THE JOURNALIST SURVIVAL GUIDE

ANANIMATEDVIDEOGUIDE

Samir Kassir eyes

الدرس ٧

كيف تحمي الكمبيوتر من القرصنة والبرمجيات الخبيثة

أهميّتها

كما هي الحال عند تشييد بيت، من الضروري أن ترسي أساساً قويّاً قبل أن تشرع في بناء البيت من فوقه. فإذا كانت البرمجيات الخبيثة قد استشرت في نظام الكمبيوتر الخاص بك، أو كان تكهّن كلمات السرّ لكلّ حساباتك أمراً في غاية السهولة، سيمسي أيّ برنامج إضافي لحماية البيانات عديم الجدوى.

لعلّ الخطوة الأساسية الأولى هي التأكّد من أنّ نظام التشغيل خالٍ من الفيروسات والبرمجيات الخبيثة الأخرى. فضلاً عن ذلك، تشكّل كلمات السرّ الخطوة الأولى للدخول إلى أيٍّ من المحتويات الخاصة بك (البريد الإلكتروني، وسائل الإعلام الاجتماعي، حساب «سكايب»، الصور وغيرها) المخزّنة على شبكة الإنترنت.

برنامج مضاد للفيروسات

ما هو الفيروس؟

الفيروس نوع من أنواع البرمجيات الخبيثة التي يمكن أن تتلف المعلومات الموجودة داخل جهاز الكمبيوتر، أو تضرّ بها أو تلوّثها، بما في ذلك البيانات الموجودة على محرّكات الأقراص الخارجية. كما يمكنها أن تتحكّم بجهازك وتستخدمه لشنّ هجمات على أجهزة كمبيوتر أخرى.

تنتشر الكثير من هذه الفيروسات عبر الإنترنت، سواء عن طريق البريد الإلكتروني أم الصفحات الإلكترونية الخبيثة أم غيرها من الوسائل المعتمدة لنقل الفيروسات إلى أجهزة الكمبيوتر غير المحمية. كما ينتشر نوعٌ آخر من الفيروسات عبر الوسائط القابلة للإزالة، وبخاصة أدوات مثل شرائح الذاكرة (يو. إس. بي) ومحرّكات الأقراص الصلبة الخارجية التي تتيح للمستخدمين كتابة المعلومات وقراءتها أيضاً.

الوقاية من الإصابة بالفيروس

كن حذراً جداً عند فتح الملفّات المرفقة بالبريد الإلكتروني. ويُفضّل ألا تفتح أيّ ملف مرفق إذا وردك من مصدر غير معروف. أما إذا اضطررت لفعل ذلك، فيجدر بك أولاً حفظ الملف المرفق ضمن مجلّد على جهاز الكمبيوتر، ومن فتح التطبيق الملائم بنفسك (مثل «مايكروسوفت وورد» أو «أدوبي أكروبات»). فإذا لجأتَ إلى القائمة «ملفّ» في البرنامج المذكور لفتح الوثائق المرفقة بطريقة يدوية، عوضاً عن نقرها مرّتين أو السماح لبرنامج البريد الإلكتروني بفتحها تلقائياً، ستكون أقل عرضةً لالتقاط فيروس.

فكّر في المخاطر المحتملة قبل إدراج الوسائط القابلة للإزالة في جهاز الكمبيوتر الخاص بك، مثل الأقراص المدمجة وأقراص الفيديو الرقمية وشرائح الذاكرة (يو. إس. بي). تحقّق أولاً إذا كان برنامج مكافحة الفيروسات في الكمبيوتر قد خضع لآخر التحديثات اللازمة، وتأكّد من أنه شغّالٌ كما يجب. ولا ضير أيضاً من تعطيل ميزة «القراءة التلقائية» لنظام التشغيل، لا سيّما وأنّ الفيروسات قد تستغلّ هذه الميزة لإصابة جهازك. أما السبيل إلى تعطيلها في برنامج «ويندوز إكس. بي»، فمن خلال الدخول إلى جهاز الكمبيوتر، ونقر الزرّ الأيمن للفأرة على محرّك الأقراص المدمجة أو أقراص الفيديو الرقمية، ومن ثم اختيار الخصائص والنقر على خانة القراءة التلقائية. بعد ذلك، إختر، بالنسبة لكلّ نوع من أنواع المحتويات، زرّ «لا تقم بأيّ إجراء» أو «إسألني اختيار إجراء كلّ مرة»، ثم أنقر علامة الموافقة.

