5 conseils aux salariés qui travaillent en Home Office

Nous savons que le travail à domicile est une situation inédite, voire déroutante, pour certains d'entre vous. Nous tenons à ce que vous puissiez assurer une sécurité maximale sur tous vos supports numériques.

Avec les cinq précautions détaillées ci-dessous, vous sécuriserez votre travail, et vous protégerez aussi votre domicile des cyber-attaques, pour votre bien et celui de votre famille.

1. À vous de jouer !

Disons-le d'emblée, la technologie seule ne peut pas vous protéger intégralement : le premier rempart, c'est vous ! Les cybercriminels savent désormais que, pour obtenir ce qu'ils veulent, il est plus simple de passer par vous-même plutôt que d'attaquer directement votre ordinateur ou d'autres appareils. Pour connaître votre mot de passe, vos données professionnelles ou pour prendre le contrôle de votre ordinateur, ils tenteront de vous piéger, souvent en créant un sentiment d'urgence pour vous mettre en condition de le leur révéler. Par exemple, ils peuvent vous appeler en se faisant passer pour le support technique de Microsoft et en prétendant que votre ordinateur est infecté. Ou bien ils vous envoient un courriel vous avertissant qu'un colis n'a pas pu être livré et vous leurrent en vous amenant à cliquer sur un lien malveillant.

Voici les signes révélateurs les plus courants d'une attaque d'ingénierie sociale (https://www.ebas.ch/fr/lingenierie-sociale-social-engineering/) :

- un individu cherche à créer un fort sentiment d'urgence, souvent en utilisant la peur, l'intimidation, une crise ou une échéance importante ;
- une mise sous pression pour contourner ou ignorer les politiques ou procédures de sécurité, ou une offre, mais qui est trop belle pour être vraie (non, vous n'avez pas gagné à la loterie !) ;
- un message, prétendûment d'un ami ou d'un collègue, mais avec une signature, un timbre de voix ou une façon de s'exprimer qui ne lui ressemble pas.

Au bout du compte, la meilleure défense contre ces attaques, c'est vous!

En savoir plus (https://www.ebas.ch/fr/5-faire-attention-et-etre-vigilant/)

2. Réseau domestique

Presque tous les réseaux domestiques commencent par un réseau sans fil (ou Wi-Fi). C'est ce qui permet à tous vos appareils de se connecter à Internet. Les réseaux sans fil à domicile sont gérés à travers votre routeur Internet ou, séparément, à travers un point d'accès sans fil dédié. Tous deux fonctionnent de la même manière : en diffusant des signaux sans fil auxquels se connectent les appareils domestiques. D'où l'importance de garantir la sécurité de votre réseau pour protéger votre habitation.

Nous recommandons les mesures suivantes :

- Modifiez le mot de passe administrateur par défaut : dans le compte administrateur, vous pourrez configurer les paramètres de votre réseau sans fil. Un cybercriminel parvient sans difficulté à trouver le mot de passe par défaut fourni par le fabricant.
- N'autorisez l'accès qu'aux personnes que vous jugez fiables : pour ce faire, il faut assurer un système de sécurité solide afin que seules les personnes en qui vous avez confiance puissent se connecter à votre réseau sans fil. Un système de sécurité fort exigera de quiconque un mot de passe pour pouvoir se connecter à votre réseau sans fil. Il cryptera leur activité une fois qu'ils seront connectés.
- Générez des mots de passe forts : les mots de passe que les personnes utilisent pour se connecter à votre réseau sans fil doivent être solides et différents du mot de passe de l'administrateur. Rappelons que vous n'aurez à saisir le mot de passe qu'une seule fois pour chacun de vos appareils, car ils stockent et mémorisent le mot de passe.

Je ne suis pas sûr·e de savoir comment procéder...
Demandez à votre fournisseur d'accès à Internet, consultez son site web, vérifiez la documentation fournie avec votre point d'accès sans fil ou consultez le site web du fournisseur.

Utilisez une connexion VPN pendant le travail
Une connexion VPN vous permet de connecter de manière sécurisée le dispositif depuis lequel vous travaillez à la maison au réseau de l'entreprise. Les données échangées seront ainsi protégées par cryptage pendant leur transport (chiffrement de bout en bout).

3. Mots de passe

Lorsqu'un site vous demande de créer un mot de passe, faites-en sorte qu'il soit fort : plus il comporte de caractères, plus il est solide. L'un des moyens les plus simples de s'assurer un mot de passe sûr est d'utiliser une phrase de passe, ou phrase secrète. Cette dernière n'est autre qu'un mot de passe composé de plusieurs mots, tels que « bourbon au miel d'abeille ». Utiliser une phrase de passe unique signifie en utiliser une différente pour chaque appareil. Ainsi, si une phrase de passe est compromise, tous vos autres comptes et appareils sont toujours en sécurité.

Vous ne parvenez pas à vous souvenir de toutes ces phrases de passe?
Utilisez un gestionnaire de mots de passe, qui est un programme spécialisé stockant de manière sécurisée toutes vos phrases de passe dans un format crypté (et qui possède également de nombreuses autres fonctionnalités intéressantes !). Enfin, activez l'authentification en deux étapes (également appelée authentification à deux facteurs ou à plusieurs facteurs) chaque fois que cela est possible. Ce système ajoute à la saisie de votre mot de passe une deuxième étape, comme un code envoyé à votre smartphone ou une application qui génère le code pour vous. L'authentification en deux étapes est probablement la mesure la plus importante que vous puissiez prendre pour protéger vos comptes en ligne – en outre, elle est beaucoup plus facile que vous ne l'imaginez.

En savoir plus (https://www.ebas.ch/fr/4-proteger-les-acces-internet/)

4. Mises à jour

Les cybercriminels sont constamment à la recherche de nouvelles failles de vulnérabilité dans les logiciels utilisés par vos appareils. Lorsqu'ils les découvrent, ils cherchent à les exploiter à l'aide de logiciels ad hoc et à pirater les appareils que vous utilisez. Pendant ce temps, les entreprises qui ont créé les logiciels pour ces appareils s'évertuent à publier rapidement les mises à jour. En veillant à ce que vos ordinateurs et vos appareils mobiles installent ces mises à jour sans tarder, vous rendez la tâche beaucoup plus difficile aux pirates informatiques. Pour

cela, il suffit d'activer la mise à jour automatique chaque fois que cela est possible. Cette règle s'applique à presque toutes les technologies connectées à un réseau, dont bien sûr les appareils de travail, mais aussi les téléviseurs connectés à Internet, les interphones pour bébés, les caméras de sécurité, les routeurs familiaux, les consoles de jeu, et même votre voiture.

Assurez-vous que chacun de vos ordinateurs, appareils mobiles, programmes et applications fonctionne avec la dernière version de son logiciel.

En savoir plus (https://www.ebas.ch/fr/3-prevenir-avec-les-mises-a-jour-logicielles/)

5. Les enfants et les visiteurs

Contrairement à ce qui se passe au bureau, où vous n'avez probablement pas des enfants, des visiteurs ou d'autres membres de votre famille qui utilisent votre ordinateur portable ou d'autres appareils de travail, à la maison le risque existe bel et bien que ces personnes effacent ou modifient accidentellement des informations, ou, pire encore, infectent votre appareil par inadvertance.

Faites bien comprendre au reste de la famille et à vos amis qu'ils ne peuvent pas utiliser vos appareils de travail.

Il y a-t-il plusieurs personnes à utiliser un même appareil ?
Créez un compte utilisateur distinct pour chaque personne utilisant le même appareil. De cette manière, vous réaliserez au moins une séparation logique entre les environnements et chaque utilisateur ne pourra accéder qu'aux dossiers relevant de ses compétences.

Source: SANS Institut (https://security-awareness.sans.org/sites/default/files/2020-03/03-SSA-WorkingFromHome-FactSheet.pdf)

Ces recommandations sont basées sur la brochure de l'Institut SANS (https://security-awareness.sans.org/sites/default/files/2020-03/03-SSA-WorkingFromHome-FactSheet.pdf) (en anglais).