النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- مقدمة
- خمس محاور بسيطة
- حماية الأبناء عند زيارتهم لأصدقائهم أو أقاربهم

ساعد من حولك لحماية أنفسهم

مقدمة

الكثير منا يشعر بالراحة عند استخدام التقنية خصوصاً عند ما نعلم أننا نستخدمها بأمان. ولكن قد لا يشعر بعض أصدقائنا أو أفراد عائلتنا بذلك. وربما يشعرون بالخوف عند التعامل مع الأجهزة أو الاتصال بالإنترنت. وهذا يجعلهم عرضة لمخاطر الانترنت. استخدام التقنية لا يجب أن يكون مخيفاً، في الواقع الأمر بسيط جداً بمجرد فهم أساسيات أمن المعلومات. وقد تكون أفضل من يساعدهم على فهم هذه الأساسيات.

المحرر الضيف

راندي مارشيني (Twitter: @randymarchany) رئيس أمن المعلومات في معهد فرجينيا للتقنية، ومدرس معتمد في معهد سانس SANS.

خمس محاور بسيطة

هنا خمس محاور بسيطة يمكنك العمل من خلالها لمساعدة الآخرين للتغلب على تلك المخاوف والاستفادة بشكل آمن من التقنية. يمكنك معرفة المزيد حول كلٍ من هذه المحاور من خلال قائمة المصادرالإضافية في نهاية هذه النشرة.

١. **الهندسة الاجتماعية:** الهندسة الاجتماعية هي تقنية شائعة يستخدمها مجرمو الانترنت لإقناع المستخدمين للقيام بشيء لا ينبغي القيام به، مثل اطلاعهم على كلمة المرور الخاصة بهم، تحميل و تشغيل برامج مصابة على أجهزتهم أو الحصول على بيانات حساسة. هذا ليس شيئا جديدا، فالتحايل والخداع موجود منذ آلاف السنين. الفرق هنا ان مجرمي الانترنت يطبقون هذه المفاهيم من خلال شبكة الإنترنت. يمكنك مساعدة الآخرين من خلال اعلامهم بأكثر الأساليب التي يستخدمها مجرمو الإنترنت، مثلا عندما يطلب منهم شخص ما القيام بعمل معين بإلحاح شديد، أو عندما يبلغهم شخص ما بفوزهم بمبلغ ضخم أو هدية قيمة جداً، أو عندما يدعي شخص ما أنه أحد الأصدقاء القدامى ولكنه لا يعطي الكثير من المعلومات حول شخصيته. أطلع أصدقاءك ومعارفك على أمثلة من هذه الهجمات مثل رسائل التصيد من خلال البريد الإلكتروني أو المكالمات الهاتفية التي تدعي انها من الدعم الفني لشركة كبيرة (مايكروسوفت مثلاً). شيء آخر، أحرص دائما على ابلاغ جميع من حولك بأهمية المحافظة على سرية كلمات المرور الخاصة بهم وعدم إطلاع أي شخص عليها.
٢. **كلمات المرور:** كلمات المرور القوية أحد أهم الوسائل لحماية الأجهزة والحسابات على الانترنت. احرص على تعليم من حولك كيف يمكنهم إنشاء كلمات مرور قوية. تعتبر عبارات المرور خيار جيد حيث أنها أسهل في الكتابة والتذكر، فهي تتكون من عدة كلمات يسهل على المستخدم تذكرها ويكون من الصعب على مجرمي الشبكة تخمينها. تأكد من أنهم يستخدمون كلمات مرور مختلفة للحسابات المختلفة. بالإضافة إلى ذلك، يمكن اعلامهم بوجود تطبيقات تساعد على حفظ كلمات المرور بشكل آمن. إذا كان استخدام تطبيق إدارة

ساعد من حولك لحماية أنفسهم

ساعد الآخرين على استخدام التقنية بشكل أفضل من خلال هذه المحاور الخمس الأساسية.

كلمات المرور صعب عليهم، أبلغهم بكتابة كلمات المرور على ورقة وحفظها في مكان آمن للرجوع إليها عند الحاجة. وأخيرا، بالنسبة للحسابات الهامة والحساسة (حساب البنك مثلاً) يمكنك إعلامهم بوجود خيارات للتحقق الثنائي من شخصية المستخدم (المصادقة الثنائية). يعد التحقق الثنائي أحد أكثر الخطوات فعالية التي يمكنك اتخاذها.

٣. **تحديث الأنظمة**: من المهم الحفاظ على أنظمة تشغيل الأجهزة محدثة باستمرار فهي خطوة رئيسية لتأمينها. هذا الإجراء هام لجميع الأجهزة المحمولة، ولأي جهاز آخر متصل بالإنترنت مثل أجهزة الألعاب، والتلفاز أو حتى السماعات. أبسط طريقة لضمان أن جميع الأجهزة محدثة هو تمكين التحديث التلقائي كلما كان ذلك ممكناً.

٤. **مكافحة الفيروسات**: في بعض الأحيان نقوم بالنقر على الروابط أو تثبيت برامج ربما لا ينبغي أن نقوم بتثبيتها، الأمر الذي يمكن أن تصيب أجهزتنا بالبرمجيات الضارة. تم تصميم تطبيقات مكافحة البرمجيات الضارة لحمايتنا عند حدوث مثل تلك الأخطاء. في حين أن تطبيقات مكافحة البرمجيات الضارة لا يمكن أن توقف جميع البرمجات الضارة، لكنها تساعد على كشف ووقف الهجمات الأكثر شيوعا. تأكد من تثبيت وتفعيل تطبيق مكافحة البرمجيات الضارة على جميع الأجهزة العديد من تطبيقات مكافحة البرمجيات الضارة تحتوي على حلول أمنية إضافية مثل جدران الحماية واكتشاف المواقع الضارة.

٥. **النسخ الاحتياطي**: المحاور أعلاه لا تمنع حدوث الهجوم ولكنها تقلل من احتمالية نجاحه. عند تعرضك لهجوم قد تفقد بسببه بيانات هامة. النسخ الاحتياطي غالبا ما يكون الطريقة الوحيدة التي يمكن من خلالها استرداد البيانات إن تم حذفها بشكل خاطئ أو بسبب هجوم «ناجح» مثل هجوم طلب الفدية Ransomware. أعلم من حولك بضرورة استخدامهم لنظام نسخ احتياطي للملفات بشكل آلي. تتوفر حالياً العديد من التطبيقات التي تقوم بعمل نسخ احتياطي للملفات الخاصة بك على الحوسبة السحابية. يمكن تنفيذ النسخ الاحتياطي كل يوم أو كل ساعة أو كلما قمت بإجراء تغيير على ملف. هذه الحلول تسهل عملية النسخ الاحتياطي للبيانات واستعادة البيانات أيضاً.

حماية الأبناء عند زيارتهم لأصدقائهم أو أقاربهم

قد تكون اتخذت الاحتياطات اللازمة لحماية ابنائك عند استخدامهم للإنترنت في منزلك. لكن زيارة بعض الأقارب، مثل الأجداد، قد لا يكون لدى هؤلاء الأقارب مستوى الحماية المناسب إليك بعض الاجرآت التي يمكنك اتخاذها للمساعدة في حماية الأبناء عند زيارتهم للآخرين، وخاصة الأقارب

ساعد من حولك لحماية أنفسهم

- **شروط الاستخدام:** تأكد من أن الشروط التي تطبقها في المنزل لاستخدام الانترنت من قبل أبنائك معروفة للجميع. على سبيل المثال، أقصى مدة يمكن للأبناء استخدام الانترنت لكل يوم، من هم الأشخاص الذين يمكن لأبنائك التواصل واللعب معهم عبر الانترنت أو ما هي الألعاب التي يمكنهم أو لا يمكنهم اللعب بها؟ لا تدع أبنائك هم من يبلغ هذه الشروط بل قم بطباعة هذه الشروط وتوزيعها على أقاربك الذين يقوم أبنائك بزيارتهم بشكل متكرر.
- **التحكم:** بعض الأبناء لديهم معرفة جيدة باستخدام التقنية ربما أفضل من الكثير من الأقارب. فربما يقوم الابن بالحصول على كلمة المرور الخاصة بجهاز جده ومن خلال ذلك يتمكن من تحميل بعض البرامج او الألعاب التي قد لا ترغب في ان يقوم بتحميلها. تأكد من أن الأقارب يفهمون أنه لا ينبغي إعطاء الأبناء أي كلمات مرور أو تمكينهم من الوصول الى مستخدم بحقوق إدارية (administrator).

وأخيرا، أنصح من حولك بالاطلاع على نشرة أوتش! الشهرية حتى يمكنهم معرفة المزيد حول أمن المعلومات بأنفسهم. يتم نشر هذه النشرة مجانا بأكثر من 20 لغة. يمكن الاشتراك من خلال الرابط https://securingthehuman.sans.org/ouch.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول إلى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة securingthehuman.sans.org/ouch/archives.

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة و المتخصصين في أمن المعلومات.

مصادر إضافية

عدد أوتش بعنوان الهندسة الاجتماعية:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201701_aa.pdf
عدد أوتش بعنوان عِبَارات المُرور:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201704_aa.pdf
عدد أوتش بعنوان تطبيقات إدارة كلمات المرور:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201709_aa.pdf
عدد أوتش بعنوان التحقق باستخدام خطوتين:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_aa.pdf
عدد أوتش بعنوان النسخ الاحتياطي والاستعادة:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201708_aa.pdf
عدد أوتش بعنوان حماية الأطفال على الانترنت:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201705_aa.pdf

مجلس التحرير: والت سكريفن، فيل هوفمان، كاثي كليك، شيريل كونلي

ترجمها إلى العربية: طلال موسى الخروبي، محمد سرور