يمكنك أيضاً الحؤول دون الإصابة بالفيروسات من خلال الانتقال إلى البرمجيات الحرّة والمفتوحة المصدر التي تعتبر غالباً أكثر أماناً، ولا تكون هدفاً منتظماً لصانعي الفيروسات كغيرها من البرامج.

من أهمّ الأدوات لمكافحة الفيروسات، نذكر «أفاست» المتوفّرة على أجهزة «وندوز» و«ماك» على السواء.

استخدام برنامج مكافحة الفيروسات على نحو فعّال

لا تشغّل برنامجَين لمكافحة الفيروسات في الوقت نفسه. فمن المحتمل أن يؤدي ذلك إلى تباطؤ سرعة الكمبيوتر أو تعطّله بالكامل. قم بإلغاء تثبيت أحد البرنامجين، قبل أن تبدأ بتنزيل الآخر.

تأكّد من أنّ برنامج مكافحة الفيروسات الذي اخترته يتيح لك إجراء تحديثات. فلا يخفى عليك أنّ العديد من الأدوات التجارية التي يتمّ تنزيلها على أجهزة الكمبيوتر الجديدة، قبل شرائها، تشترط على المستخدم تسجيل اسمه (وتسديد ثمن معيّن) في مرحلة معيّنة وإلا عجز عن إجراء المزيد من التحديثات. لكن، تجدر الإشارة إلى أنّ جميع البرمجيات التي توصي بها هذه الوثيقة تسمح بإجراء التحديثات مجّاناً.

تأكّد من أن برنامج مكافحة الفيروسات يحدّث نفسه بشكل منتظم. فخبراء الإنترنت يصنعون الفيروسات الجديدة وينشرونها كلّ يوم، وبالتالي

سرعان ما سيمسي جهازك عرضةً للهجمات إذا لم تحرص على مواكبة التطوّر في مجال تعريفات الفيروسات الجديدة. في هذا الإطار، يقوم برنامج «أفاست»، عندما تكون متّصلاً بشبكة الإنترنت، بالبحث عن التحديثات تلقائياً.
إذا كان جهاز مكافحة الفيروسات يتضمّن ميزة كشف الفيروسات، مكّنها بحيث تكون «شغّالة دائماً». جديرٌ بالذكر أنّ معظم الأدوات المختلفة تتضمّن ميزةً كهذه، وإن اختلفت في أسمائها. قد تحمل اسم «حماية لحظية» أو «حماية دائمة» أو ما شابه.
إمسح كلّ الملفّات في جهاز الكمبيوتر بانتظام لتتأكّد من خلّوها من الفيروسات. ليس من الداعي تنفيذ هذه الخطوة يومياً (لا سيّما إذا كنتَ قد مكّنتَ ميزة «شغّالة دائماً» في برنامج مكافحة الفيروسات، كما هو مبيّن أعلاه)، لكن لا بدّ من تنفيذها بين الحين والآخر. أما معدّل إجراء هذه المسح، فيختلف باختلاف الظروف. هل أوصلتَ جهازك بشبكات مجهولة مؤخّراً؟ مع من كنتَ تتشارك في استخدام شرائح الذاكرة؟ هل تصلك بانتظام مرفقات غريبة عبر البريد الإلكتروني؟ هل عانى شخص آخر في منزلك أو مكتبك مشكلات مع الفيروسات مؤخّراً؟ إذا أجبتَ بنعم عن أيٍّ من هذه الأسئلة، يجدر بك مسح نظام الكمبيوتر بأسرع ما يمكن.

