النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

استخدام تطبيقات الأجهزة الذكية بشكل آمن

لمحة عامة

المحرر الضيف

جوشوا رايت Joshua Wright مدير تقني في مؤسسة Counter Hack وأيضا مدرب في سانز SANS . مؤلف دورة امن الأجهزة المحمولة و القرصنة الأخلاقية و كشف اسرار القرصنة لشبكات الواي فاي تطبيقات الأجهزة الذكية بشكل آمن SEC575. تابع جوش علي تويتر **@joswr1ght**.

الأجهزة اللوحية والهواتف الذكية واحدة من التقنيات الأساسية التي نستخدمها في حياتنا الشخصية والمهنية على حد سواء. والذي يجعل الاجهزة المحمولة متعددة الجوانب والاستخدامات توفر ملايين التطبيقات التي يمكننا الاختيار بينها. هذه التطبيقات تمكننا ان نكون اكثر انتاجية وسرعة في التواصل والمشاركة مع الاخرين. كما تتوفر تطبيقات تعليمية وترفيهية في مختلف المجالات ومختلف الأعمار. لكن هناك مخاطر عديدة قد تحدث عند استخدام تلك التطبيقات. وإليك بعض الخطوات التي يمكنك اتخاذها لاستخدام هذه التطبيقات بشكل آمن.

الحصول على تطبيقات الأجهزة الذكية

الخطوة الاولى يجب عليك التأكد من تحميل التطبيقات من مصادر آمنة وموثوقة. حيث أن قراصنة الانترنت لديهم القدرة على إنشاء وتوزيع تطبيقات خبيثة لمختلف الأجهزة الذكية تبدو كأنها شرعية. عند تثبيتك لأي من هذه التطبيقات يتمكن القراصنة من السيطرة على جهازك المحمول. عن طريق تحميل التطبيقات من مصادر موثوقة وآمنة تقلل احتمالية ثبيت تطبيق خبيث. ماقد لاتدركه هو ان نوع الجهاز المحمول الذي تستخدمه يحدد الخيارات الخاصة بك عند تحميل التطبيقات. حيث ان اجهزة ابل مثل أي-باد و أي-فون يمكنها فقط تحميل تطبيقات الجوال من متجر ابل. وميزة هذا ان إدارة متجر ابل تقوم بفحص لجميع التطبيقات قبل اتاحتها على المتجر. قد لا تستطيع إدارة المتجر اكتشاف جميع التطبيقات المصابة .ولكنها تقوم بإزالة التطبيقات التي تكتشف أو تشتبه بها انها خبيثة.

يستخدم نظام ويندوز للأجهزة الذكية نهجا مماثلاً لأبل لإدارة متجر التطبيقات. أما نظام اندرويد فيمنح مستخدميه مرونة أكبر حيث يسمح بتنزيل التطبيقات من اي موقع على شبكة الانترنت .لكن هذه المرونة تتطلب منك أن تكون اكثر حذرا عند تنزيل التطبيقات من مواقع غير موثوقة. لقد تمكنت جوجل من تطوير متجر لتطبيقات المحمول مماثل لشركه ابل واسمته

استخدام تطبيقات الأجهزة الذكية بشكل آمن

Google play. وتقوم إدارة متجر قوقل بمراجعة التطبيقات قبل نشرها. لذا نوصي بشدة بتحميل تطبيقات أندرويد من متجر Google play فقط.

ولمزيد من الحماية يمكنك تثبيت أحد تطبيقات مكافحة الفيروسات على جهازك الذكي. بغض النظر عن الجهاز الذي تستخدمه، ننصحك بتجنب تنزيل التطبيقات الجديدة، أو التي تم تحميلها من عدد قليل من المستخدمين، أو التي ليس لها سوى عدد قليل جدا من التعليقات الإيجابية.التطبيقات المتاحة منذ مدة طويلة وتم تحميلها من قبل عدد كبير من الناس وتحتوي على الكثير من التعليقات الايجابية هي فقط الموثوق فيها ويمكنك تحميلها . بالاضافة الى ذلك ثبت فقط التطبيقات التي تحتاجها وتستخدمها .اسال نفسك هل انا فعلا احتاج لهذا التطبيق؟ حيث ان هذه التطبيقات لا تجلب فقط نقاط ضعف جديدة ولكن من المحتمل ان تنتهك خصوصيتك. عندما تتوقف عن استخدام تطبيق معين نوصي بحذفه من جهازك.

