أوتش! | أكتوبر (تشرين الأول) ٢٠١٤

النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- نظرة عامة
- خمس محاور رئيسية

خمس محاور تبقيك آمناً

نظرة عامة

كلما اكتسبت التكنولوجيا دورا أكثر أهمية في حياتنا، كلما ازدات التقنية تعقيدا. ونظرا لسرعة تغيرها، فإن مواكبة النصائح الأمنية يمكن أن تكون مربكة. ستجد أن هناك دائما إرشادات جديدة بشأن ماينبغي أو مالاينبغي أن تفعل. ومع ذلك، فحيث أن تفاصيل كيفية البقاء آمن قد تتغير مع مرور الوقت، فهناك دائما أشياء مهمة يمكنك القيام بها لحماية نفسك. بغض النظر عن التقنية التي تستخدمها حالياً أو المكان الذي تستخدم فيه هذه التكنولوجيا، نوصي بخمس خطوات رئيسية كالآتي.

المحرر الضيف

ليني زيلتسير يعمل في شركة NCR ضمن فريق ويركز على الحفاظ على أمن العملاء ويقم مقرر «البرمجيات الخبيثة» في معهد SANS. حساب ليني على تويتير **@lennyzeltser** ويكتب مدونة أمنية في **blog.zeltser.com**.

خمس محاور رئيسية

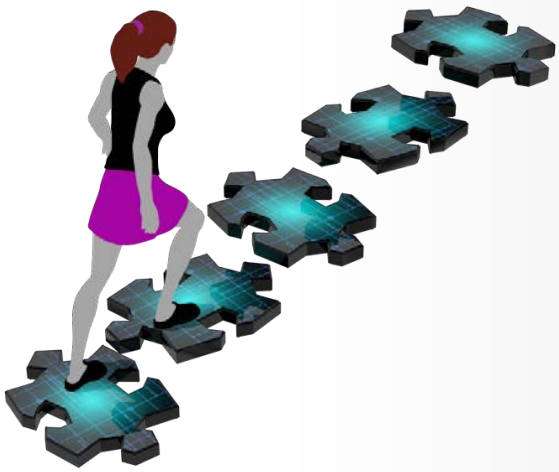
كل محور من هذه المحاور الخمس سنشرحه في ما يلي ولمعرفة المزيد حول كل محور، راجع «موارد اضافية» في نهاية النشرة.

١. **أنت:** أولا وقبل كل شيء، ضع في اعتبارك أن التكنولوجيا وحدها لا يمكن أن تحميك. المهاجمون تعلموا أن أسهل طريقة لتجاوز معظم التقنيات الأمنية هي من خلال مهاجمة المستخدم. إذا كانوا يريدون كلمة السر أو بطاقة الائتمان الخاصة بك فإن أسهل شيء بالنسبة لهم هوالقيام بالإحتيال عليك لكي تمنحهم هذه المعلومات. على سبيل المثال، يمكن أن يتصلوا بك هاتفيا ويتظاهروا بأنهم من شركة «مايكروسوفت» و يدعوا أن جهازك مصاب، وفي الواقع هم مجرمو إنترنت ويريدون أن يصلوا إلى جهازك. أو ربما يرسلوا لك رسالة بالبريد الإلكتروني توضح أن هناك بضاعة مرسلة لك ويطلب منك النقر على رابط لتأكيد عنوانك، و في الحقيقة أنه يراد منك زيارة موقع خبيث على شبكة الإنترنت لكي يخترق جهازك. في نهاية المطاف، أعظم دفاع ضد المهاجمين هو أنت. كن حذرا، بإستخدام الحس السليم يمكنك التغلب على معظم الهجمات.

٢. **التحديث:** تأكد أن جميع أجهزة الحاسب والأجهزة النقالة، والتطبيقات وأي جهاز آخر متصل بالشبكة يقوم بتشغيل أحدث إصدار من البرامج. مجرمو الإنترنت يبحثون باستمرار عن نقاط الضعف في التقنيات التي تستخدمها. عندما يكتشفون نقاط الضعف، يستخدمون برامج خاصة لإستغلال الضعف وإقتحام كل ما تستخدم بما في ذلك الشبكة، جهازك والأجهزة النقالة. وفي الوقت نفسه، يبذل مطوروا

خمس محاور تبقيك آمناً

البرمجيات مافي وسعهم للحفاظ على تحديث برامجهم. عند اكتشاف إحدى نقاط الضعف، فإن المطور يقوم بإصلاحها وطرح تحديث يحتوي ذلك الاصلاح وعليك عند ذلك الحصول على التحديث باسرع ما يمكن. من خلال تحديث أجهزة الحاسب والأجهزة النقالة، يمكنك تقليل عدد نقاط الضعف المعروفة، مما يجعل من الصعب إختراق جهازك. لضمان حصولك على أحدث تحديث، مكن التحديث التلقائي كلما أمكن ذلك. تنطبق هذه القاعدة على الاجهزة المتصلة بالشبكة، بما في ذلك التلفزيون والشاشات المتصلة بالإنترنت، أجهزة التوجيه المنزلية وأجهزة الألعاب. إذا كان نظام التشغيل، الخاص بالحاسب أو الجهاز المحمول أو أي جهاز آخر تستخدمه لم يعد معتمدا، ولن يتلقى أية تحديثات، نوصي بتغير ذلك النظام والحصول على اصدار جديد ومعتمد.



