حماية البيانات :تأمين النظام الخاص بك الرقمية والأجهزة الخاصة بك

الفصل3

التهديدات التي يتعرض لها الأصول الرقمية الخاصة بك

- سرقة الهوية والمتسللين
- فيروسات الكمبيوتر
- مضايقات على الانترنت والهندسة الاجتماعية

الأهداف

9.1 وصف كيفية تلتزم سرقة الهوية وأنواع اللصوص الحيل هوية ارتكاب.

9.2 قائمة وتصف أنواع مختلفة من المتسللين.

9.3 وصف أدوات مختلفة تستخدم المتسللين وأنواع الهجمات التي قد تشن ضد أجهزة الكمبيوتر.

9.4 اشرح ما هو فيروس الكمبيوتر، والسبب في أنهم يشكلون تهديدا للأمن الخاص بك، كيف يمسك جهاز الحوسبة فيروس، والأعراض قد عرض.

9.5 إدراج فئات مختلفة من فيروسات الكمبيوتر، ووصف تصرفاتهم.

9.6 اشرح ما هي البرامج الضارة، وقائمة الأنواع الشائعة من البرامج الضارة.

9.7 تعريف البريد المزعج، ووصف استراتيجيات لمكافحته.

9.8 اشرح ما هي الكوكيز وما إذا كانت تشكل تهديدا أمنيا.

9.9 وصف تقنيات الهندسة الاجتماعية، وشرح استراتيجيات لتجنب الوقوع فريسة لهم.

الجريمة الإلكترونية

- **الجريمة الإلكترونية:** ارتكب أي عمل إجرامي في المقام الأول من خلال استخدام جهاز كمبيوتر
- **مجرمو الإنترنت:** هل الأفراد الذين يستخدمون جomputers الشبكة والإنترنت يرتكبون جريمة

الأنواع الشائعة من الجرائم السيبرانية

- FBI-Related Scams

- Identity Theft

- Nonauction/ Non-Delivery of Merchandise

- Advance Fee Fraud

الأنواع الشائعة من الجرائم السيبرانية

1. الحكومة الانتحال احتيال تنطوي على الناس التظاهر لتمثيل المنظمة الرسمية مثلFBI
2. للبضائع التي لم تكن موجودة حيث جمع الأموال الجناة وتختفي unningالمزادات R دون تسليم البضائع
3. "حسن نية"الاحتيال رسوم مقدما تنطوي على إقناع الناس لإرسال الأموال كبادرة لتمكينهم من الحصول على السداد أكبر في عودة
4. وتشمل سرقة الهوية سرقة شخص معلومات شخصية

سرقة الهوية

ما هي الجريمة الإلكترونية الأكثر ضررا ماليا التي يعاني منها الأفراد؟

عندما يسرق السارق المعلومات الشخصية مثل الاسم والعنوان ورقم ccurs **سرقة الهوية** س الضمان الاجتماعي وتاريخ الميلاد ورقم الحساب المصرفي، ومعلومات بطاقة الائتمان، ويمتد حتى الديون في اسمك.

سرقة الهوية

- **ما هي أنواع من الحيل لا هوية اللصوص ارتكاب؟**
  - تزييف الموجودة لديك الائتمان أو الخصم نذل
  - طلب تغيير العنوان أو حساب مصرفي
  - فتح بطاقة ائتمان جديدة في اسمك
  - الحصول على الخدمات الطبية تحت اسمك
  - شراء منزل مع الرهن العقاري تحت اسمك

سرقة الهوية

استخدام أساليب اللصوص الآخرين للحصول على المعلومات الشخصية الأخرى:

- سرقة المعلومات الشخصية من محفظتك أو محفظة
- سرقة البريد أو تبحث عن طريق القمامة لكشف حساب بنكي أو فواتير بطاقات الائتمان
- خداع الناس في الكشف عن معلومات حساسة عبر الهاتف
- أن تسجيل المعلومات ATM تركيب أجهزة القشط على

