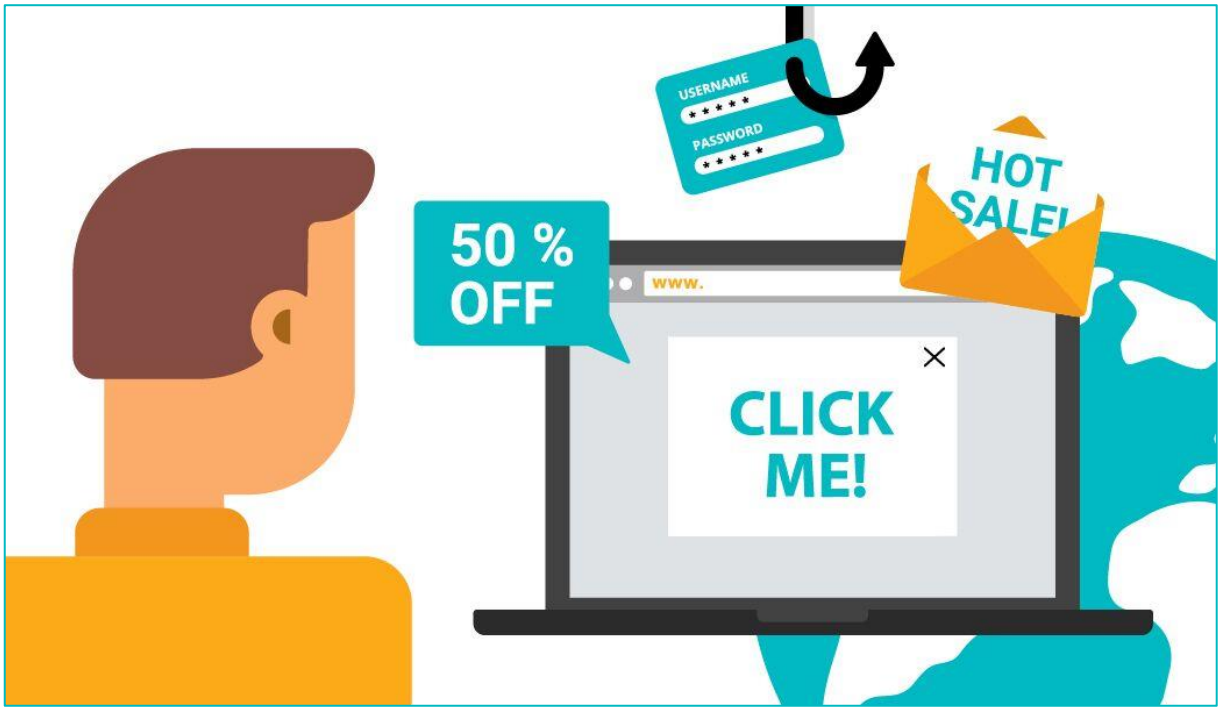
Travailler physiquement dans un bureau au sein de son entreprise comporte de nombreux avantages : les outils de sécurité sont déjà mis en place, les processus de protections des données sont opérationnels, les pratiques d'accès à l'information, et des équipes dédiées à veiller globalement au respect des politiques de sécurité de l'entreprise sont également en place.

Quand votre environnement de travail change physiquement de place, travail à domicile, cyber café ou tout autre lieu public, vous ne pouvez vous reposer sur aucun niveau de sécurité. Ceci fait de vos outils de travail une cible facile pour de nombreuses personnes, allant du vol de votre ordinateur au hacker aguerri qui entrera aisément dans votre système, puis dans celui de votre entreprise, et subtilisera de l'information vitale pour les revendre à qui veut, des concurrents par exemple.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES WORK FROM HOME

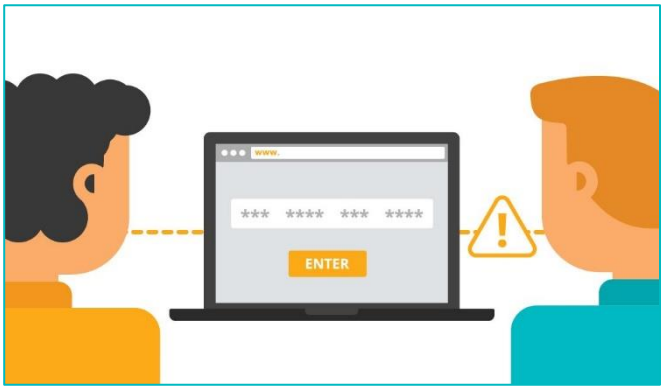


MANQUE DE SENSIBILISATION ET DE CONNAISSANCE PERSONELLES

Dans bien des cas, le télétravail est un gain de productivité car le salarié voit une amélioration de sa qualité de vie au travail. Cependant, sans une vigilance accrue et permanente, un salarié à distance ne pourrait sans doute pas remarquer qu'il est surveillé/pisté, hameçonné ou attaqué.

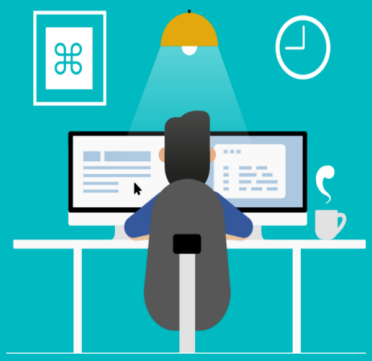
De plus, les salariés à distance tombent dans l'habitude d'un accès presque sans limite aux données de leur entreprise à partir d'équipements personnels non sécurisés ou pire, permettent à des personnes tierces d'utiliser ou de naviguer sur la toile avec l'équipement portable de l'entreprise. Malheureusement, la plupart des gens sont habitués à ces principes d'accès illimité sans vraiment vérifier les conséquences ni évaluer le niveau de compromission qu'ils font supporter à leur organisation.

Accès illimité au système d'informations de l'entreprise



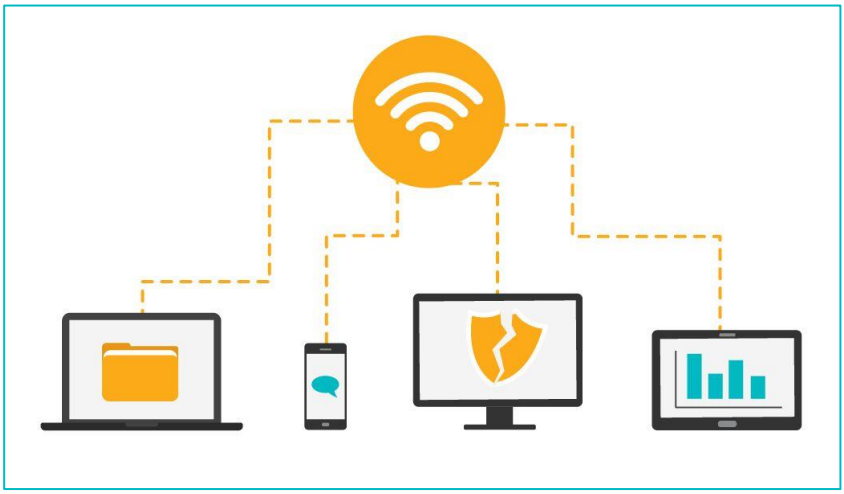
De nombreuses sociétés donnent à leurs travailleurs à distance les mêmes accès qu'à l'intérieur de leur entreprise, comprenant l'accès complet au réseau de l'entreprise, l'accès aux nuages d'informations, les systèmes internes, etc… Cependant, si le salarié n'est pas assez vigilant et manque de connaissance, ses privilèges peuvent donner aux attaquants un moyen d'accès illimité au système d'informations de l'entreprise.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES WORK FROM HOME

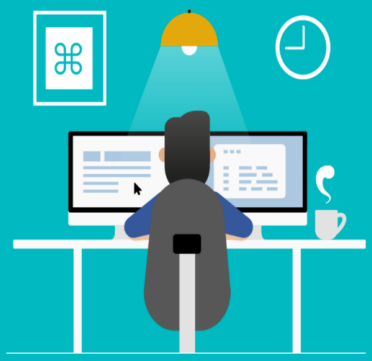
CONNEXIONS PUBLIQUES NON SECURISEES



Combien de fois avez-vous utilisé un point d'accès Wifi public lors de vos déplacements professionnels, dans un aéroport ou dans votre chambre d'hôtel ? La majorité de ces réseaux ne possèdent pas de sécurité, si bien que les utiliser dans le cadre de votre travail expose votre équipement à une attaque potentielle.

La menace est réelle car la plupart de ces réseaux publics ne chiffrent pas les communications et ne requièrent pas d'authentification des personnes pour se connecter. De tels réseaux, y compris un réseau à domicile, peuvent permettre à des personnes malveillantes, d'accéder à l'ensemble des informations échangées sur Internet, à des courriers confidentiels, des données privées d'accès aux services entreprises et même, bien entendu, à des informations bancaires et numéros de cartes de crédit.

