OUCH! Décembre 2020

Votre publication mensuelle de conscientisation à propos de la Sécurité

Protéger l'écart de génération

Aperçu

Essayer d'utiliser les technologies récentes de la meilleure façon possible et ce de façon sécuritaire peut être accablant pour la plupart d'entre nous, mais ça peut être très difficile pour les membres de la famille qui ne sont pas aussi familier avec la technologie. Par conséquent, nous voulons partager quelques étapes afin de rassurer les membres de la famille qui peuvent avoir de la difficulté avec la technologie et ne pas comprendre les risques inhérents qui viennent avec l'utilisation de cette dernière.

Se concentrer sur les bases

Souvent, la meilleure façon d'aider à sécuriser les autres est de rendre la sécurité le plus simple possible pour ceux-ci. Se concentrer sur le minimum d'étapes qui auront le meilleur effet.

1. **L'ingénierie sociale:** Les attaques d'ingénierie sociale sont une des principales façon utilisées pour nous cibler. Expliquer comment les escrocs et les imitateurs opèrent depuis des milliers d'années, la seule différence de nos jours est que les mauvaises personnes utilisent Internet pour nous tromper. Des exemples, tel que des courriels d'hameçonnage qui semble être en provenance de votre institution bancaire ou un avis de suivi de colis ou des appels frauduleux voulant se faire passer pour un support technique ou bien du gouvernement. Assurez vous que les membres de votre famille comprennent qu'ils ne doivent jamais divulguer leur mot de passe, leur numéro de carte de crédit, des informations personnel ou l'accès à leur ordinateur à quiconque. Rappelez leur que plus le sentiment d'urgence est grand, plus grande est la probabilité qu'il s'agisse d'une attaque. Certains criminel s'attaquent à nos proches qui cherche l'amour et prétendent être leur candidat parfait. Pour conclure, assurez-vous qu'ils sachent que s'ils se sentent inconfortable ou ont des questions à propos de courriel ou d'une personne qui les appellent, qu'ils peuvent vous appeler pour obtenir votre assistance.
2. **Réseau sans-fil à la maison:** Prenez le temps de vous assurer que leur réseau Wi-Fi est protégé par un mot de passe et qu'il changent le mot de passe du compte d'administration initial. Vous pouvez aussi songer à configurer le réseau Wi-Fi afin qu'il utilise une configuration DNS sécurisé tel que celle-ci qui est sans fraishttps://www.opendns.com. Les services DNS sécurisé ne font pas qu'aider les gens à éviter de naviguer sur des sites infectés mais peuvent vous permettre de contrôler quel site web les gens peuvent accéder ou pas, ce qui peut être très appréciable s'il s'agit de vos enfants.
3. **Mise à jour:** Insister sur la nécessité d'appliquer les mises à jours récentes sur les systèmes d'exploitation, les applications et les équipements rend la tâche plus complexe aux criminels qui essaient de les exploiter. La façon la plus simple d'appliquer ce conseil est d'activer la mise à jour

© SANS Institute 2020

automatique lorsqu'elle est disponible. Si vous avez un équipement ou système d'exploitation qui est tellement vieux que vous ne pouvez plus le mettre à jour, nous recommandons que vous le remplaciez avec un modèle plus récents qui support les nouvelles mises à jour.

4. **Mots de passe:** Des mots de passe complexe et bien protégés sont la clé permettant de protéger aussi bien les équipements que les comptes en ligne. Montrer à vos familles comment créer de longue phrase sécurisé. Les phrases sécurisés peuvent être facile à utiliser et à se souvenir pour eux. Une autre idée serait l'installation d'un gestionnaire de mot de passe et leur expliquer comment s'en servir. Ceci peut permettre à ceux que vous appréciés d'utiliser Internet de façon simple et sécuritaire, en ayant qu'à retenir un mot de passe qui ouvrira la voûte. Selon la situation, vous pourriez même être en mesure de la gérer pour eux à distance. Si ce n'est pas possible, peut-être leur suggérer d'écrire leurs mots de passe dans un carnet et de le conserver dans un endroit sécuritaire et accessible. Pour tout les comptes virtuel critiques, tel que leur comptes bancaire, vous pouvez aussi configurer une authentification à deux facteurs. Assurez-vous d'avoir un plan de divulgation concernant les comptes en ligne de la même façon dont vous préparez votre testament pour des biens physiques.
5. **Copies de sauvegarde:** Lorsque tout les reste échoue, les copies de sauvegarde peuvent être votre sortie de secours. Assurez vous que les membres de votre famille ont une méthode simple et fiable pour leur copies de sauvegarde. Pour plusieurs, une solution infonuagique est souvent la plus simple.

Si vous avez des gens qui se sentent dépassés, aidez-les en vous attardant qu'à l'essentiel, gardez la sécurité le plus simple possible. Aussi, soyez patient, laissez place à l'erreur et aider les autres à ne pas les répéter. Finalement, suggérez leur de s'abonner à OUCH! Lettre d'information.

Rédacteur invité

Chris Dale (Twitter @chrisadale) est un consultant principale chez River Security, une firme européenne de consultation, et un instructeur certifié SANS (https://www.sans.org/profiles/chris-dale/).
Vous pouvez rejoindre Chris sur LinkedIn ici: https://www.linkedin.com/in/chrisad/

Ressources

Ingénierie sociale. https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Gestionnaire de mots de passe: https://www.sans.org/security-awareness-training/resources/password-managers-0
Mise à jour: https://www.sans.org/security-awareness-training/resources/power-updating
Copie de sauvegarde: https://www.sans.org/security-awareness-training/resources/got-backups
Héritage numérique: https://www.sans.org/security-awareness-training/resources/digital-inheritance

Traduit pour la communauté par: Jérôme Boutin et Sebastien Kierszka
OUCH! Publié par SANS Security Awareness et distribué sous Creative Commons BY-NC-ND 4.0 license. Vous pouvez partager ou distribuer cette lettre de nouvelles tant que vous ne la vendez pas ou ne la modifiez pas.
Équipe d'éditeur: Walter Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley