أوتش! | فبراير (شباط) ، ٢٠١٥

النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- ضياع أوسرقة الأجهزة
- شبكات «واي فاي» العامة
- أجهزة الحاسب في الأماكن العامة

البقاء آمنا أثناء السفر

نظرة عامة

في هذه النشرة سنعرض كيفة الإتصال بشكل آمن بشبكة الإنترنت وإنجاز المهام أثناء السفر.

المحرر الضيف

ستيف آرمسترونغ هو المدير الفني ل «CyberCPR at Logically Secure» ، وهو مدرب معتمد ومؤلف لعدة دورات تدريبية في معهد سانز. يمكنك متابعته على تويتر **@Nebulator** وعلى جوجل **+SteveArmstrongSecurity**.

الإستعداد للسفر

الشبكة الخاصة بك في المنزل أو في شبكة جهة عملك تكون عادةً آمنة، و لكن أثناء السفر يجب أن نفترض دائما أن أي شبكة نقوم بالاتصال بها غير موثوقة. فنحن لا نعلم من يتصل بتلك الشبكة، وما التهديدات التي قد يشكلونها. نتحدث فى مايلى عن بعض التدابير التي ننصح بالقيام بها قبل السفر، بأسبوع أو أسبوعين، لحماية البيانات الخاصة بك أثناء السفر.

- حدد ما هي البيانات التي لن تحتاجها أثناء سفرك ثم قم بإزالتها من الجهاز الذي ستستخده أثناء السفر. هذا سيقلل من تأثير فقدان أو سرقة جهازك أو إذا تم حجزه من قبل الجهات الأمنية أو الجمركية أثناء سفرك. إذا كنت تسافر في مهمة عمل, استفسر إذا ما كانت توفر جهة عملك بعض الاجهزة لاستخدام الموظفين أثناء السفر.
- للسفر الدولي، تحقق من أشكال الوصلات الكهربائية التى تستخدم فى الدولة التي ستسافر إليها، قد تحتاج لأخذ وصلة كهربائية خاصة لتتمكن من شحن أجهزتك. وبالإضافة إلى ذلك، تحقق كذلك من شركة الاتصالات التي تتعامل معها لمعرفة تكاليف الاتصال بشبكة الانترنت في الدولة (الدول) التي ستتواجد بها أثناء سفرك. في الغالب يكلف استخدام البيانات أثناء السفر اسعارا مرتفعة جداً، لهذا ننصحك بعدم السماح لجهازك الجوال بالاتصال بالانترنت أثناء السفر دوليا أو عليك الاشتراك في خدمة انترنت دولي بسعر مناسب.
- ثبت أحد البرامج التى تمكنك من تتبع جهازك عن بعد، كما تمكنك ايضا ان مسح بيانات الجهاز إذا تمت سرقته أو فقدانه. العديد من الأجهزة الذكية تحوي هذه الخاصية، عليك تمكينها والجهاز بحوزتك لتتمكن من استخدامها في حال فقد منك. تذكر أن هذه البرامج تتطلب أن يكون الجهاز متصلاً بالإنترنت لتقوم بمهمتها.

قبل السفر بيوم أو يومين:

البقاء آمنا أثناء السفر

- حدث جميع التطبيقات والبرمجيات المضادة للفيروسات بحيث تقوم بتشغيل أحدث الإصدارات.
- قم بتفعيل كافة إعدادات الأمان المناسبة على جهازك، مثل جدار الحماية.
- استخدم كلمة مرور قوية لقفل جميع الأجهزة النقالة الخاصة بك, فبهذه الطريقة لا يستطيع أحد الوصول إلى معلوماتك الخاصة في حال إذا فقدت جهازك.
- قم بتشفير كافة البيانات جميع الأجهزة الخاصة بك بحيث إذا فقدت أو سرقت، فإن البيانات لا يمكن الوصول إليها. بعض الأجهزة مثل «اى فون» تقوم بالتشفير تلقائيا إذا قمت بتعيين كلمة أو رمز مرور على الجهاز.
- قم بعمل نسخة احتياطية كاملة لجهازك. بهذه الطريقة إذا حدث أى شيء أثناء السفر فان لديك نسخة من المعلومات محفوضة في موقع آمن.

