آوتش! | فبراير ٢٠١٧

النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- الاستعداد للسفر.
- فقدان الأجهزة أو سرقتها
- الربط مع شبكات واي فاي Wi-Fi.
- أجهزة الحاسوب العامة.

حافظ علي أمن بياناتك اثناء السفر

تمهيد

نريد الحصول على أقصى فائدة من التكنولوجيا في جميع الأوقات، بما في ذلك عند السفر. في هذه النشرة سوف نعرض كيف يمكنك الاتصال بالإنترنت واستخدام أجهزتك بشكل آمن أثناء السفر.

المحرر الضيف

مارك وليامز هو «مهندس المؤسسة الأمنية» في بلويشيلد بلوكروس في ولاية تينيسي. وهو أيضا مدرب في سانز SANS ورئيس فرع «شاتانوغا ISSA «. سافر كثيراً ولديه معرفة واسعة بالمخاطر المتوقعة أثناء السفر.

الاستعداد للسفر

شبكة منزلك أو مكان عملك عادة ما تكون آمنة، لكن أثناء السفر يجب أن نفترض أن أي شبكة اتصال اخرى لا يمكن الوثوق بها. أنت لا تعلم من يستطيع الاتصال بتلك الشبكات وماذا يمكنه أن يفعل. هنا بعض الخطوات البسيطة التي سوف تؤمن بشكل كبير الحماية لك ولبياناتك قبل السفر.

- البيانات المؤمنة جيدا هي التي لن تأخذها معك عند سفرك. قم بتحديد ما هي البيانات التي لن تحتاج إليها والبيانات التي سوف تحملها معك. هذا يمكن أن يقلل إلى حد كبير خطر تعرض بياناتك للكشف في حال فقدان جهازك أو سرقته أو تم التحفظ عليها من قبل الجمارك أو أمن الحدود مثلاً. إذا كانت رحلتك تخص العمل اسال قسم تقنية المعلومات في جهة عملك إذا كان هناك أجهزة مخصصة للسفر.
- اقفل الأجهزة الخاصة بك بكلمة مرور قوية. بهذه الطريقة اذا سرقت أو فقدت، لا يمكن الوصول إلى البيانات الخاصة بك عليها. وبالإضافة إلى ذلك، قم بتثبيت او تفعيل تشفير القرص الكامل على أجهزة الهاتف المحمول وأجهزة الحاسوب المحمولة. بالنسبة لمعظم الأجهزة المحمولة ، يتم تمكين هذا تلقائيا عند استخدام قفل الشاشة screenlock.
- تثبيت أو تمكين تطبيق على جهازك يمكنك من تتبعه عن بعد، ومسح بياناتك الموجودة عليه إذا تم سرقة الجهاز او فقدانه.
- قم بتحديث الأجهزة والتطبيقات وبرنامج مضاد للفيروسات قبل أن تسافر بحيث تقوم بتشغيل أحدث الإصدارات. حيث تركز العديد من الهجمات على الأنظمة و البرامج القديمة والغير محدثة.
- خد نسخة احتياطية كاملة من جميع بياناتك. بهذه الطريقة إذا حدث شيء ما لأجهزتك أثناء السفر لا يزال لديك نسخة من البيانات الأصلية في مكان آمن.

حافظ علي أمن بياناتك اثناء السفر

- بالنسبة للسفر الدولي، تحقق من شركة الجوال التي تتعامل معها لمعرفة تكاليف الاتصال بالإنترنت من جوالك في البلد الذي تسافر إليه. في كثير من الأحيان تكون التكاليف عالية جداً. لذا ننصح بإيقاف خاصية البيانات أثناء التجوال و شراء شريحة بيانات أو اتصال مسبق الدفع من البلد الذي تسافر إليه.

للبقاء أمنا أثناء السفر، عليك تأمين الأجهزة الخاصة بك قبل مغادرة المنزل والاحتفاظ بها في مكان آمن وتشفير جميع الأنشطة عند الدخول إلى الإنترنت من شبكات واي فاي العامة.