« هذه المحاور الخمس الرئيسية ، تعتبر الأهم لحماية نفسك وفي نفس الوقت تساعك على الاستفادة من أحدث التقنيات.

٣. **كلمات المرور**: الخطوة التالية لحماية نفسك تنطوي على استخدام كلمة مررو قوية و فريدة لكل من الأجهزة والحسابات والتطبيقات الخاصة بك. الكلمات الرئيسية هنا هي «قوية» و«فريدة». كلمة المرور القوية لا يمكن تخمينها بسهولة من قبل مجومو الإنترنت أو من قبل برامجهم الآلية. بدلا من كلمة واحدة، إستخدم كلمة مرور طويلة تتكون من كلمات متعددة مع بعض الرموز والأرقام. «فريدة» تعني إستخدام كلمة مرور مختلفة لكل حساب و جهاز على الانترنت. بهذه الطريقة إذا تم اكتشاف كلمة مرور واحدة، فكل حساباتك الأخرى لا تزال آمنة. لا يمكن أن نتذكر كل تلك الكلمات الفريدة و القوية؟ لا تقلق، لا يمكننا نحن كذلك. وهذا هو السبب في أننا نوصي بإستخدام أحد تطبيقات ادارة كلمات المرور وهو عبارة عن تطبيق مخصص للهاتف الذكي أو الحاسب يمكنك من تخزين جميع كلمات المرور الخاصة بك بشكل آمن و مشفر. أخيرا، إذا كان أي من حساباتك يدعم التحقق باستخدام خطوتين، نحن نوصي بشدة أن تمكن ذلك دائما لأن هذا الخيار هو واحد من أقوى الطرق لحماية حسابك.

٤. **التشفير**: وهو يضمن لك أنك أنت فقط و أشخاص تثق بهم يمكنهم الاطلاع على معلومات معينة. يمكن تشفير البيانات المخزنة على جهازك كما يمكنك تشفير المعلومات عند ارسالها عبر الشبكة. تشفير البيانات المخزنة على جهازك يعني حماية المعلومات المخزنة كملفات على القرص الثابت. معظم أنظمة التشغيل تسمح لك بتشفير بياناتك تلقائيا باستخدام ميزات مثل «تشفير القرص كاملا». ننصحك بتمكين هذه الميزة كلما أمكن ذلك. تشفير البيانات عند ارسالها عبر الشبكة يعني تشفير البيانات عندما تتنقل من جهازك إلى

خمس محاور تبقيك آمناً

أجهزة الآخرين. للتحقق من ان اتصالك بصفحة معينة (كصفحة البنك مثلا) عليك التأكد من أن عنوان الموقع الذي تزوره يبدأ ب « https» وأنه توجد صورة قفل مغلق بجانبه.

٥. **النسخ الإحتياطية:** مهما كنت حذراً قد يتعرض أحد من أجهزتك أو حساباتك للخطر. إذا حدث هذا، فخيارك الوحيد في كثير من الأحيان لضمان أن جهازك خالٍ من البرمجيات الخبيثة هو أن تمسح بشكل كامل كل المعلومات وتعيد بناء الجهاز «من الصفر». المهاجم قد يمنعك من الوصول إلى ملفاتك وصورك وغيرها من المعلومات المخزنة على النظام. الخيار الوحيد يمكن أن يكون بإستعادة كافة معلوماتك من النسخة الاحتياطية. تأكد من أنك تقوم بأخذ نسخ احتياطية بانتظام وتحقق من أنه يمكنك إستعادة المعلومات من هذه النسخ. معظم أنظمة التشغيل والأجهزة المحمولة تدعم النسخ الاحتياطي التلقائي.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول الى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة http://www.securingthehuman.org.

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة المتخصصين في أمن المعلومات بكلية علوم وهندسة الحاسب الآلي بجامعة الملك فهد للبترول والمعادن.

مصادر إضافية

Email Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
Securing Your New Tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Strong Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
Two-Step Verification:	http://www.securingthehuman.org/ouch/2013#august2013
Encryption:	http://www.securingthehuman.org/ouch/2014#august2014
Personal Backup and Recovery:	http://www.securingthehuman.org/ouch/2013#september2013

مجلس التحرير: بيل وايمان، والت سكريفن، فيل هوفمان، لانس سبيتسر، كارمن رويل هاردي
ترجمها إلى العربية: طلال موسى الخروبي، فرج أحمد عز الدين.