STAY SECURE AS A REMOTE WORKER

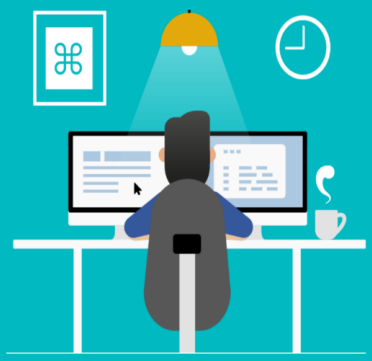


SECURITY COURSES WORK FROM HOME

Que pouvez-vous faire pour vous protéger vous et votre société quand vous travaillez en dehors de votre bureau ?

Fort heureusement, nous pouvons tous nous protéger dans le cas du télétravail. Tout est question de vigilance, de bonnes habitudes, et il faut être sensibilisé aux procédures nécessaires de sécurité.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES WORK FROM HOME

Etape 1: Vous préparez vous-même et votre matériel

Quand vous devez travailler en dehors de votre bureau, lors de vos déplacements ou à la maison, assurez-vous d'être bien préparé pour exécuter vos tâches de manière efficace. Votre équipe du support informatique doit vous fournir les moyens d'accès adéquates aux applications et fichiers de l'entreprise.

Avant de quitter votre bureau, prenez votre ordinateur et ses équipements périphériques nécessaires, les documents dont vous aurez besoin, mais évitez autant que possible ceux avec des contenus à caractère confidentiel, plan de développement, données classifiées… Cette précaution réduira le nombre de choses sur lesquels vous devrez porter votre attention, et en cas de vol de matériel, l'impact pour votre société.

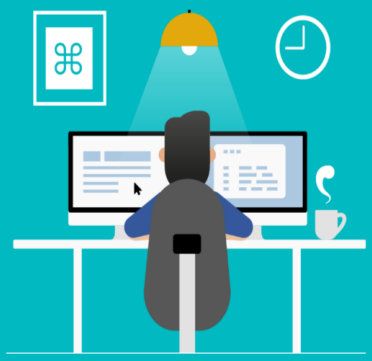
Etape 2: Gardez vos équipements à jour et sécurisés

Pour sécuriser votre équipement informatique, vous devez vérifier que tous les logiciels installés soient à jour, en incluant le système d'exploitation lui-même. Gardez à l'esprit qu'aucun système informatique ne peut être 100% sécurisé. Des vulnérabilités ou failles de sécurité sont découvertes en permanence et peuvent affecter n'importe quelle version de vos OS. De plus, le risque est encore plus grand quand votre système est ancien, voire plus du tout supporté. Il est donc judicieux que tous les équipements fonctionnent avec leur dernière version.

La plupart des vulnérabilités sont corrigées en deux mois. Imaginez ce que peut être l'exposition aux attaques pendant cette période ! Pour éliminer les délais liés à la mise à jour de votre système, il est recommandé de positionner l'option "mise à jour automatique".

Une fois que votre système est programmé pour être en permanence à jour, il faut maintenant se porter sur la mise à jour de vos applications. Ceci inclut, bien entendu, vos outils d'édition comme, par exemple, la suite Office, les outils de création, le navigateur internet et tout autre logiciel qui pourrait avoir des vulnérabilités.Par principe, les logiciels modernes embarquent des fonctions détection de présence de mise à jour. Il vous suffit donc de veiller à leur téléchargement et installation dans les meilleurs délais.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES WORK FROM HOME

Etape 3: Verrouillez votre ordinateur quand vous vous éloignez

Quand vous vous éloignez de votre bureau, veillez à ce que l'ordinateur soit en mode sécurisé. Ce dernier et les informations qu'il contient sont certainement importantes pour votre entreprise, mais aussi très intéressantes pour un tiers ou un concurrent.

Voici une liste de précautions que vous devez suivre pour assurer un niveau minimum de sécurité à votre équipement et son contenu :

- ✓ Etape 3.1: Autoriser le verrouillage

  Si vous devez vous éloigner de votre ordinateur, que ce soit au bureau, entouré de vos collaborateurs, ou à votre domicile, entouré de vos proches, pensez à verrouiller votre ordinateur. Pour ne pas oublier, pensez à configurer votre équipement pour qu'il se verrouille automatiquement après une minute d'inactivité pour un téléphone ou une tablette et cinq minutes pour un ordinateur.

