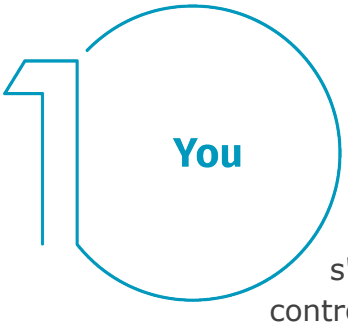
SANS SECURITY AWARENESS

Les 5 principales étapes pour travailler en toute sécurité à domicile

Nous savons que travailler de chez soi est une expérience nouvelle pour certains d'entre vous, et l'adaptation à un nouvel environnement peut sembler insurmontable. Vous permettre de travailler en sécurité de chez vous fait partie de nos objectifs. Vous trouverez ci-dessous cinq mesures simples pour travailler en toute sécurité. Mieux encore, toutes ces mesures vous protégeront, vous et votre famille, en créant un environnement cyber-sécurisé à la maison.



Vous : retenez surtout que la technologie seule ne permet pas de vous protéger complètement. La meilleure protection, c'est vous. Les criminels savent que, pour atteindre leur but facilement, c'est vous qu'ils doivent cibler et non votre ordinateur ou vos appareils. S'ils veulent s'approprier votre mot de passe, vos données de travail ou le contrôle de votre ordinateur, ils essaieront de vous berner, souvent en créant un sentiment d'urgence. Par exemple, ils vous appelleront en se faisant passer pour l'assistance technique de Microsoft et prétendront que votre ordinateur est infecté. Ou ils vous enverront un e-mail indiquant qu'un colis n'a pas pu être livré et vous incitant à cliquer sur un lien malveillant. Vous devez soupçonner une attaque d'ingénierie sociale dans les cas suivants :

- Quelqu'un induit un sentiment d'urgence extrême par la peur, l'intimidation, une crise ou un délai important. Les cybercriminels savent créer des messages convaincants qui semblent provenir d'une entreprise fiable, comme une banque, le gouvernement ou une société internationale.
- On vous incite à ignorer ou à contourner les règles et procédures de sécurité, ou on vous offre quelque chose de trop beau pour être vrai (non, vous n'avez pas gagné à la loterie).
- Un message d'un ami ou d'un collègue, dont la signature, le ton utilisé ou le style ne lui ressemble pas.

Au bout du compte, la meilleure défense contre ces attaques, c’est vous.

Réseau à domicile : la grande majorité des réseaux à domicile débutent par un réseau sans fil (souvent appelé Wi-Fi). Il vous permet de connecter tous vos appareils à Internet. La plupart des réseaux sans fil à domicile sont contrôlés par votre routeur Internet ou un point d'accès sans fil dédié séparé. Ils fonctionnent de la même manière : ils émettent des signaux sans fil auxquels les appareils domestiques se connectent. Pour protéger votre domicile, il est donc essentiel que vous sécurisiez votre réseau sans fil. Nous vous conseillons de suivre ces étapes :

- Modifiez le mot de passe administrateur par défaut de l'appareil contrôlant votre réseau sans fil. C'est le compte administrateur qui vous permet de configurer les paramètres de votre réseau sans fil.
- Assurez-vous que seules des personnes de confiance peuvent se connecter à votre réseau sans fil. Pour cela, mettez en place des paramètres de sécurité forts. Ainsi, quiconque souhaite se connecter à votre réseau sans fil devra saisir un mot de passe et, une fois cette personne connectée, ses activités en ligne seront chiffrées.
- Assurez-vous que le mot de passe utilisé pour se connecter à votre réseau sans fil est fort, et différent du mot de passe administrateur. Souvenez-vous qu'il ne faut saisir ce mot de passe qu'une seule fois pour chaque appareil, car ces derniers le stockent et le gardent en mémoire.

Comment suivre ces étapes ? Demandez à votre fournisseur d'accès à Internet, consultez leur site Web, lisez la documentation de votre point d'accès sans fil ou ouvrez le site Web du client.

Mots de passe : lorsqu'un mot de passe doit être créé sur un site, créez-en un fort. Plus il comportera de caractères et plus il sera fort. Utiliser une phrase de passe est très facile à faire et très difficile à deviner. Une phrase de passe n'est rien d'autre qu'un mot de passe composé de plusieurs mots, tels que "*abeille miel bourbon.*" Utiliser une phrase de passe unique signifie qu'elle doit être différente pour chaque appareil ou compte en ligne. Ainsi, si l'une de vos phrases de passe est compromise, tous vos autres comptes et appareils restent protégés. Vous oubliez vos phrases de passe ?

Utilisez un gestionnaire de mots de passe, programme spécialisé qui stocke toutes vos phrases de passe de manière sécurisée et sous un format chiffré

(entre autres fonctionnalités très utiles !). Enfin, activez la vérification en deux étapes (aussi appelée authentification à deux facteurs), si possible. Elle utilise votre mot de passe, mais elle ajoute une deuxième étape, comme un code envoyé vers votre smartphone ou une application qui crée le code pour vous. La vérification en deux étapes est probablement l'étape la plus importante pour protéger vos comptes en ligne, et elle s'avère beaucoup plus simple que vous ne le pensez.

Mises à jour : vérifiez que chacun de vos appareils, appareils mobiles, programmes et chacune de vos applications est à jour. Les cybercriminels cherchent en permanence de nouvelles failles dans les logiciels utilisés par vos appareils. Lorsqu'ils découvrent des failles, ils utilisent des programmes spéciaux qui les exploitent et piratent les appareils que vous utilisez. Dans le même temps, les sociétés qui ont créé les logiciels de ces appareils s'échinent à les corriger en publiant des mises à jour. En installant rapidement ces mises à jour sur vos ordinateurs et appareils mobiles, vous compliquez la tâche aux cybercriminels. Pour rester à jour, activez simplement les mises à jour automatiques si possible. Cette règle s'applique à presque toutes les technologies connectées à un réseau, soit non seulement vos appareils de travail, mais aussi votre TV connectée, votre baby phone, vos caméras de sécurité, votre routeur, vos consoles de jeu et même votre voiture.

Enfants / Invités : au bureau, vous n'avez probablement pas à redouter que vos enfants, invités ou proches utilisent votre ordinateur portable de travail ou tout autre appareil de travail. Assurez-vous que vos proches et amis comprennent qu'ils ne doivent pas utiliser vos appareils de travail car ils risquent d'effacer ou de modifier des informations par accident, ou pire encore, de les infecter sans le vouloir.