النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- الشبكة اللاسلكية الخاصة بك
- الأجهزة الخاصة بك

حماية شبكة المنزل الخاصة بك

لمحة عامة

خلال السنوات الماضية كانت الشبكات المنزلية أكثر سهولة، ليست سوى نقطة اتصال لاسلكية متصلة بجهاز حاسب آلي أو جهازين لتصفح الانترنت، للتسوق أو اللعب عبر الإنترنت. ولكن مؤخرًا، الشبكات المنزلية أصبحت أكثر تعقيداً. نحن الآن نستخدم الشبكات المنزلية لربط الأجهزة بالانترنت ليس فقط للتصفح أو تحميل الوسائط المتعددة. في هذا العدد سنتحدث عن كيفية إنشاء شبكة منزلية آمنة لك ولأسرتك.

المحرر الضيف

شيرل كونلي مديرة فريق التوعية الأمنية في Lockheed Martin، والتي ساهمت بتفعيل حملة I Campaign™ لتصل لأكثر من ١٠٠،٠٠٠ موظف. من مختلف التخصصات والمجالات في الشركة، بالإضافة لبرنامج التوعية العالمي من مخاطر الاصطياد الإلكتروني. تابع شيرل عبر **@conleychera**.

الشبكة اللاسلكية الخاصة بك

معظم الشبكات المنزلية تحتوي شبكة لاسلكية (Wi-Fi)، والتي تمكنك من توصيل أجهزتك بشكل لاسلكي بالإنترنت، بدءًا من الأجهزة المحمولة والحاسبات اللوحية وأجهزة الألعاب وحتى أجهزة التلفاز. أغلب هذه الشبكات المنزلية يتم ربطها من خلال جهاز ربط سلكي (وأحياناً لا سلكي) والذي يتم تثبيته عادةً من قبل مزوّد خدمة الإنترنت ليوصلك بشبكة الإنترنت. يقوم العديد من الناس بتوصيل الشبكة السلكية عبر وحدة مستقلة تسمى نقطة الاتصال اللاسلكية، والتي بدورها توصل الاجهزة بالإنترنت بغض النظر عن أي الطريقتين تستخدم لربط أجهزتك اللاسلكية، كلا الطريقتين تعمل بنفس الآلية عبر بث إشارة الشبكة اللاسلكية، ومختلف الأجهزة في منزلك تتصل بالشبكة اللاسلكية عبر هذه الإشارة. ومن ثم تستطيع هذه الأجهزة الوصول للإنترنت كبقية الأجهزة المتصلة بالشبكة المنزلية. وهذا يعني أن حماية الشبكة اللاسلكية هو عامل رئيسي لحماية الشبكة المنزلية الخاصة بك، ولذا ننصح باتباع النصائح التالية لحمايتها.

- تغيير كلمة مرور الافتراضية لحساب المشرف على نقطة الوصول الى شبكة الإنترنت أو الشبكة اللاسلكية. حساب المشرف هو الذى يسمح لك بتغيير إعدادات الشبكة اللاسلكية. العديد من نقاط الوصول اللاسلكية تأتى مع كلمة مرور إفتراضية معروفة وغالبا ما تنشر على شبكة الإنترنت. لذا تأكد من تغيير كلمة مرور المشرف إلى كلمة مرور قوية ولا تبلغ بها اي احد
- تغيير الاسم الافتراضي للشبكة اللاسلكية (التي تسمى أحيانا SSID). هذا هو الإسم الذى تبحث عنه أجهزتك عندما تريد الاتصال بالشبكة. إعطى شبكتك إسم مميز يمكنك التعرف عليه بسهولة، ولكن تأكد من أنه لا يحتوي على أي معلومات شخصية. لا فائدة تذكر من جعل شبكتك مخفية لأن معظم أدوات المسح اللاسلكي أو أي مهاجم ماهر يمكنه بسهولة اكتشاف الشبكات المخفية.

حماية شبكة المنزل الخاصة بك

لحماية شبكتك المنزلية، قم بتأمين الشبكة اللاسلكية وتحديثها وحماية جميع الأجهزة بكلمة مرور قوية.

