THE JOURNALIST SURVIVAL GUIDE

ANANIMATEDVIDEOGUIDE

SK eyes
Samir Kassir eyes

الدرس ١٣
كيفية تخزين وتبادل البيانات المشفّرة

أهميته

إنّ حماية محرّكات الأقراص الصلبة بواسطة كلمات السرّ أمرٌ لا يجدي نفعاً. فمن السهل جداً فصل القرص الصلب عن الكمبيوتر النقّال، ومن ثم الدخول إليه من كمبيوتر آخر، تماماً كما تفعل عندما تطّلع على محتويات أيّ قرص صلب تستخدمه لتخزين البيانات أو الاحتفاظ بنسخة احتياطية عنها. فضلاً عن ذلك، يحدث كثيراً أن تفقد معظم الأجهزة الصغيرة (كشرائح الذاكرة أو أجهزة الكمبيوتر النقال إلخ.)، أو تُسرق منك بكلّ سهولة.

من هنا، لعلّ استخدام تقنية التشفير يساعدك على حماية بياناتك الأكثر دقة والحفاظ على أمنها.

ما هو التشفير؟

التشفير هو استخدام الرياضيات بطريقة ذكية لتشفير المعلومات أو إعادة ترتيبها، بحيث لا يتمكّن من قراءتها أو فك تشفيرها إلا الشخص الذي يملك معلومة محدّدة، ككلمة سرّ أو مفتاح تشفير مثلاً.

ستبدو هذه البيانات- بالنسبة لشخص يحاول قراءة وثيقة مشفّرة من البيانات دونما الاستعانة بكلمة سر، أو مفتاح لإلغاء تأمين المعلومات- أشبه بسلسلة عشوائية من الأرقام والأحرف والرموز الأخرى. ولا يخفى عليك أنّ تخزين البيانات السرية قد يعرّضك للخطر، أنت والأشخاص الذين تعمل معهم. ومع أنّ التشفير يخفّف من هذا الخطر إلا أنه لا يلغيه تماماً. من هنا، تتمثّل الخطوة الأولى لحماية المعلومات الحسّاسة بالتخفيف من كميّتها المتوافرة على أجهزة الكمبيوتر. فإذا لم يكن من سبب مقنع يدفعك إلى تخزين ملفّ معيّن، أو نوعٍ محدّد من المعلومات ضمن ملفّ، من الأفضل بكلّ بساطة أن تقوم بحذفه.

«تروكربت» (Truecrypt)

«تروكربت» أداةٌ تمكّنك من إنشاء حاويات تخزين مشفّرة تخفي فيها كلّ ملفّاتك الحسّاسة. يشبه عمل هذه الأداة خزانة حديدية مقفولة تُحفظ فيها البيانات؛ وهي تتمتّع بعدة خصائص مهمّة تتيح لك تصميم استراتيجية أمن المعلومات كما يناسبك. فضلاً عن ذلك، يتيح لك «تروكربت» إمكانية تشفير قرص الكمبيوتر بأكمله، بما في ذلك ملفّاتك كافة، والملفّات المؤقتة التي تقوم بإنشائها خلال عملك، وكل البرامج التي تنزّلها، إضافةً إلى كل ملفات نظام تشغيل «وندوز». جديرٌ بالذكر أنّ «تروكربت» يدعم إمكانية إنشاء المجلّدات المشفّرة (وهي أقسام في جهاز يمكنها تخزين الملفّات بشكلٍ منفصل عن النظام الأساسي) على أجهزة تخزين محمولة. كما يقدّم ميزة «الإنكار/إخفاء الهوية»، حيث يجعل مجلّدات التخزين المشفّرة تبدو وكأنها أيّ ملفات أخرى، على غرار الأفلام والوثائق وملفّات الموسيقى.

للمزيد من المعلومات عن «تروكربت»: *https://securityinabox.org/en/truecrypt_main*

«جي. بي. جي. ٤ يو. إس. بي» (GPG٤USB)

«GPG٤USB» هو برنامج محمول، خفيف الوزن وبسيط يتيح لك تشفير الرسائل والملفّات، أو فكّ تشفيرها. وهو يقوم على تشفير مفتاح عام. وفقاً لهذه الطريقة، يجدر بكلّ شخص أن يستحصل على مفتاحَين خاصّين به. الأول يُعرف بالمفتاح الشخصي (أو السري)، ويكون محمياً بكلمة سرّ أو عبارة وصول، ولا يجوز إطلاع أحد عليه. أما الثاني، فيُعرف بالمفتاح العام، ويمكن تبادله مع أيّ من مراسليك، كما يمكن لمراسليك أن يطلعوك على مفاتيحهم العامة بدورهم (للمزيد من المعلومات عن تبادل المفاتيح، أنقر هنا).

ما إن تحصل على المفتاح العام لمراسلك، حتى يصبح بإمكانك أن ترسل إليه رسائل إلكترونية مشفّرة. وسيكون المراسل الشخص الوحيد القادر على فكّ تشفير رسائلك الإلكترونية وقراءتها، لأنه الوحيد الذي يملك حقّ استعمال المفتاح الشخصي المطابق. نسجاً على المنوال نفسه، إذا أرسلت نسخةً عن مفتاحك العام إلى جهات الاتصال المدرجة في بريدك الإلكتروني، من دون أن تطلعهم على المفتاح الشخصي المطابق، ستكون الوحيد القادر على قراءة الرسائل المشفّرة التي يبعث بها إليك هؤلاء الأشخاص.

ملاحظة: تنبّه إلى أنّ النسخة الأصلية وغير المشفّرة لوثائقك وملفّاتك قد تبقى موجودةً على جهازك الكمبيوتر. فتذكّرا، أنت ومراسلك، أن تحذفا هذه النسخ عن أجهزة الكمبيوتر كلّما دعت الحاجة إلى ذلك.

للمزيد من المعلومات حول برنامج «GPG٤USB»:
https://securityinabox.org/en/gpg4usb-keysimportexport

برنامج «بدجن» للدردشة خارج السجل

«بدجن» برنامج مجّاني ومفتوح المصدر للتراسل الفوريّ، يتيح لك تنظيم وترتيب مختلف حساباتك الشخصية للتراسل الفوري ضمن واجهة واحدة. لكن قبل أن تبدأ باستخدام «بدجن»، يجب أن تكون قد فتحتَ حساباً للتراسل الفوري، تقوم بتسجيله في ما بعد ضمن برنامج «بدجن». على سبيل المثال، إذا كنت تملك حساب بريد إلكتروني على «جيمايل»، يمكنك عندئذ استعمال خدمة «غوغل توك» للتراسل الفوري، التابعة لـ«جيمايل»، بواسطة «بدجن». فما عليك إلا استعمال معلومات الدخول نفسها التي تستخدمها للاطلاع على حسابك الحالي كي تسجّل دخولك إلى حسابك عبر «بدجن».

ملاحظة: نشجّع جميع المستخدمين على الاطلاع على أكبر قدر ممكن من المعلومات عن سياسات الخصوصية والأمن المعتمدة لدى البرنامج الذي يزوّدهم بخدمة التراسل الفوري. ومن المراجع المفيدة في هذا المجال، نذكر TOS-DR.

تعتبر خدمة الدردشة خارج السجل أداة ملحقة طُوّرت خصيصاً من أجل برنامج «بدجن». وهي تؤمّن ميزات الخصوصية والأمن التالية:
المصادقة: أنت على يقين من أنّ المراسل لا يكذب بشأن هويّته.
الإنكار/إخفاء الهوية: بعد انتهاء جلسة الدردشة، لن يعود بالإمكان التحديد إن كانت الرسائل صادرة عنك أو عن مراسلك.
التشفير: لا يمكن لأحد غيرك الوصول إلى رسائلك الفورية وقراءتها.
للمزيد من المعلومات عن الدردشة خارج السجل بواسطة برنامج «بدجن»: *https://securityinabox.org/en/pidgin_main*

إنتاج:
مركز الدفاع عن الحريات الإعلامية والثقافية «سكايز» – مؤسسة سمير قصير

تم إعداد محتوى الفيديو بمساعدة من:
فريق تكنولوجيا المعلومات والاتصالات في المعهد الديمقراطي الوطني للشؤون الدولية

المنتج التنفيذي: **مارون صفير**
تصميم وتحريك: **kook creative studio**

مستشار تقني: **أندرو كود**
ترجمة: **نور الأسعد**
صوت (عربي): **ريما خداج**
الصوت (انجليزي): **أندرو كود**
تسجيل الصوت: **Creative Impact**
موسيقى: **«Mining by Moonlight» by Kevin MacLeod**

تم تنفيذ هذا المشروع بفضل دعم **الصندوق الوطني للديمقراطية.**