صمام الأمان لاستخدام تطبيقات الأجهزة الذكية بشكل آمن هو تثبيت التطبيقات من مصادر موثوق بها فقط، وتثبيت تحديثاتها عندما تكون متاحة، ومنح أذونات التطبيق بحذر.

أخيرا.. لاتقم بعمل كسر لحماية جهازك باستخدام jailbreak او root. هذه العملية تسمح بتحميل تطبيقات غير شرعية علي جهازك وتقوم بتغير الكثير من وظائف الجهاز. ولا تقتصر على بعض الميزات الأمنية في جهازك ولكن تؤدي ايضا الي فقدان الضمان والدعم الفني للجهاز من الشركة المصنعة.

الصلاحيات

عندما تقوم بتثبيت تطبيقات الجوال من مصدر موثوق .تأكد من إعداده بامان وحماية خصوصيتك. دائما فكر قبل اعطاء السماح لتطبيقات الجوال بالدخول، هل تريد منح التطبيق الصلاحية التي يطالب بها؟ هل انت تحتاج هذا التطبيق حقا ؟ على سبيل المثال بعض التطبيقات تستخدم الموقع الجغرافي اذا سمحت لهذا التطبيق بمعرفة موقعك دائما . يمكن لصاحب التطبيق ان يتعقب تحركاتك وبالتالي يتمكن من بيع تلك المعلومات للاخرين .اذا كنت لاترغب في منح هذه الصلاحيات وتم رفض طلبك من قبل التطبيق يمكنك تحميل تطبيق اخر يلبي الاحتياجات الخاصة بك. تذكر، لديك الكثير من الخيارات.

استخدام تطبيقات الأجهزة الذكية بشكل آمن

تحديث التطبيقات

تطبيقات الجوال يجب تحديثها باستمرار تماما مثل أنظمة التشغيل لأجهزة الكمبيوتر و المحمول. حيث ان المخترقون يبحثون باستمرار عن نقاط الضعف في التطبيقات ليطوروا هجمات لاستغلال نقاط الضعف هذه .كما ان المطورون الذين انشأوا النظام يقومون باطلاق تحديثات جديدة لاصلاح نقاط الضعف وحماية الجهاز المحمول الخاص بك. لذلك من الافضل ان تتاكد دائما من تثبيت التحديثات . معظم الأجهزة تتيح ميزة التحديث التلقائي للتطبيقات. نوصي بتفعيل هذه الميزة لجميع التطبيقات على جهازك. إذا لم يكن ذلك ممكنا، فإننا ننصح ان تتحقق كل أسبوعين على الأقل للحصول على تحديثات لتطبيقات الجوال الخاص بك. وأخيرا، عندما يتم تحديث التطبيقات دائما تأكد من الصلاحيات الجديدة لتلك التطبيقات وعل ترغب باستمرار استخدامها.

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 "الهندسة الاجتماعية":	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201701_aa.pdf
عدد أوتش حول "تخلص بأمان من هاتفك المحمول":	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201612_aa.pdf
عدد أوتش حول "أمن جهاز التابلت الجديد" (باللغة الانجليزية):	https://securingthehuman.sans.org/ouch/2016#january2016
ارشيف نشرة أوتش:	https://securingthehuman.sans.org/ouch/archives
دورة في أمن أجهزة المحمول:	https://sans.org/sec575

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

ترجمها إلى العربية: طلال موسى الخروبي، محمد سرور