النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- ما هو التشفير ؟
- ما الذي تستطيع تشفيره ؟
- التشفير بالشكل الصحيح

التشفير

ما هو التشفير ؟

ربما سمعت من البعض كلمة «التشفير» وأهمية استخدامه لحماية ملفاتك وتعاملاتك التقنية. ولكن في الحقيقة التشفير قد يكون أكثر تعقيدًا من ذلك وعليك أن تفهم إمكانياته وحدوده. في هذا العدد سنشرح التشفير بشكل مبسط وكيف يمكن استخدامه بالشكل الصحيح لحمايتك.

المحرر الضيف
فرانسيسكا بوسكو (**@francibosco**) باحثة وتدير عدة مشاريع متعلقة بأمن المعلومات، الجرائم الإلكترونية، والاستخدام التخريبي للتقنية. تعمل في معهد أبحاث الجريمة والعدالة الاقليمي التابع للأمم المتحدة، أحد مؤسسي مركز التقنية والقانون Tech and Law Cente.

لدي الكثير منا العديد من الملفات الهامة والحساسة موزعة في أجهزة متعددة. في حال سرقة أو ضياع أحد هذه الأجهزة، ربما يتمكن من يحصل على ذلك الجهاز من الاطلاع على تلك الملفات الحساسة والمهمة. وكذلك الحال بالنسبة لتعاملاتك المالية أو الشرائية عبر الإنترنت، أي شخص يستطيع مراقبة هذه العمليات ربما يتمكن من سرقة بياناتك وحسابك البنكي أو رقم بطاقة الائتمان. التشفير يحميك في هذه الحالات المختلفة من خلال ضمان عدم قدرة أي شخص غير مصرّح له من الوصول أو تعديل بياناتك الحساسة.

فكرة التشفير قديمة منذ آلاف السنين، واليوم التشفير أكثر تعقيدًا من الأمس، ولكنّه يؤدي نفس الغرض- نقل رسالة بشكل سرّي من مكانٍ إلى آخر، مع ضمان حفظ سرية المعلومة بحيث يتمكن من يُصرّح له فقط بالاطلاع عليها. عندما تكون المعلومات غير مشفرة تسمى نص عادي (plain-text)، وهي تعني أن أي شخص قادر على قراءتها والوصول لها. التشفير يحول هذه المعلومات إلى نص غير قابل للقراءة يسمى نص مشفّر (cipher-text). التشفير اليوم يتم من خلال استخدام عمليات رياضية معقدة وباستعمال مفاتيح محددة لتحويل المعلومات إلى نص مشفّر. هذه المفاتيح هي التي تغلق الوصول إلى المعلومات المشفرة أو تفتحه. وفي معظم الحالات، ترتبط هذه المفاتيح بكلمة المرور أو رمز الدخول الخاص بمستخدم الجهاز.

ما الذي تستطيع تشفيره ؟

سنوضح فيما يلي أهمية تشفير البيانات المخزنة وتشفير البيانات اثناء ارسالها من خلال شبكة الانترنت تشفير البيانات الخزنة أمر هام لحماية المعلومات في حالة فقدان جهازك أو سرقته. الأجهزة المحمولة والهواتف الذكية تحتوى على قدر كبير من المعلومات، ولكن للاسف

التشـفير

يمكـن فقـدان أو سرقـة هـذه الأجهـزة بسـهولة، كمـا هـي الحـال مـع وسـائط التخزيـن المتنقلـة مثـل الأقـراص المدمجـة، ذاكـرة الفـلاش أو الأقـراص الصلبـة الخارجيـة. توفـر معظـم الاجهـزة الحديثـة خاصيـة تشـفير كافـة البيانـات المخزنـة عليهـا. تحتـاج في الاغلـب لتفعيـل هـذه الخاصيـة ليتـم تشـفير كل مـا تقـوم بتخزينـه تلقائيـا، ولـن تحتـاج لتصنيـف البيانـات كبيانـات يجـب تشـفيرها وبيانـات لا يجـب تشـفيرها. اليـوم، معظـم أجهـزة الحاسـب تـأتي مـع خيـار «تشـفير القـرص الكامـل»، ويمكـن أن تمكـن هـذا الخيـار تلقائيـا أو يدويـا. هـذا الخيـار يسـمى بتسـميات مختلفـة بأختـلاف نظـام التشـغيل.

هـو طريقـة قويـة لمسـاعدتك على تأمـين بياناتك، لكـن قوتـه تعتمد عـلى قوة مفتاح التشـفير الخاص بك.