فقدان الأجهزة أو سرقتها

بمجرد أن تبدأ السفر حافظ علي سلامة أجهزتك، على سبيل المثال لا تترك الأجهزة في السيارة بحيث يمكن للناس أن تراهم بسهولة، ببساطة يستطيع أي شخص تحطيم زجاج السيارة والاستيلاء على أي شيء ذي قيمة يمكن أن يراه. وفقا لدراسة أجرتها شركة فرايزون للاتصالات Verizon، أن احتمالية فقد الجهاز تصل لأكثر من 100 ضعف من احتمالية سرقته. لذا تحق بشكل دائم ومتكرر من أن الأجهزة دائما معك، وخصوصاً بعد التفتيش الامني في المطار، أو عند النزول من سيارة الأجرة أو الخروج من مطعم، أو عند مغادرة غرفتك في الفندق أو قبل النزول من الطائرة. وتذكر دائما تفقد جيب مقعد الطائرة أو سيارة الأجرة.

الربط مع شبكات واي فاي Wi-Fi.

الوصول إلى الإنترنت أثناء السفر في كثير من الأحيان يعني استخدام نقاط وصول الواي فاي Wi-Fi العامة، مثل تلك التي توجد في الفندق، المقهى أو المطار. هناك مشكلتان مع خدمة الواي فاي Wi-Fi في الأماكن العامة: لا تستطيع معرفة من يشغلها و لا من يستخدمها. لذلك ينبغي النظر اليها أنها غير آمنة. في الواقع هذا هو أهم سبب لأخذ الاحتياطات اللازمة لتأمين أجهزتك قبل السفر. وبالإضافة إلى ذلك، تستخدم خدمة الواي فاي موجات الراديو، وهذا يمكن أي شخص يتواجد بالقرب منك من مراقبة اتصالك. لهذه الأسباب، إذا كنت تستخدم واي فاي Wi-Fi في الأماكن العامة، تحتاج إلى التأكد من أن كل نشاطك على شبكة الإنترنت مشفرة. على سبيل المثال، عند الاتصال عبر الانترنت باستخدام المتصفح الخاص بك تأكد من أن المواقع التي تزورها مشفرة. يمكنك التأكد من هذا من خلال البحث عن HTTPS:// أو صورة قفل مغلق في شريط العنوان. وبالإضافة إلى ذلك، قد يكون لديك ما يسمى VPN (الشبكة الافتراضية الخاصة) التي تقوم بتشفير كل من نشاطك على شبكة الإنترنت. يمكنك الحصول على ال VPN من جهة عملك كما يمكنك شراء نسخة للاستخدام الشخصي. إذا كنت قلقا أنه

حافظ علي أمن بياناتك اثناء السفر

لا يوجد واي فاي Wi-Fi يمكنك الوثوق بها، استخدم اتصال البيانات عبر شبكة الهاتف الخاص بك. تحذير: كما ذكرنا سابقا، هذا يمكن أن تكون مكلفا عند السفر دوليا، تحقق مع مزود خدمة الجوال الخاص بك أولا.

أجهزة الحاسب العامة

لا تستخدم أجهزة الحاسب العامة، مثل تلك الموجودة في الفنادق أو في مقاهي الإنترنت، لتسجيل الدخول إلى أي من حساباتك أو الوصول إلى المعلومات الحساسة. فأنت لا تعرف من الذي استخدم الجهاز قبلك، وقد يكون الجهاز مصاب بأحد البرمجيات الخبيثة (بتعمد من مستخدم سابق أو ربما دون قصد منه). استخدام الأجهزة التي تثق بها وتستطيع التحكم بها كلما كان ذلك ممكنا. يمكنك استخدام أجهزة الحاسب العامة للحصول على معلومات عامة مثل أحوال الطقس أو تصفح الاخبار. اذا قمت بتسجيل الدخول إلى أي من حساباتك كحساب جوجل مثلاً فكأنك وجهت دعوة للقراصنة لاختراق حسابك.

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

عبارات المرور: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_aa.pdf

النسخ الاحتياطي واستعادة البيانات: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_aa.pdf

ما هي البرمجيات الخبيثة: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_aa.pdf

التشفير: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201606_aa.pdf

مجلس التحرير: بيل وايمان، والت سكريفن، فيل هوفمان، لانس سبيتسنر، كارمن رويل هاردي، شيريل كونلي

ترجمها إلى العربية: طلال موسى الخروبي، محمد سرور