النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- **ما هو التشفير؟**
- **تشفير البيانات عند تخزينها**
- **تشفير البيانات عند ارسالها**

التشفير

ما هو التشفير؟

فقد تسمع الكثير من الناس تستخدام مصطلح «التشفير» وكيف يجب استخدامه لحماية نفسك والمعلومات الخاصة بك. ومع ذلك، قد يبدو مفهوم التشفير غامضا بعض الشيء كما أن التشفير لا يمكنه حمايتك من كل شيء. في هذه النشرة نشرح بعبارات بسيطة جداً ما هو التشفير

المحرر الضيف

كريستوفر كراولي (**@CCrowMontance**; **+ChrisCrowley**) هو مستشار يسكن في واشنطن عاصمة الولايات المتحدة الامريكية. وهو المدرب الرئيسي مقرر «أمن الأجهزة المحمولة و القرصنة الأخلاقية (SEC575) ومؤلف مقرر «إدارة فريق الاستجابة للحوادث (MGT535)

ولماذا يجب استخدامه وكيفية تنفيذ ذلك بشكل صحيح.

لديك كمية هائلة من المعلومات الحساسة على الأجهزة الخاصة بك، مثل المستندات المالية، والصور، والبريد الإلكتروني، و السجلات الطبية. ماذا سيحصل اذا فقدت أحد هذه الاجهزة أو سرق منك؟ ستكون كل تلك المعلومات مالية جداً عرضةً لأن يطلع عليها أشخاص آخرون. يمكن لمجرمي الشبكة استخدام بعض هذه المعلومات لاجراء معاملات المالية أو التسوق من خلال حساباتك البنكية. اذا كانت البيانات على جهازك مشفرة فلن يتمكن غيرك من الإطلاع عليها وبالتالي لن يتمكن من استغلالها.

عندما لا يتم تشفير البيانات، فهذا يعني أن أي شخص يمكنه بسهولة قراءة هذه البيانات أو الوصول إليها. تشفير هذه البيانات يحولها لشكل غير قابل للقراءة و يسمى نص مشفر. يتم التشفير باستخدام عمليات حسابية معقدة باستخدام «مفتاح» سري لتحويل البيانات الخاصة بك إلى نص مشفر. يجب استخدام المفتاح لتشفير أو لفك تشفير البيانات، تماما كما نستخدم مفتاح الباب لفتح أو قفل الباب. يمكن اعتبار كلمة المرور كمفتاح التشفير بحيث يتمكن الشخص الذي يعرف كلمة المرور من الوصول إلى البيانات الخاصة بك. لحماية المعلومات الخاصة بك مشفرة تحتاج إلى حماية المفتاح الخاص بك. بشكل عام يمكن تشفير البيانات عند تخزينها (مثل البيانات المخزنة على جهازك المحمول) كما يمكن تشفير البيانات عند ارسالها (مثل نقل المعلومات عبر الإنترنت) .

تشفير البيانات عند تخزينها

الهدف الرئيسي لتشفير البيانات عند تخزينها هو حماية البيانات في حالة فقدان أو سرقة الجهاز الخاص بك. منذ خمسة عشر عاماً لم تكن المشكلة كبيرة حيث كانت معظم أجهزة الحاسب الآلي كبيرة وثقيلة ومن الصعب تحركها. أم الآن فالأجهزة المحمولة خفيفة وسهلة النقل ومع

التشـفير

ذلـك فهـي أجهـزة عاليـة المواصفـات وسـعتها التخزينيـة كبـيرة. كمـا أن وسـائط التخزيـن الحاليـة (مثـل USB فـلاش) كبـيرة السـعة وخفيفـة الحمـل ويمكـن فقدهـا بسـهولة. الأن توفـر أنظمـة التشـغيل الحديثـة خاصيـة تشـفير القـرص الكامـل (FDE) وهـذا يعـني أن كل البيانـات الـتي يتـم تخزينها يتـم تشـفيرها تلقائياً. فما عليـك فعلـه ببسـاطة هـو تفعيـل هـذه الخاصيـة. عـلى سـبيل المثـال، اذا كان لديـك نظـام التشـغيل Mac OS X فيمكنـك اسـتخدام FileVault أمـا بالنسـبة لنظـام Windows فيمكنـك اسـتخدام Bitlocker إذا كان نظـام التشـغيل لديـك يدعـم «تشـفير كامـل القـرص»، نحـن نـوصي بشـدة بتفعيـل هـذه الخاصيـة. كمـا تدعـم معظـم الهواتـف الذكيـة خاصيـة «تشـفير القـرص الكامـل» لأجهـزة التخزيـن الداخليـة الخاصـة بهـا بمجـرد أن يقـوم المسـتخدم باختيـار رمـز مـرور لقفـل الهاتـف. لمعرفـة مـا إذا كان جهـازك يدعـم هـذه الخاصـة يمكنـك الاستفسـار مـن الشركـة المصنعـة أو البحـث عـن الموضـوع عـبر الإنترنـت.