للبقاء آمناً أثناء السفر عليك تأمين الأجهزة الخاصة بك قبل أن تغادر المنزل، حافظ عليها في مكانٍ آمن، واستخدم التشفير عند الاتصال بالإنترنت.

ضياع أوسرقة الأجهزة

كن حذراً أثناء السفر حتى لا تفقد أجهزتك بضياع أو سرقة. على سبيل المثال، لا تترك الأجهزة في السيارة بحيث يمكن للمارة رؤيتها بسهولة، فقد يقوم أحدهم بكسر زجاج السيارة للإستيلاء على ما فيها. كما ننصح أن تستخدم الكيبل الخاص بربط أجهزة الحاسب المحمول إذا أمكن ذلك. بالرغم من انتشار السرقات بشكل كبير إلا أن إحتمالية فقدان جهازك تقدر ب 15 مرة أكثر من احتمالية سرقته. حيث يمكن أن تتفقد جهازك في أحد المطارات أو في سيارة أجرة أو في أحد المطاعم، أو عند مغادرتك غرفة الفندق أو قبل النزول من الطائرة.

شبكات «واي فاي» العامة

الوصول إلى الإنترنت أثناء السفر في كثير من الأحيان يعني استخدام نقاط «واي فاي» العامة، مثل تلك التي توفرها الفنادق أو المقاهى أو المطارات. تكمن المشكلة مع نقاط «واي فاي» أن من يديرها قد لا يكون موثوقاً كما أن من يتصل بها غير معروف لديك. لذا ينبغي التعامل مع هذه الشبكات على أنها غير آمنة. في الواقع لهذا السبب اقترحنا الاحتياطات السابقة لتأمين أجهزتك قبل أن تسافر.

بالاضافة إلى ذلك، شبكة «الواي فاي» تستخدم موجات الراديو للاتصال، مما يعني أن أي شخص بالقرب منك يمكنه أن يراقب اتصالاتك. لهذا السبب عليك استخدام التشفير في جميع اتصالاتك عند استخدام شبكة «واي فاي» العامة. فمثلاً عند الاتصال عبر الانترنت باستخدام المتصفح، تأكد من أن المواقع التي تزورها تستخدم التشفير (يكون هذا واضحاً عندما ترى صورة قفل مغلق في أسفل المتصفح). بالنسبة للاتصالا الخاصة بالعمل فنقترح استخدام ما يسمى (الشبكة الافتراضية الخاصة) والتي تشفر كل البيانات المتبادلة عند استخدامها. يمكنك

البقاء آمنا أثناء السفر

طلب حساب خاص لهذه الخدمة من مكتب الدعم الفني بجهة عملك. كما يمكنك الحصول على حساب للاستخدام الشخصمن إحد مزودي الخدمة. إذا كنت تشعر بالقلق من عدم وجود نقاط «واي فاي» العامة يمكنك الوثوق بها، يمكنك الاتصال بالأنترنت من خلال هاتفك الذكي. (تحذير: كما ذكرنا سابقا، هذا الاتصال عادةً ما يكون مكلفا جدا عند السفر، تحقق مع مزود الخدمة أولا).

أجهزة الحاسب في الأماكن العامة

لا تستخدم أي أجهزة حاسب عامة، مثل أجهزة الحاسب في الفنادق والمكتبات أو في مقاهي الإنترنت. فأن لا تعرف من الذي استخدم هذا الجهاز قبلك، قد يكون هذا الجهاز مصاباً بأحد البرامج المؤذية بقصد أو بدون قصد. كلما أمكن ذلك، استخدم أجهزة يمكنك التحكم والثقة بها. إذا كان لابد من استخدام جهاز حاسب عام، لا تستخدم أي خدمة تتطلب منك تسجيل الدخول أو كتابة كلمة المرور الخاصة بك.

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

عدد أوتش "تطبيقات إدارة كلمات المرور ":	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_aa.pdf
عدد أوتش "التحقق بخطوتين ":	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_aa.pdf
عدد أوتش "التشفير ":	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201408_aa.pdf
عدد أوتش "تأمين الكمبيوتر اللوحي":	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201312_aa.pdf
تقرير فيرايزون للإختراق 2014 (باللغة الانجليزية):	http://www.verizonenterprise.com/DBIR/2014/

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

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus