كيف تحمى عائلتك من مخاطر التكنولوجيا

نظرة عامة

قد تكون محاولة تحقيق أقصى استفادة من التكنولوجيا الحالية بشكل آمن أمرا مربكا لنا جميعا، ولكنها تعتبر تحديا بشكل خاص لأفراد العائلة الذين لم يعتادوا على استخدام التكنولوجيا. لذلك، أردنا مشاركة بعض الخطوات الأساسية للمساعدة فى تأمس أفراد الأسرة الذين قد يعانون من سوء فهم مخاطر الى تأى مع استخدام التكنولوجيا.

ركز على الأساسيات

كثرا ما تكون أفضل طريقة للمساعدة فى تأمس الآخرين هى جعل الأمان بسيطا قدر الإمكان بالنسبة لهم. بحيث يتم الركز على أقل عدد من الخطوات الى سيكون لها أكر الأثر.

1. **الهندسة الاجتماعية:** تعد هجمات الهندسة الاجتماعية إحدى الطرق الأساسية الى يستهدف بها معظمنا. حيث أن طرق الاحتيال والخداع موجودة منذ آلاف السنس، والاختلاف الآن فى أن الأسرار يستخدمون الإنرنت فى عمليات الخداع. ومن أمثلة الخداع الحديثة يتم إرسال بريد الكرونى لك يتظاهر بأنه البنك الذي تتعامل معه أو شحنة طرد أو المحتالس الذين يتصلون وهم يتظاهرون بأنهم من الدعم الفنى أو الحكومة ويطلبون منك بيانات حساسة. تأكد من أن أفراد العائلة يفهمون أنه لا ينبغى أبدا إعطاء كلمة المرور أو بطاقة الائتمان أو المعلومات الشخصية أو الوصول إلى أجهزة الكمبيوتر الخاصة بهم لأي شخص. ذكرهم أنه كلما كانت الرسالة أكر إلحاحا زادت احتمالية حدوث هجوم. يدمر المجرمون أحبتنا خاصة أولئك الذين يتوقون للحب حيث يوهمونهم بأنهم الأمل المنشود وأخرا. تأكد من أنهم إذا شعروا بعدم الارتياح ,أو طلب منهم البريد الالكرونى الخاص أو شخص أراد الاتصال بهم . بأن يتصلون بك أولا قبل إعطاء أي بيانات.
2. **شبكة Wi-Fi المرلية:** تأكد أن الشبكة اللاسلكية (Wi-Fi) المرلية محمية بكلمة مرور مع تغيير الإعداد ت الافراضية مثل كلمة مدير النظام الافراضية. يمكن زيادة درجة أمان الشبكة المحلية باستخدام تقنيات خادم النطاق الأمى المجانى (OpenDNS) من خلال الموقع المجانى التالى (https://www.opendns.com). ويمكن من خلال خدمة DNS ليس فقط منع حماية افراد الاسرة من زيارة المواقع المصابة بل أيضا يمكنك التحكم فى المواقع الى يتصفحونها وخصوصا اذا كانوا أطفالا.
3. **التحديثات:** تحديث الأنظمة والبرامج والأجهزة يجعل من الصعب على المجرمس اخراقها. إن أبسط طريقة لضمان ذلك هى تمكس التحديث التلقائى حيثما أمكن ذلك. إذا كان لديك جهاز أو نظام قديم جدا ولا يمكنك تحديثه، نوصيك باستبداله بجهاز جديد يدعم التحديث.

© SANS Institute 2020

4. **كلمة المرور:** كلمات المرور القوية والآمنة هى مفتاح الحماية عبر الإنترنت. قم بتدريب أفراد عائلتك حول كيفية إنشاء عبارات مرور طويلة. قد يكون من الأسهل بالنسبة لهم استخدام عبارات المرور وتذكرها من انشاء كلمات معقدة. فكرة أخرى هى تثبيت مدير كلمات المرور وتعليمهم كيفية استخدامه. بحيث يسمح لأحبائك باستخدام الإنترنت بطريقة سهلة وآمنة، ما عليك سوى تذكر كلمة مرور واحدة لإلغاء قفل الخزنة. ربما تستطيع إدارة حساباتهم عن بعد، ذلك يعتمد على نوعية البرنامج المستخدم. إذا لم يفلح ذلك، فربما اطلب منهم كتابة كلمات المرور الخاصة بهم فى كتاب ثم تخزينها فى مكان مناسب وآمن. بالنسبة إلى أي حسابات مهمة عبر الإنترنت، مثل حساباتهم المالية، قد ترغب أيضا فى إعداد التحقق من خطوتين. تأكد من أن لديك خطة قديمة لأي حسابات عبر الإنترنت بنفس الطريقة التى تعد بها وصية للأصول المادية.
5. **النسخ الاحتياطى:** عندما تفقد بياناتك أو يتم اختراقها وتدمرها، ستوفر لك النسخ الاحتياطية الحل. تأكد من أن أفراد العائلة لديهم نسخ احتياطية بسيطة وموثوقة. بالنسبة للكثيرين، غالبا ما يكون نهج النسخ الاحتياطى مستند إلى السحابة هو الأبسط والأسهل فى الاسترجاع.

إذا كان لديك أفراد من العائلة يشعرون بالإرهاق، ساعدهم بالتركيز فقط على الأساسيات، مع الحفاظ على الأمن بسيطا قدر الإمكان. كذلك، تحلى بالصبر، وامنح الوقت والمساحة لارتكاب الأخطاء، وساعد الآخرين على عدم تكرارها. أخيرا، فكر فى جعلهم يشركون فى OUCH! النسرة الإخبارية.

المحرر الضيف

كريس ديل (حسابه على تويتر @chrisadale) هو مستشار رئيسى فى شركة استشارات أمنية أوروبية River Security، كما انه مدرب معتمد من شركة SANS (https://www.sans.org/profiles/chris-dale/).
ملف كريس المهنى فى موقع لينكدإن: https://www.linkedin.com/in/chrisad/

الموارد

الهندسة الاجتماعية: https://www.sans.org/security-awareness/ouch-newsletter/2017/social-engineering
برامج إدارة كلمة المرور: https://www.sans.org/security-awareness-training/resources/password-managers-0
أهمية التحديثات: https://www.sans.org/security-awareness-training/resources/power-updating
هل لديك نسخة احتياطية لبياناتك؟: https://www.sans.org/security-awareness-training/resources/got-backups
لمراث الرقمى: https://www.sans.org/security-awareness-training/resources/digital-inheritance

ترجمها للعربية: محمد سرور، فؤاد أبو عويمر، درويش الحلو، اسلام الكرد
تنسر !OUCH من قبل فريق الوعى الأمنى فى SANS وتوزع بموجب الرخصة Creative Commons BY-NC-ND 4.0. لك الحرية فى المشاركة أو توزيع هذه النسرة الإخبارية شرط عدم تعديلها أو بيعها. الفريق التحريري: والت سكريفنس، فل هوفمان، ألان واغونر، شرلى كونلى