النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- أنت
- كلمات المرور
- التحديثات
- النسخ الاحتياطي

أربع محاور أساسية لكي تبقى بأمان

لمحة عامة

التقنية أصبحت أساسية في حياتنا وتطورها المستمر يجعل من الصعب الحماية من مخاطرها. دائما هناك إرشادات جديدة بشأن ما ينبغي أو لا ينبغي أن تقوم به. ومع ذلك، فإن تفاصيل كيفية البقاء بأمان قد تتغير مع مرور الوقت، دائما هناك أشياء أساسية يمكنك القيام بها لحماية نفسك. بغض النظر عن التقنية التي تستخدمها أو المكان الذي تعمل فيه، نوصي بأربع محاور أساسية. لمعرفة المزيد عن أي من المحاور أدناه، يرجى الرجوع إلى قسم المصادر الاضافية في نهاية هذه النشرة.

المحرر الضيف
ريان جونسون بعمل على التحقق من جهوزية المنظمات المختلفة للاستجابة المناسبة عند حدوث اختراقات في مجال امن المعلومات، يقوم ريان بتدريس تقنيات التحري المتقدمة في مجال أمن الشبكات في معهد سانس. يمكن متابعة ريان على تويتر (@ForensicRJ).

١. **أنت**: أولا وقبل كل شيء، ضع في اعتبارك أن التقنية وحدها لن تكون قادرة على توفير الحماية الكاملة لك. قد يلجأ مجرمو الانترنت على مهاجمة المستخدمين عوضاً عن محاولة اختراق تقنيات الحماية الحديثة. محاولة خداع المستخدم للحصول كلمة المرور أو رقم بطاقة الائتمان أو بعض البيانات الشخصية الخاصة أسهل بكثير من اختراق جهاز المستخدم للحصول على هذه المعلومات. على سبيل المثال، يمكنهم الاتصال والتظاهر بأنهم من الدعم الفني لشركة مايكروسوفت وإبلاغ المستخدم أن جهازه مصاب بأحد البرمجيات الخبيثة، ويحاولون اقناع المستخدم لإعطائهم صلاحية التحكم بجهازه. أو ربما تصلك رسالة بريد الكتروني تبلغك أن البضائع التي طلبتها لم تتمكن شركة البريد من تسليمها بسبب خطأ في العنوان وأن عليك تعديل العنوان من خلال رابط محدد، عند دخولك على الرابط المحدد يتم نقلك الى موقع خبيث من إعداد مجرمي الانترنت يتم بواسطته اختراق جهازك. هكذا تبدأ العديد من الهجمات مثل برمجيات الفدية Ransomware أو خدعة الرئيس التنفيذي CEO Fraud . في نهاية المطاف، أهم وسيلة دفاع ضد المهاجمين هو أنت. كن حذراً دائماً. باستخدام الحس السليم يمكنك ايقاف معظم الهجمات.

٢. **كلمات المرور**: المحور التالي لحماية نفسك هو استخدام كلمة مرور فريدة وقوية لكل من الأجهزة الخاصة بك وحساباتك على الانترنت. المفتاح هنا أن تكون كلمات قوية وفريدة من نوعها. كلمة مرور قوية تعني كلمة لا يمكن تخمينها بسهولة من قبل القراصنة أو

أربع محاور أساسية لكي تبقى بأمان

من قبل برمجيات اختراق كلمات المرور. مشكلة بعض كلمات المرور القوية أنه من الصعب تذكرها ويصعب ادخالها؟ حاول استخدام عبارة مرور بدلا من ذلك. بدلا من كلمة واحدة، استخدام عدة كلمات من السهل أن تتذكرها، مثل «أين كوب قهوتي؟». وكلما كانت عبارة المرور اطول كلما كانت أفضل. استخدام كلمة مرور مختلفة لكل جهاز وحساب على الإنترنت يحميك في حال تم اكتشاف إحدى كلمات المرور الخاصة بك، تبقى كل من حساباتك الأخرى والأجهزة آمنة. لا يستطيع الكثير من الناس تذكر جميع كلمات المرور الخاصة بهم، لذا ننصح باستخدام أحد تطبيقات إدارة كلمات المرور، وهي تطبيقات تقوم بتخزين كلمات المرور الخاصة بك بشكل آمن ومشفر.

هذه المحاور الأربع الرئيسية، تحقق حماية كبيرة لبياناتك وأجهزتك وأنت تتمتع باستخدام أحدث التقنيات.

وكحماية إضافية ننصح بتفعيل خاصية التحقق بخطوتين كلما كان ذلك ممكناً، فكلمات المرور وحدها لم تعد كافية لحماية الحسابات، ونحن جميعا بحاجة إلى شيء أقوى. التحقق بخطوتين يوفر حماية أفضل من كلمة المرور لوحدها. وهو يستخدم كلمة المرور الخاصة بك، ولكن يضيف وسيلة تحقق أخرى، مثل رمز يرسل كرسالة نصية إلى هاتفك. التحقق بخطوتين خطوة سهلة وفعالة لحماية نفسك.

٣. **التحديثات:** تأكد من أن أجهزة الكمبيوتر والأجهزة المحمولة والتطبيقات وأي شيء آخر متصل بالإنترنت يتم تحديثه باستمرار. مجرمو الإنترنت يبحثون باستمرار عن نقاط ضعف جديدة في البرامج المستخدمة على الأجهزة المختلفة. عندما يكتشفون نقطة ضعف في نظام معين، فإنهم يكتبون نصوصاً برمجية خاصة لاستغلال نقطة الضعف واختراق الأجهزة التي تعمل بذلك النظام. في الوقت نفسه، فإن الشركات التي أنشأت هذه الأنظمة تعمل على إصلاح أي نقاط ضعف تظهر في أنظمتهم عن طريق إطلاق التحديثات. فلا بد من تثبيت هذه التحديثات لإصلاح نقاط الضعف في تلك الأنظمة وبالتالي حماية الأجهزة من الاختراق. لكي تبقي أجهزتك محدثة دائما، ببساطة قم بتمكين التحديث التلقائي كلما كان ذلك ممكنا. طبق هذه القاعدة على أي جهاز مربوط بشبكة الانترنت، بما في ذلك التلفزيون والشاشات المتصلة بالإنترنت وأجهزة مراقبة الأطفال، وأجهزة الراوتر وأجهزة الألعاب وربما حتى السيارة. إذ كانت لديك أجهزة تستخدم أنظمة تشغيل قديمة لم تعد الشركات التي أنشأتها تقوم بإصدار تحديثات لها ، فإننا نوصي باستبدالها بأخرى جديدة معتمدة أو تغيير أنظمة التشغيل عليها إلى أنظمة تشغيل حديثة.

أربع محاور أساسية لكي تبقى بأمان

٤. **النسخ الاحتياطي:** مهما كان الانسان حذرا، قد يتم اختراق أحد أجهزته. وقد يكون الحل الوحيد الذي أمامه أن يقوم بحذف كافة البيانات ويعيد تسجيل جميع محتوياته من جديد. قد يقوم مخترق الجهاز بتشفير كافة البيانات على الجهاز المخترق أو مسحها بما في ذلك الملفات الشخصية والصور وغيرها من المعلومات المخزنة على النظام. غالبا ما تكون الطريقة الوحيدة لاستعادة كافة المعلومات الشخصية الخاصة بك هي النسخة الاحتياطية. تأكد من أنك تفعل النسخ الاحتياطي والقيام بالتحقق من أنك تستطيع استعادتهم عند الحاجة. معظم أنظمة التشغيل والأجهزة المحمولة تدعم النسخ الاحتياطي التلقائي. بالإضافة إلى ذلك، فإننا نوصي بتخزين نسخة احتياطية في الحوسبة السحابية Cloud أو في جهاز معزول عن الانترنت لحمايتها من الاختراق أو الإتلاف.

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 حول التصيد (باللغة الإنجليزية):	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_en.pdf
عدد أوتش حول مدير كلمات المرور (باللغة الإنجليزية):	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_en.pdf
عدد أوتش حول التحقق باستخدام خطوتين:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_aa.pdf
عدد أوتش حول عبارات المرور:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_aa.pdf
عدد أوتش حول النسخ الاحتياطي واستعادة البيانات:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_aa.pdf

مجلس التحرير: بيل وايمان، والت سكريفن، فيل هوفمان، لانس سبيتسر، كارمن رويل هاردي، شيريل كونلي
ترجمها إلى العربية: طلال موسى الخروبي، محمد سرور