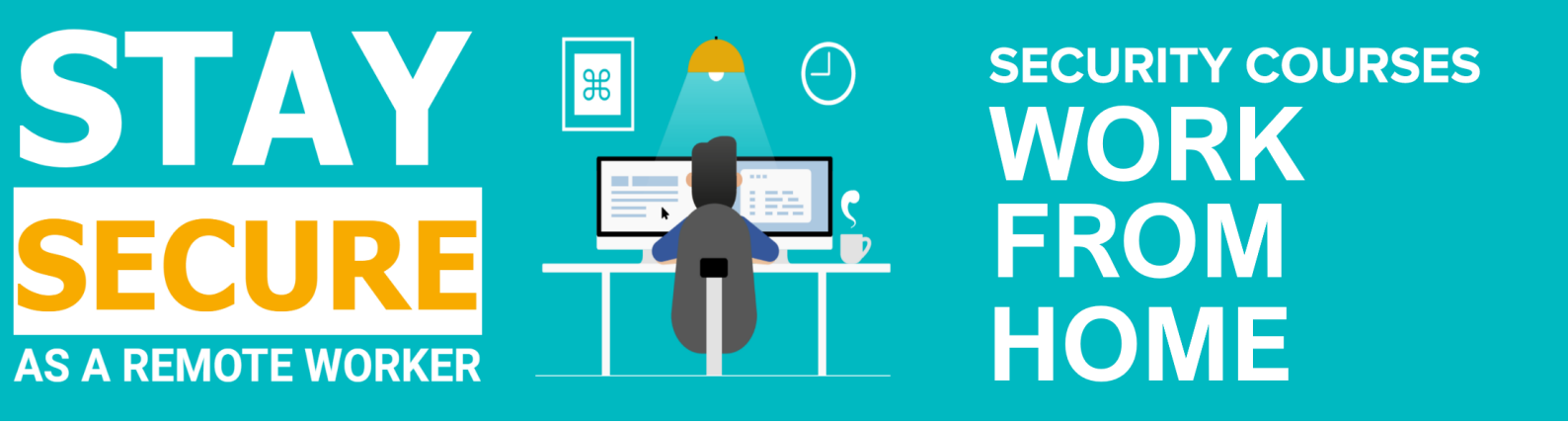
- ✓ Etape 3.2: Supprimer l'identification automatique

- ✓ Vous devez être le seul à avoir accès à votre équipement. Veillez donc à vous identifier systématiquement avec votre mot de passe, code ou biométrique.

- ✓ L'identification automatique est un réel danger pour les entreprises, soyez donc certain d'avoir supprimé cette fonction.

- ✓ Etape 3.3: Utilisez des mots de passe forts

  Nous ne pouvons que rappeler l'importance d'utiliser des mots de passe sérieux, complexes à "casser" avec tous vos équipements. Les mots de passe triviaux, basés sur une suite de chiffres, des noms propres, des noms de personnes, des lieux, des informations personnelles - la plupart étant présentes sur vos réseaux sociaux, date de naissance, lieu de naissance etc, sont réellement à bannir. Un mot de passe fort doit ressembler à une suite aléatoire de lettres, de chiffres, de caractères spéciaux, minuscules et majuscules. Il doit à minima comporter 8 symboles (lettres/chiffres/...).



✓ Etape 3.4: Investissez dans un gestionnaire de mots de passe (beaucoup sont gratuits)

Quand vous utilisez des mots de passe forts, uniques pour chaque équipement, ou accès à des vos applications, ou des sites internet, il devient difficile de les gérer manuellement. Parfois vous aurez tendance à les oublier, à les confondre et vous ne souhaitez surtout pas les noter sur une feuille de papier ou un pense-bête. C'est justement pour cette raison que les gestionnaires de mots de passe sont intéressants car ils gardent secret un nombre illimité de mots de passe, protégés et chiffrés par un unique mot de passe (maitre). Quelques exemples de solutions : 1Password, LastPass et bien d'autres.

✓ Etape 3.5: Utilisez une authentification à deux facteurs (2FA)

Dans bien des cas, l'utilisation d'un mot de passe unique pour l'accès à vos comptes n'est pas suffisant et en particulier pour l'accès à votre système d'informations entreprise, courrier électronique ou gestionnaire de mots de passe. Tous contiennent des informations sensibles qu'ils faut protéger coûte que coûte, et sans limite de temps.
C'est la raison pour laquelle l'authentification à deux facteurs a été introduite il y a quelques années. Cette méthode vous oblige non seulement à entrer votre mot de passe mais également une information additionnelle de vérification qui validera votre identité. Ceci peut être matérialisé par un code à usage unique envoyé par SMS ou une application d'authentification tierce.
Mettre en place une authentification à deux facteurs est réellement une méthode qui vous aidera à renforcer votre niveau de sécurité.

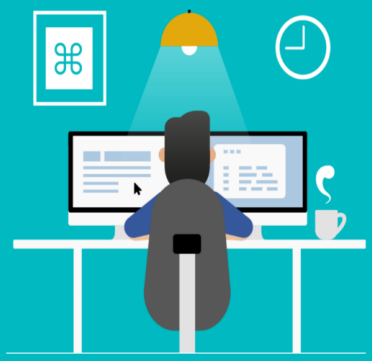
✓ Étape 3.6: Autorisez la localisation de votre équipement, et l'option d'effacement à distance

Dans le cas de perte ou de vol, avoir positionné l'option de localisation et d'effacement des contenus à distance n'est pas seulement une bonne mesure de précaution, mais est simplement indispensable. Ceci évite le risque que vos données personnelles et aussi les données de votre entreprise ne tombent dans les mains de gens malveillants.

✓ Etape 3.7: Réinitialisation système

La réinitialisation d'un système ou d'un équipement devrait également être effectuée quand celui-ci n'est plus utilisé. Réinitialisez le avant de le vendre, le donner voir même le jeter.
Souvenez-vous, réinitialiser veut également dire que toutes vos informations vont être effacées de votre équipement. Une sauvegarde préalable est nécessaire pour une utilisation ultérieure de celles-ci.

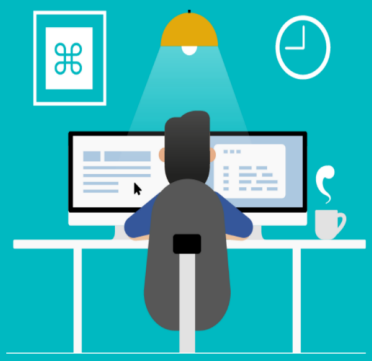
STAY SECURE AS A REMOTE WORKER



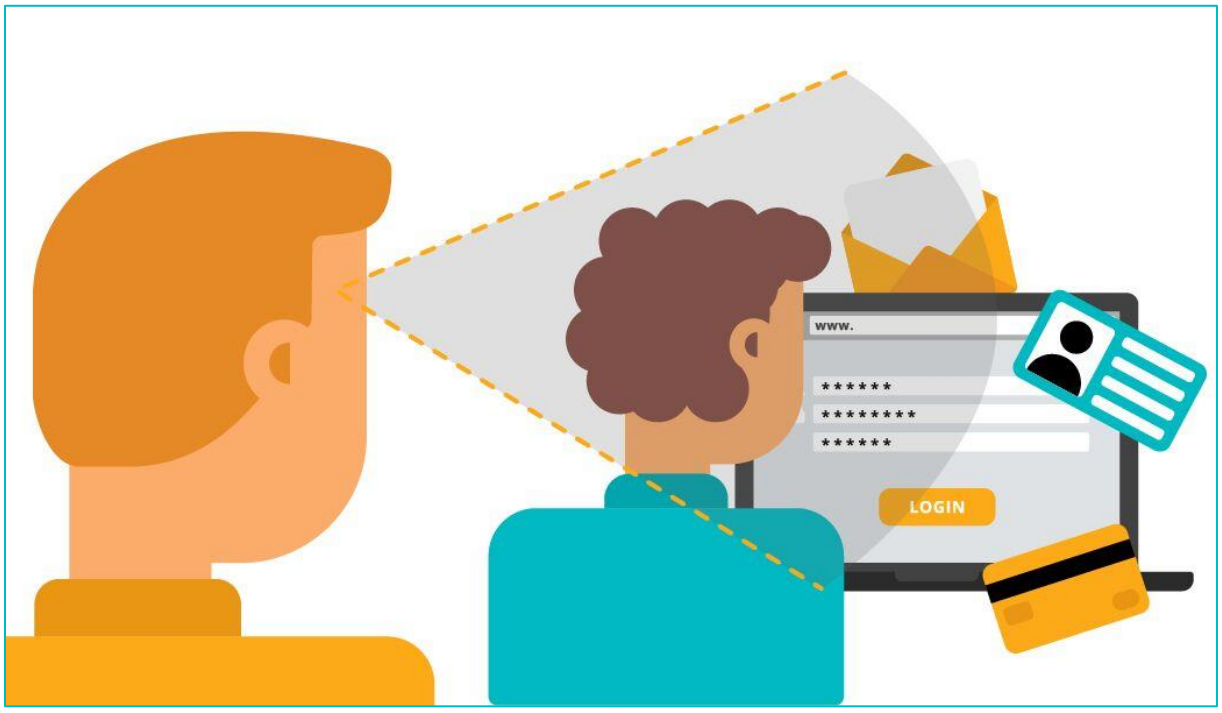
SECURITY COURSES
WORK FROM HOME

Etape 4: Méfiez-vous de votre environnement

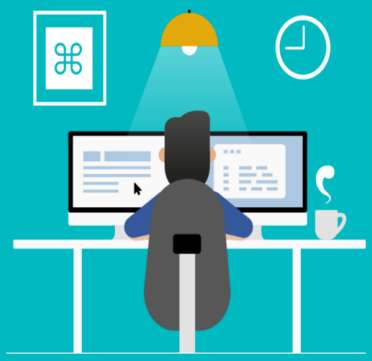
Votre environnement physique est très important, le négliger peut compromettre non seulement la sécurité des personnes, mais aussi vos équipements et les informations de votre société. C'est en particulier le cas lors du travail à domicile ou à l'extérieur de votre société en général. Restez vigilant de toutes les activités autour de vous, ne laissez pas vos équipements (ordinateurs/disques durs/clés USB, …) libre d'accès, chez vous ou dans un lieu public. Le temps que vous alliez vous préparer un café, vos équipements peuvent être dérobés ou compromis. La perte de ceux-ci et des informations qu'ils contiennent peut, non seulement causer un stress et l'arrêt de votre travail, mais aussi résulter en pénalités pour vous et votre société.



Etape 5: Faite attention à vos zones de confidentialité



Quand vous travaillez dans un lieu public, faites attention à votre zone de confidentialité. Si possible, disposez votre bureau tel que votre siège se trouve dos au mur, ainsi personne ne peut regarder votre écran sans que vous le sachiez. Une autre option consiste à acquérir un filtre d'écran qui empêche la lecture de côté ou dans des angles autre que le vôtre.

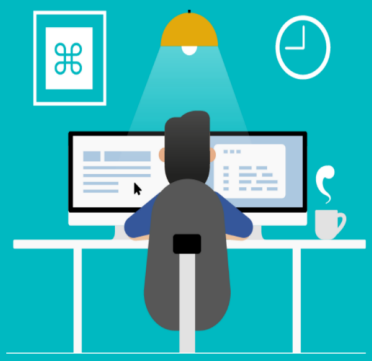


Etape 6: Protégez l'information confidentielle

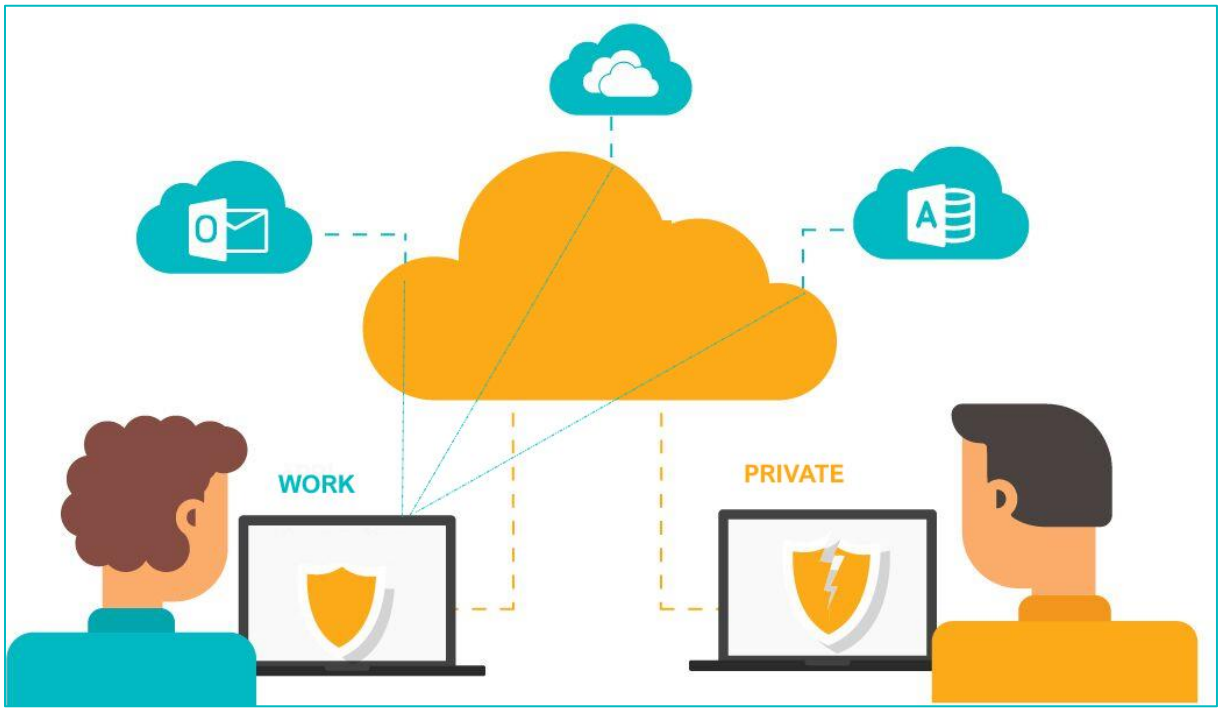
Quand vous travaillez en dehors de votre bureau, il est particulièrement important de protéger les informations confidentielles et les informations personnelles quand vous les manipulez, les transportez ou les sauvegardez. Dans la vraie vie, de nombreuses personnes malveillantes, de simples voleurs, ou des concurrents, peuvent porter atteinte aux entreprises. Ces dernières seront redevables et surtout responsables de la divulgation d'informations sensibles, classifiées, personnelles.

Gardez à l'esprit qu'un ordinateur public (cyber café, chez un ami, …) n'est absolument pas sûr et qu'il ne devrait jamais être utilisé pour détenir, utiliser, visualiser ou modifier des données personnelles ou confidentielles. Vous ne savez pas si l'équipement en question n'a pas reçu un logiciel malveillant. En conséquence, évitez de rentrer vos identifiants de banques, ou numéro de sécurité sociale. Assurez-vous de naviguer sur internet en mode privé, ne cliquez pas sur les boutons « Sauvegarder » ou « se souvenir », supprimez votre historique de navigation y compris tout ce que vous auriez téléchargé.

Même si vous voyagez avec l'ordinateur de votre société, ou que vous l'utilisez chez vous, il y a toujours un danger pour que quelqu'un puisse y avoir accès. Gardez donc l'ordinateur de votre société uniquement pour le travail et ne permettez à personne, y compris votre famille ou vos amis, de l'utiliser. Même involontaire, une compromission de ce type peut vous rendre responsable vis-à-vis de votre société.



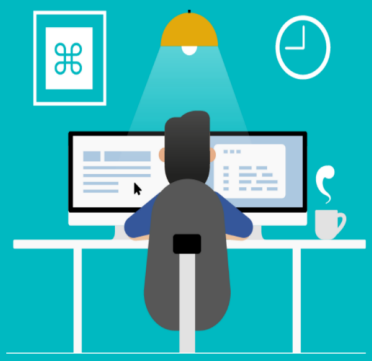
Etape 7: Gardez les données de travail sur les ordinateurs de travail



Il est fort probable que vos équipements personnels ne soit pas mis à jour régulièrement et de ce fait, n'exécute pas en arrière-plan les dernières mises à jours des tâches de sécurité, comme l'antivirus, le pare-feu, le chiffrement, etc.. Si vous n'êtes pas un spécialiste informatique (et même dans ce cas, cela ne garantit pas une protection à 100%), vous n'êtes probablement pas au fait de toutes les précautions que le service de sécurité informatique dédié peut vous apporter.

Vous pourriez être tenté d'utiliser votre ordinateur de travail pour des besoins personnels, comme par exemple faire des achats en ligne, accéder à vos comptes bancaires, ou simplement lire vos courriers personnels. Alternativement vous pourriez être tenté d'utiliser vos ordinateurs personnels pour travailler. Cependant, connecté simplement un ordinateur insuffisamment sécurisé comme le vôtre, au réseau de votre entreprise, peut compromettre la totalité de la sécurité de votre travail, celle de votre entreprise ainsi que vous rendre responsable des dommages causés au système d'informations (serveurs et données contenues) de votre entreprise.

Il y a néanmoins une manière de s'affranchir de ce risque si vous devez utiliser votre ordinateur personnel pour le travail. Il s'agit d'utiliser des applications dans le nuage comme par exemple Office 365. Grâce à ces services, vous travaillez à distance sans qu'aucune donnée ne soit synchronisée avec votre équipement personnel.



Etape 8: Evitez les réseaux Wifi Publics

Quand vous travaillez dans endroit public, il est très tentant d'utiliser les connexions gratuites à disposition. Cependant, le terme « Accès gratuit » peut assez souvent mener à de nombreux problèmes pour vous et votre société.

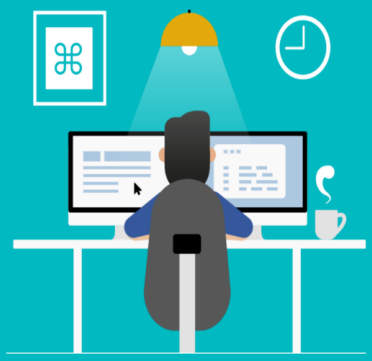
Les deux problèmes principaux liés à l'accès à un réseau Wifi public sont :

1) Réseau partagé par d'innombrables équipements au même moment,
2) Un trafic de données qui est non protégé et non chiffré et qui transite entre ce réseau Wifi et le réseau de votre entreprise.

Pour résoudre le premier point, vous pouvez opter pour l'utilisation de votre propre accès Wifi grâce à votre téléphone portable. Même si le trafic n'est pas chiffré, il ne permet pas non plus à d'autres personnes de s'y connecter et donc de capturer potentiellement des données. Bien entendu vous serez facturé par votre opérateur mais le coût est négligeable comparé à une fuite potentielle de données sur un réseau public.

Quant au deuxième point, la meilleure solution est d'utiliser une solution de réseau privé virtuel (VPN) qui offre une connexion sécurisée, chiffrée pour toutes vos correspondances sur le réseau Internet. Un VPN rend l'interception des données extrêmement difficile en cas de piratage et vous rend totalement anonyme. Cet outil vous fournit la confidentialité nécessaire.

Certains pays interdisent l'usage de ces outils, mais si celui-ci est légal, il est très judicieux de l'utiliser depuis des réseaux publics.



Etape 9: Chiffrez les données sensibles dans vos emails et dans votre équipement.

Aucune information envoyée par courrier électronique n'est sécurisée sauf si vous prenez la précaution de la chiffrer avant son envoi. Le chiffrement est le processus qui permet de coder l'information avec une clé, de telle manière que cette information ne peut être décodée facilement sans posséder cette clé. Si vous devez envoyer des informations sensibles, veillez à les chiffrer avant leur envoi.

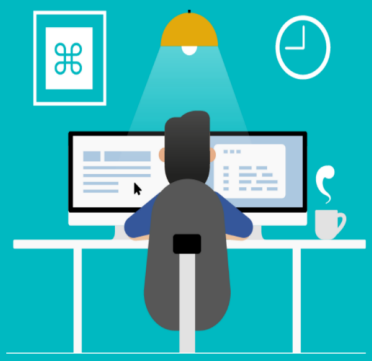
Par précaution, vous devriez toujours chiffrer toutes les données de telle sorte que si vous perdez votre ordinateur, ou celui-ci est volé, personne d'autre que vous avez accès à l'information, si ce n'est la personne qui possède le mot de passe ou justement, cette « clé ».

Etape 10: Faite attention aux support USB et connectiques des ordinateurs

Vous seriez surpris de voir combien de personnes sont capables de brancher une clé USB, trouvée abandonnée quelque part, sur leur ordinateur. Malgré le fait que cette méthode est classique et triviale, beaucoup de personnes se font prendre. Une fois qu'une clé USB malveillante a accédé au port de communication de l'ordinateur, vos données, informations et peut-être même l'ensemble du réseau de votre entreprise peuvent potentiellement être corrompus. Évitez ceci à tout prix.

Un autre risque lié à la connexion USB est de vouloir charger son téléphone portable quand vous n'avez pas le chargeur adapté avec vous. Si cela est l'unique moyen, essayez d'utiliser un « bloqueur » USB, une application qui permet le chargement mais qui interdit le transfert de données.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES

WORK FROM HOME

Etape 11: Ne laissez jamais votre ordinateur ou autres équipements dans votre véhicule, chambre d'hôtel ou autres endroits non sécurisés

Afin d'éviter le vol de vos équipements informatiques et de ce fait, toute perte de données personnelles ou entreprise, gardez les toujours près de vous. Ne les laissez pas dans votre voiture ni même dans votre chambre d'hôtel qui n'est pas plus sécurisée car tout le personnel peut y avoir accès.