عنـد ارسـال البيانـات مـن خـلال شـبكة الانترنـت تكـون عرضـة للخطـر. إذا لـم يتـم تشـفير هـذه البيانـات، فإنـه يمكـن لمجرمـي الشـبكة الاطـلاع عليهـا أو تعديلهـا. لـذا فعليـك التأكـد مـن أن جميـع المعلومات الحساسـة الـتي يتـم تبادلهـا عـبر الإنترنـت تتـم مـن خـلال اتصـال مشـفر. أحـد أكـثر أنـواع التشـفير شـيوعا عـلى الانترنـت الـذي يتـم مـن خـلال المواقـع الـتي تبـدأ ب https. هـذا يعـني أن جميـع اليانـات المتبادلـة بـين المتصفـح عـلى جهـازك وموقـع الانترنـت يتـم تشـفيرها. عندمـا تقوم بالتصـال بأحـد المواقـع الـتي توفـر هـذه الخاصيـة سـتجد رمـز القفـل في المتصفـح الخـاص بـك، (وربمـا تحـول شريـط عنـوان صفحـة الانترنـت إلى اللـون الأخـضر في بعـض برامـج التصفـح). مثـال آخـر عـلى تشـفير البيانـات عنـد ارسـالها يتـم مـن خـلال تشـفير رسـائل البريـد الإلكـتروني. حيـث توفـر معظـم برامـج البريـد الإلكـتروني خاصيـة التشـفير للرسـائل المرسـلة والمسـتقبلة ويمكنـك تفعيـل هـذه الخاصيـة اذا رغبـت في ذلـك مثـالٌ ثالـث هـو تشـفير الرسـائل المتبادلـة مـن خـلال برامـج الدردشـة مثـل إي-مسـج، ويكـر، سـقنل، واتـس-أب أو تيليقـرام. تفعيـل التشـفير في هـذه التطبيقـات يمنـع الآخريـن مـن الوصـول إلى البيانـات أو الصـور الـتي يتـم تبادلهـا.

التشفير بالشكل الصحيح

لكي تكون متأكدا من حماية بياناتك بواسطة التشفير، من المهم جدا التأكد من استخدامه بالشكل الصحيح.

- قـوة التشـفير تعتمـد بشـكل أسـاسي عـلى قـوة مفتـاح التشـفير، إذا اسـتطاع أي شـخص تخمينـه او الحصـول عليـه ، سـوف يصـل الي جميـع البيانـات المشـفرة باسـتخدام ذلـك المفتـاح. قـم بحمايـة مفتاتيـح التشـفير الخاصـة بـك. إذا كنـت تسـتخدم عبـارة مـرور لحمايـة مفتـاح

التشـفير

التشفير، تأكد من انها كلمة مرور قوية, كلما زاد طول الكلمة وتعقيدها كلما كان إكتشافها أو تخمينها أصعب. لا تنسي كلمة المرور الخاصة بالتشفير أو مفتاح التشفير فبدون ذلك لن تستطيع فك تشفير بياناتك والوصول اليها. إذا كنت لا تستطيع تذكر كلمات المرور قم باستخدام أحد برامج إدارة كلمات المرور.

- أمر آخر يؤثر في قوة التشفير هو مدى أمان الأجهزة المستخدمة. إذا كان تم اختراق جهازك أو أصيب بأحد البرمجيات الخبيثة فقد يستطيع مخترق الجهاز من تخطي التشفير والوصول الي بياناتك. من الهام جدا أن تتخدد إجراءات اخري لتأمين أجهزتك وتحديث برنامج مكافحة البرمجيات الخبيثة باستمرار.
- العديد من تطبيقات المحمول وتطبيقات الحاسوب تقدم خدمات التشفير لحماية بياناتك واتصالاتك. إذا كانت تطبيقاتك لا تقدم خدمة التشفير قم بالبحث عن بديل عنها.

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

مصادر إضافية: ماهو التشفير وكيف يعمل (باللغة الانجليزية):	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
عدد أوتش: عبارات المرور:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_aa.pdf
عدد أوتش: إدارة كلمات المرور (باللغة الانجليزية):	https://securingthehuman.sans.org/ouch/2015#october2015
عدد أوتش: ما هي البرمجيات الخبيثة:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_aa.pdf
عدد أوتش: تأمين الجهاز اللوحي الجديد(باللغة الانجليزية):	https://securingthehuman.sans.org/ouch/2016#january2016

مجلس التحرير: بيل وايمان، والت سكريفن، فيل هوفمان، لانس سبيتسنر، كارمن رويل هاردي, شيريل كونلي
ترجمها إلى العربية: طلال موسى الخروبي، فرج أحمد عز الدين, محمد سرور، زياد الشهري.