الحماية من برامج التجسس

ما هو برنامج التجسس؟

برنامج التجسس هو نوع من أنواع البرمجيات الخبيثة التي يمكنها تتبّع سير عملك، سواء على جهاز الكمبيوتر أم عبر الإنترنت، فإرسال المعلومات المستخلصة إلى شخصٍ، ما كان يجدر به الاطلاع عليها. يمكن لهذه البرامج أن تسجّل الحروف التي تنضدها على لوحة المفاتيح، فضلاً عن حركات الفأرة، والمواقع التي تتصفّحها، والبرامج التي تشغّلها وما إلى هنالك. نتيجةً لذلك، بوسع هذه البرامج أن تقوّض من مستوى أمن جهازك، كما تكشف معلومات سريّة عنك وعن نشاطاتك ومعارفك. تلتقط أجهزة الكمبيوتر برامج التجسّس بالطريقة نفسها التي تلتقط فيها الفيروسات، وبالتالي يمكن الاستناد إلى العديد من الاقتراحات المذكورة أعلاه للتحصّن ضدّ هذا الصنف الثاني من البرمجيات الخبيثة.

الوقاية من برامج التجسّس

إبقَ متنبّهاً عند تصفّح المواقع الإلكترونية. تنبّه لنوافذ المتصفّح التي تُفتح تلقائياً، واقرأها بتمعّن عوضاً عن مجرّد نقر زرّ نعم أو كلا. عندما ينتابك الشك، إختر إغلاق «النوافذ المنبثقة» من خلال نقر حرف X عند الزاوية العليا في أقصى اليمين، عوضاً عن الاكتفاء بنقر زرّ «إلغاء». يمكن لهذا الأمر هذا أن يمنع الصفحات الإلكترونية من الاحتيال عليك لتنزيل البرمجيات الخبيثة على جهاز الكمبيوتر الخاص بك. إياك والموافقة على تشغيل هذا النوع من المحتويات إذا كان وارداً من مواقع إلكترونية لا تعرفها أو لا تثق بها.

لمكافحة برامج التجسّس بشكل روتيني، ننصحك باستخدام أداة مكافحة برامج التجسس، المعروفة باسم «سبايبوت» (Spybot)، التي تمسح جهاز الكمبيوتر الخاص بك (تماماً كما يفعل برنامج مكافحة الفيروسات) وتتخلّص، بطريقة آمنة، من برامج التجسّس التي تتعقّب أثر نشاطاتك على الكمبيوتر.

كلمات السرّ

كيف تختار كلمة سرّ قوية

عند اختيار كلمة السرّ، يجب أن تراعي الخصائص الأساسية التالية:
الطول: يجب أن تتكوّن كلمة السرّ من ٨ أحرف أو علامات على الأقل
القوّة: يجب أن تراعي التنوّع (إستخدم أحرفاً مختلفة، ورموزاً، وانتقِ أحرفاً مختلفة الأحجام)
التناوب: غيّر كلمات السرّ على أساس شبه منتظم
إحرص على تبديل كلمات السرّ لأهمّ حساباتك الشخصية (الفايسبوك، البريد الإلكتروني إلخ.)
الفرادة: لا تستخدم كلمات السر نفسها مراراً وتكراراً

من الطرق المعتمدة لتذكّر كلمة السرّ هي استخدام «عبارة وصول» مؤلّفة من عدّة كلمات- عادةً ٤ كلمات عشوائية أو أكثر.
حتى وإن انتقيتَ كلمات سرّ أسهل حفظاً بنسبةٍ طفيفة، سيكون من المستحيل تقريباً حفظ كلمة سرّ مميّزة لجميع المواقع الإلكترونية التي تملك حسابات شخصية فيها. لذا، إستخدم برنامجاً لإدارة كلمات السرّ مجانياً ومفتوح المصدر، مثل «كي باس» (Keepass) كي يسهّل عليك هذه المهمّة.
بوسع برنامج «كي باس» أن يخزّن جميع كلمات السرّ الخاصة بك، بما فيها كلمة السرّ الرئيسة للدخول إلى الكمبيوتر، كي تتمكّن من إجراء التحديثات اللازمة إذا طلب منك نظام الكمبيوتر ذلك. بالإضافة إلى ذلك، تمكّنك ميزة «النسخ واللصق» في برنامج «كي باس» من حماية كلمات السرّ الخاصة بك، لا سيّما إذا تعرّض جهازك لخطر هجمات من برامج رصد لوحة المفاتيح، أو أنواع أخرى من البرمجيات الخبيثة.

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.**