- التأكد من أن الأشخاص الذين تثق بهم، هم فقط من يمكنهم الاتصال واستخدام الشبكة اللاسلكية الخاصة بك، و أن هذه الأتصالات مشفرة. قم بذلك عن طريق تمكين نظام تشفير قوي. ننصح باستخدام آلية « WPA2». من خلال استخدام هذه الالية، لا يمكن الاتصال بشبكة منزلك بدون أستخدام كلمة سر، وبمجرد التوصيل يتم تشفير جميع المعلومات المتبادلة على الإنترنت. تأكد من أنك لا تستخدم آلية تشفير قديمة مثل « WEP » أو أنك لا تستخدم أي تشفير فهذا يجعل شبكتك مفتوحة. الشبكات المفتوحة تسمح لأي شخص بالاتصال بالشبكة اللاسلكية الخاصة بك دون أي مصادقة.
- التأكد من أن كلمة المرور التي يستخدمها الأشخاص للاتصال بشبكتك اللاسلكية الخاصة بك هي كلمة قوية وأنها تختلف عن كلمة مرور المشرف. تذكر أنك على الأرجح تحتاج فقط إلى إدخال كلمة المرور مرة واحدة فقط لكل من الأجهزة الخاصة بك، لأن هذه الأجهزة تقوم بتخزين وتذكر كلمة المرور.
- العديد من الشبكات اللاسلكية تدعم ما يسمى بشبكة زائر. هذا يسمح للزوار بالاتصال بالإنترنت، ولكن يحمي شبكتك المنزلية لأنهم لا يتمكنون من الاتصال بأي من الأجهزة الأخرى على شبكتك المنزلية. إذا قمت بإضافة شبكة الزائر، تأكد من تمكين «WPA2» وكذلك كلمة مرور مختلفة لهذه الشبكة.
- عليك تعطيل خاصية الربط مع الشبكة الخاصة بك من دون معرفة كلمة المرور.
- إذا كان لديك صعوبة في تذكر كل كلمات المرور المختلفة، نوصيك باستخدام أحد برامج ادارة كلمات المرور ليخزنها لك بشكل آمن.

غير متأكد من كيفية القيام بهذه الخطوات؟ اطلب المساعدة من مزود خدمة الإنترنت، وتحقق من التعليمات المرفقة مع جهاز توجيه الإنترنت أو نقطة الوصول اللاسلكية أو الرجوع إلى موقع كل منهما.

الأجهزة الخاصة بك

الخطوة التالية هي معرفة ما هي الأجهزة المتصلة بشبكة منزلك والتأكد من أن كل تلك الأجهزة آمنة. قد يكون الأمر سهلا إذا كان عدد الأجهزة قليل. لكن هذه الايام والتي نريد أن نكون دائما مربوطين بشبكة الانترنت ونريد ربط كل شيء تقريباً بالشبكة الداخلية، بما في ذلك أجهزة التلفاز،

حماية شبكة المنزل الخاصة بك

أجهزة الألعاب، أجهزة مراقبة الأطفال، السماعات، الترموستات أو ربما حتى سيارتك. هنالك بعض التطبيقات التي تساعدك لاكتشاف الاجهزة المربوطة مع الشبكة المنزلية الخاصة بك مثل Fing. يمكنك تثبيت أحد هذه التطبيقات على جهاز الكمبيوتر أو الجوال وسيقوم هذا التطبيق بمسح الشبكة اللاسلكية الخاصة بك وتقديم تقرير عن كل جهاز متصل بها. عندما تحدد جميع الأجهزة على الشبكة المنزلية الخاصة بك، عليك التأكد من أن جميعها مؤمنة. أفضل طريقة للقيام بذلك هو ضمان تشغيل الإصدار الأحدث من نظام التشغيل على جميع الأجهزة. بالإضافة الي تمكين التحديث التلقائي عليها كلما أمكن ذلك. إذا كان أي من الأجهزة الخاصة بك تتطلب كلمة مرور، دائما استخدام كلمة مرور قوية ومختلفة عن الكلمات الأخرى. أخيرا، تأكد من زيارة موقع موفر خدمة الإنترنت حيث يقوم بعض مزودي الخدمة بتوفير تطبيقات مجانية تساعدك على تأمين الشبكة المنزلية الخاصة بك.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول إلى 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

عدد أوتش "عبارات المرور":	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_aa.pdf
عدد أوتش "إدارة كلمات المرور" باللغة الانجليزية:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_en.pdf
عدد أوتش "تأمين الجهاز اللوحي الجديد" باللغة الانجليزية:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_en.pdf
اصنع خارطة للشبكة المنزلية باللغة الانجليزية:	http://l.rud.is/home-network-mapping

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