التشـفير وسـيلة قوية للحفاظ على سرية المعلومات الخاصة بك، ولكن قوة التشـفير تعتمد على قوة وسرية مفتاح التشـفير الخاص بك.

تشفير البيانات عند ارسالها

عنـد اسـتخدامك للشـبكات السـلكية أو الاسـلكية فانـك تقـوم بارسـال بيانـات مـن جهـازك عـبر الشـبكة الـى اجهـزة اخـرى وخـلال الارسـال تكـون هـذه البيانـات معرضـه لأن يطلـع عليهـا الآخـرون. إذا لـم يتـم تشـفير البيانـات قبـل ارسـالها، فإنـه يمكـن أن يقـوم أحدهـم برصـد وتسـجيل البيانـات الـتي قـام جهـازك بارسـالها. لـذا, فمـن المهـم جـدا أن يتـم تشـفير البيانـات قبـل ارسـلها وخصوصـا عندمـا تتصـل عـلى موقـع البنـك الخـاص بـك أو عندمـا تقـوم باسـتعراض بريـدك الالكـتروني، أو ربمـا حـتى عنـد الدخـول عـلى مواقـع التواصـل الاجتماعـي. نظـام التشـفير الاكـثر اسـتخداما عـلى الشـبكة هـو نظـام HTTPS. وهـذا يعـني أن جميـع البيانـات المتبادلـة بـين متصفـح الانترنـت الـذي تسـتخدمه وموقـع الانترنـت الـذي تتصفحـة مشـفرة. يمكنـك معرفـة ان البيانـات المتبادلـة يتـم تشـفيرها مـن خـلال وجـود عبـارة https:// في عنـوان الموقـع أو عندمـا يتحـول لـون شريـط العنـوان URL الى أخـضر أو عنـد ظهـور ايقونـة القفـل عـلى شاشـة المسـتعرض (قـد تشـاهد الثـلاث علامـات سـويا في بعـض المتصفحـات). عنـد الاتصـال بشـبكة واي فـاي عامـة، تأكـد مـن اسـتخدام التشـفير عندمـا يكـون ذلـك ممكنـاً. كمـا ننصحـك باسـتخدام التشـفير عنـد دخولـك لموقـع البريـد الإلكـتروني الخـاص بـك. يمكـن لموفـر خدمـة الإنترنـت الخـاص بـك مسـاعدتك في تمكـين التشـفير.

تنفيذ التشفير بشكل صحيح

بغض النظر عن نوع التشفير الذي تستخدمه عليك اتباع النصائح التالية لاستخدامه بشكل صحيح.

التشـفير

- عليك الحفاظ على مفتاح التشفير بشكل سري واختياره بشكل يصعب تخمينه، فمهما كانت عملية التشفير قوية فسيكون من السهل كشف البيانات المشفرة اذا تم كشف المفتاح
- إذا كنت تستخدم كلمة مرور لحفظ مفتاح التشفير، تأكد من أنها كلمة مرور قوية وحافظ عليها بشكل سري وآمن لأن فقدها أو نسيانها سيسبب كشف بياناتك أو فقدها.
- إذا حدث أن تم اختراق جهازك من خلال الشبكة فذلك يمكن المهاجم من الاطلاع على بياناتك دون الحاجة لمعرفة مفتاح التشفير،لذا عليك انخاذ الاحتياطات اللازمة لابقاء جهازك آمن ضد الاختراق.
- عليك دائما اختيار أقوى أنواع التشفير المتاحة لديك.

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

مصادر إضافية

نظام تشفير OS X-FileVault (باللغة الانجليزية):	http://support.apple.com/kb/ht4790
نظام تشفير iOS (باللغة الانجليزية):	http://support.apple.com/kb/ht4175
نظام تشفير Android (باللغة الانجليزية):	http://www.androidauthority.com/how-to-encrypt-android-device-326700
نظام تشفير Windows 7 (باللغة الانجليزية):	http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
عدد أوتش "سبع خطوات لجهاز حاسب آلي آمن":	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201212_aa.pdf
عدد أوتش "تطبيقات ادارة كلمات المرور" :	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_aa.pdf

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