سرقة الهوية

مع كل التغطية الإخبارية حول سرقة الهوية، والجرائم الإلكترونية الأخرى، والناس لا يجري المزيد من التحذيرات؟

- **M3AAWG:** وقد فتحت نصف مستخدمي البريد الإلكتروني غير المرغوبة، وبعضها تم تصميمها لخداعك الكشف عن معلومات حساسة.
- 46 ٪ منهم يتبعون روابط لإلغاء الاشتراك في رسائل البريد الإلكتروني غير المرغوب فيه(الذي لا يجلب سوى المزيد من رسائل البريد الإلكتروني)
- أو لأنهم مهتما في المنتجات المعروضة.

القرصنة

ما يحدد بالضبط القراصنة؟

- **القراصنة** ويعرف الأكثر شيوعا مثل أي شخص يخرق بصورة غير قانونية في نظام الكمبيوتر إما كمبيوتر فردي أو شبكة
- أنواع من المتسللين
  - (الهاكرز الأخلاقية)قبعة بيضاء
  - قراصنة قبعة سوداء
  - قراصنة الرمادية قبعة

أنواع من المتسللين

- **هل هناك أنواع مختلفة من المتسللين؟**
- مثل لاختبار nonmalicious **قراصنة قبعة بيضاء** اقتحام أنظمة لأسباب الثغرات الأمنية النظام أو لفضح الضعف لم يكشف عنها.
- **قراصنة قبعة سوداء** اقتحام أنظمة لتدمير المعلومات أو لتحقيق مكاسب غير مشروعة.
- **قراصنة الرمادية قبعة** كسر بطريقة غير شرعية في النظم لتماوج خبراتهم أو محاولة لبيع خدماتهم في إصلاح الخروقات الأمنية.

أدوات وأنواع هجوم القرصنة

يمكن للهاكر سرقة بطاقتي الخصم أو رقم الحساب المصرفي؟

- قراصنة كثيرا ما يحاول كسر في أجهزة الكمبيوتر أو المواقع التي تحتوي على معلومات بطاقة الائتمان.
- إذا قمت بإجراء المعاملات المالية عبر الإنترنت، مثل الخدمات المصرفية أو شراء السلع والخدمات التي سيتم كشف البيانات الشخصية لمجرمي الإنترنت.
- ويمكن تخزين المعلومات على القرص الثابت أو على قرص صلب الأعمال التجارية عبر الإنترنت التي يمكن أن تكون قابلة للكشف من قبل القراصنة.

أدوات وأنواع هجوم القرصنة

- ويمكن تخزين البيانات الشخصية على مختلف المواقع على سبيل المثال العديد من المواقع حتى إذا لم يتم تخزين هذه .تتطلب منك تقديم معرف تسجيل الدخول وكلمة مرور للوصول البيانات على جهاز الكمبيوتر الخاص بك قد يكون القراصنة قادرة على التقاط عندما كنت أو مسجل مفتاح (الشم)على الانترنت باستخدام محلل حزمة.

أدوات وأنواع هجوم القرصنة

- **ما هو محلل حزمة؟**
- يسافر البيانات من خلال شبكة الإنترنت في قطع صغيرة تسمى *الحزم*
- *IP* يتم تحديد الحزمة مع *عنوان*
- وبمجرد أن تصل الحزم وجهتهم، وإعادة تجميعها أنهم إلى رسائل متماسكة.
- كل علبة (أو الشمة)هو برنامج نشر من قبل المتسللين التي تبدو في **(الشم)محلل حزمة** لأنها تنتقل على شبكة الإنترنت.
- **كلوغر** هو البرنامج الذي يلتقط كل ضربات المفاتيح تتم على الكمبيوتر

أدوات وأنواع هجوم القرصنة

ماذا تفعل القراصنة بالمعلومات التي شم؟

بطاقة الائتمان الخاصة بك هو أو /مرة واحدة في الهاكر لديه معلومات الخصم هي يمكن استخدامها لشراء المواد بطريقة غير مشروعة أو يمكن بيعه لشخص ما إذا كان القراصنة يمكن جمع ما يكفي من المعلومات التي قد تكون .كيف سيكون قادرة على ارتكاب سرقة الهوية.

يمكنك حماية نفسك من علبة استنشاق عن طريق تثبيت جدار حماية واستخدام تشفير البيانات على الشبكة اللاسلكية.

أحصنة طروادة والجذور الخفية

بجانب سرقة المعلومات ما هي المشاكل الأخرى التي يمكن أن تسبب قراصنة إذا كانت كسر في جهاز الكمبيوتر الخاص بي؟

وغالبا ما تستخدم قراصنة أجهزة الكمبيوتر الفردية لارتكاب هجمات واسعة النطاق. على سبيل المثال، تحتاج قراصنة للسيطرة على العديد من أجهزة الكمبيوتر في نفس الوقت للقيام بذلك أنها غالبا ما تستخدم**حصان طروادة** الخيول. لتثبيت برامج أخرى على الكمبيوتر الضحايا.

أحصنة طروادة والجذور الخفية

- **أحصنة طروادة:** هو البرنامج الذي يبدو أن شيئا مفيدا أو مرغوب فيه، ولكن لا شيء الخبيثة في الخلفية دون علمك
- **ما الضرر الذي يمكن أحصنة طروادة تفعل؟**
  - وغالبا ما تستخدم قراصنة برنامج طروادة لتثبيت برنامج مستتر أو الجذور الخفية التي تتيح لهم الوصول إلى جهاز الكمبيوتر الضحية.
  - **مستتر والجذور الخفية:** برنامج مستتر التي تسمح للقراصنة على الوصول إلى جهاز الكمبيوتر الخاص بك، والسيطرة الكاملة تقريبا من دون علمك.
  - **الاموات الاحياء:** وغالبا ما تستخدم الجذور الخفية هي جهاز كمبيوتر تسيطر القراصنة ويشار إلى غيبوبة *الحرمان من الخدمة* الهجمات على أجهزة الكمبيوتر الأخرى.

هجمات الحرمان من الخدمة

- **ما هي الحرمان من الخدمة الهجمات؟**
- ونفى المستخدمين الشرعيين الوصول إلى النظام بسبب القراصنة يجعل مرارا طلبات من هذا النظام من خلال جهاز كمبيوتر اتخذت القراصنة منصب غيبوبة.
- يمكن التعامل مع جهاز كمبيوتر فقط عدد معين من طلبات الحصول على المعلومات في وقت واحد.
- عندما غمرت مع طلبات، وإيقاف ويرفض الإجابة عن أي طلبات للحصول على معلومات، حتى لو كانت الطلبات من مستخدم المشروعة.

هجمات الحرمان من الخدمة

- **لا يمكن ل دوس أن تعزى هجوم مرة أخرى إلى الكمبيوتر الذي أطلق عليه؟**
- نعم، فمن السهل.
- **الهجوم**والقوارب دوس هجمات من غيبوبة أكثر من **(دوس)وزعت الحرمان من الخدمة** واحد في نفس الوقت.

هجمات الحرمان من الخدمة

- قراصنة يخلق العديد من الكسالى وتنسيقها بحيث تبدأ بإرسال طلبات وهمية إلى نفس جهاز الكمبيوتر في نفس الوقت.
- الإدارية للكمبيوتر الضحية غالبا ما يكون على قدر كبير من الصعوبة وقف الهجوم لأنها تأتي من العديد من أجهزة الكمبيوتر.
- غالبا ما يتم تنسيق الهجمات تلقائيا **إقناعا**
- **الروبوتات** هي مجموعة كبيرة من البرامج التي تعمل بشكل مستقل على جهاز الكمبيوتر غيبوبة.
- من غيبوبة DOS لأنه من السهل لتعقب عليه من قراصنة الكمبيوتر واحدة تطلق هجوم أكثر من واحد في وقت.

هجمات الحرمان من الخدمة

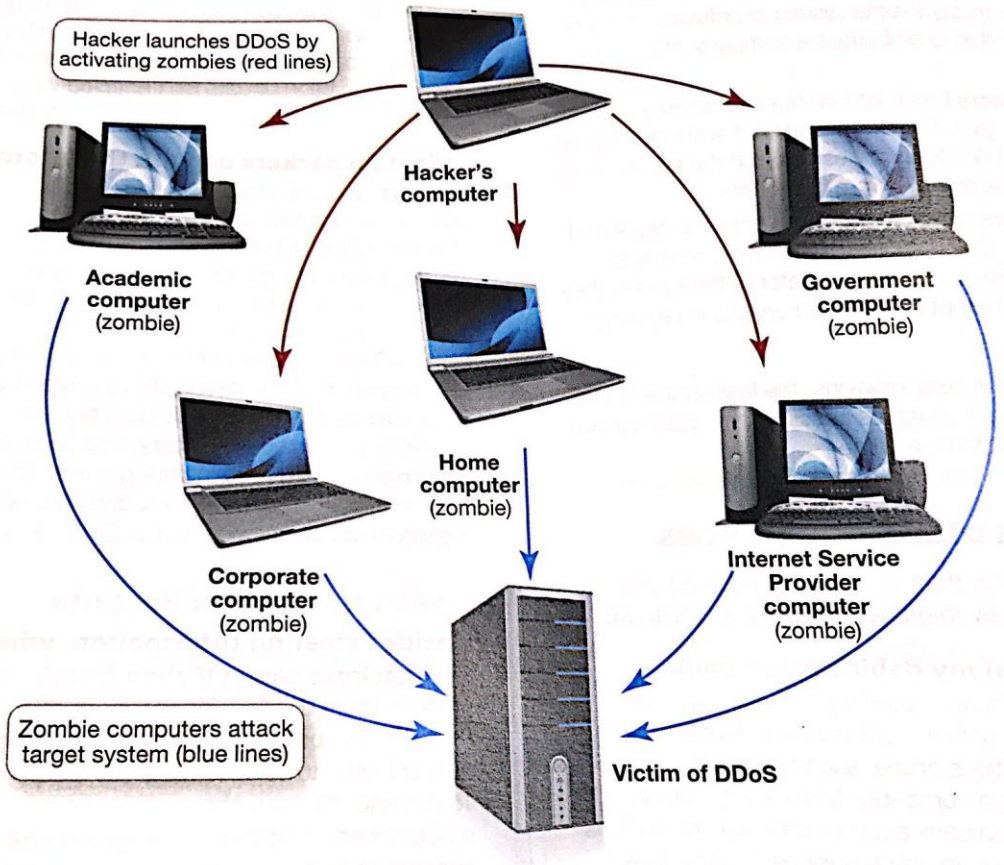


FIGURE 9.4 Zombie computers are used to facilitate a DDoS attack. *(Vovan/Shutterstock, Nicholas Monu/E+/Getty)*

كيف يمكن للقراصنة على الوصول الكمبيوتر

- **بالضبط كيف تكتسب قراصنة الوصول إلى جهاز كمبيوتر؟**

الوصول المباشر: إشراك الجلوس امام جهاز الكمبيوتر وتركيب قرصنة البرمجيات.

وصول غير مباشر: استغلال مجموعات والاتصال بشبكة الانترنت

تستخدم العديد من المتسللين المهنية مجموعات استغلال.

استغلال عدة

- البرامج التي تعمل على خوادم والبحث عن تعرض أجهزة الكمبيوتر التي زيارة خادم.
- استغلال مجموعات للبحث عن الثغرات الأمنية في المتصفحات ونظام التشغيل التي لم يتم تصحيحها من قبل المستخدم.
- ويمكن أن تقدم برامج التجسس، والسير، برنامج مستتر، أو غيرها من البرامج الضارة إلى جهاز الكمبيوتر الخاص بك.
- معظم مجموعات استغلال الاستفادة من نقاط الضعف المعروفة، حتى إذا كان برنامج مكافحة الفيروسات ونظام التشغيل هو حتى الآن، يجب أن تكون آمنة.

اتصال إنترنت

- قراصنة أيضا يمكن الوصول إلى جهاز الكمبيوتر بشكل غير مباشر من خلال اتصاله بالإنترنت.
- لا يمكنك الوصول إلى الإنترنت، ولكن .الاتصال عبر الانترنت هو طريق ذو اتجاهين الناس يمكن الوصول إلى جهاز الكمبيوتر الخاص بك.

ما هي الموانئ منطقية

FIGURE 9.5 Open logical ports are an invitation to hackers.

ما هي الموانئ منطقية

- هي افتراضية بوابات الاتصالات لا المادية أو المسارات التي تسمح لجهاز الكمبيوتر لتنظيم طلبات الحصول على المعلومات، مثل تنزيل صفحات الويب أو البريد توجيه البريد، من الشبكات أو أجهزة الكمبيوتر الأخرى.
- المخصصة لبروتوكول نقل النص 80يتم ترقيم منافذ منطقية وتعيين لخدمة معينة السابقين ميناء المنطقي التشعبي"HTTP"، بروتوكول الاتصال الرئيسي لشبكة الإنترنت.
- جميع طلبات الحصول على المعلومات من المتصفح لتدفق الإنترنت عبر منفذ المنطقي80.
- إلا إذا كنت تأخذ الاحتياطات اللازمة لتقييد الوصول إلى ميناء المنطقي، أشخاص آخرين على شبكة الانترنت قد تكون قادرة على الوصول إلى جهاز الكمبيوتر الخاص بك من خلالهم.
- يمكنك منع المشاكل الأكثر القرصنة عن طريق تثبيت جدار الحماية.

فيروسات الكمبيوتر
أساسيات الفيروسات

ما هو فيروس الكمبيوتر؟

- هو برنامج الكمبيوتر الذي تولى الذاتي لبرنامج كمبيوتر آخر وامتدت إلى الآخر أجهزة الكمبيوتر عندما الملفات الصرف.

لماذا هي فيروسات مثل تهديدا للأمن الخاص بي؟

- الفيروسات هي تهديد لأنهم التهرب من الكشفوالاختباء داخل رمز من برنامج المضيف لتجنب كشفها.
- الهواتف الذكية وأجهزة الكمبيوتر اللوحي، .الفيروسات لا تقتصر على أجهزة الكمبيوتر وأجهزة أخرى يمكن أن يصاب.

المستخدم التفاح

- داعي للقلق حول الفيروسات

أساسيات الفيروسات

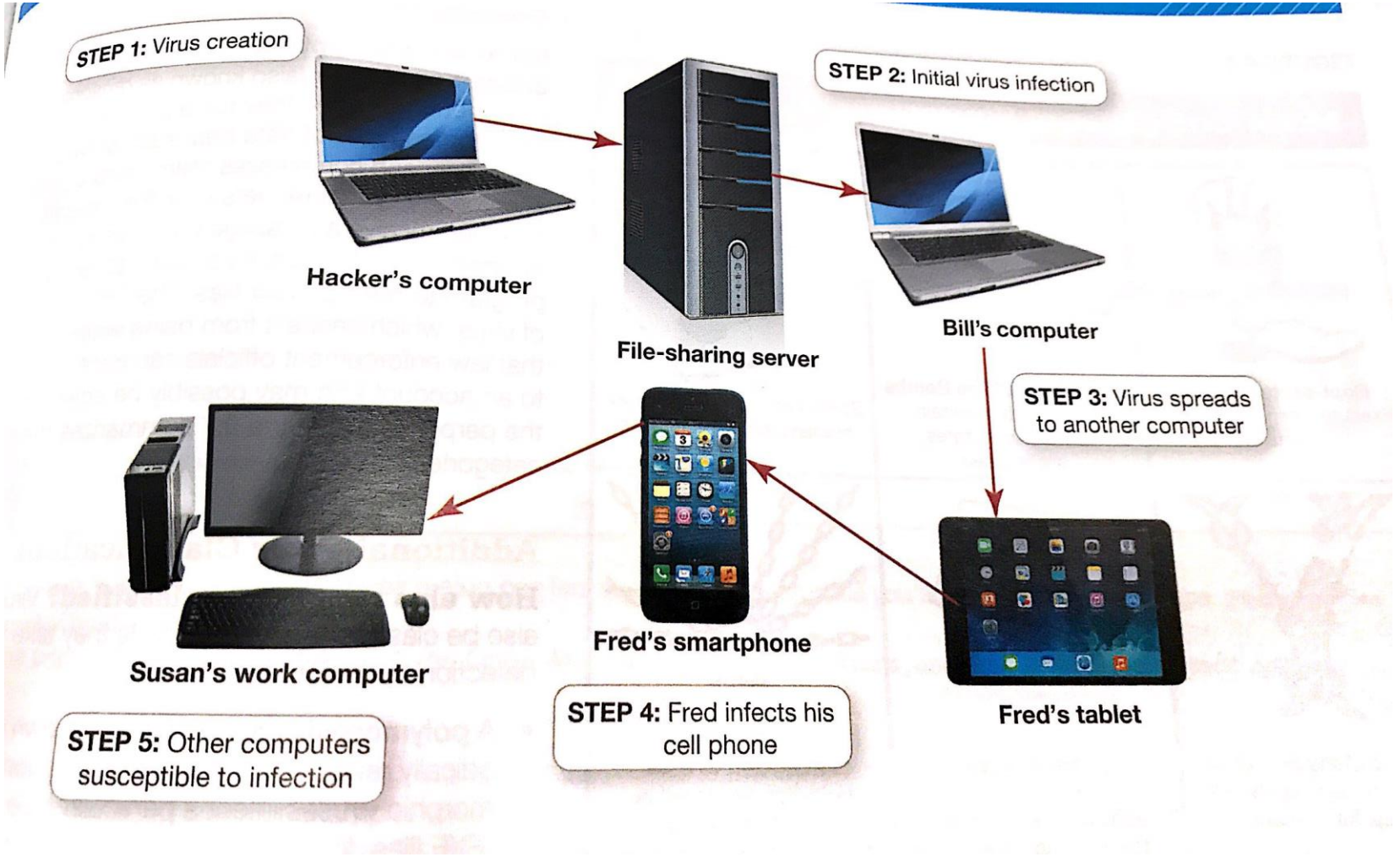
- **ماذا الفيروسات تفعل؟**
- الغرض الرئيسي فيروس هو تكرار نفسه ونسخ رمزها في العديد من الملفات الأخرى المضيفة ممكن.
- تتطلب فيروسات الكمبيوتر التفاعل البشري في الانتشار.
- فيروس غير قادر تصيب جهاز الكمبيوتر الخاص بك حتى يتم فتح الملف المصاب
- معظم الفيروسات لها أهداف ثانوية أو آثار جانبية.
- تحميل وتشغيل ملف هذا المرفق على البريد الإلكتروني هي الطرق الشائعة لإصابة جهاز الكمبيوتر الخاص بك.

أساسيات الفيروسات

كيف يصاب جهاز الكمبيوتر الخاص بي الفيروس؟

- تحميل المصابة ملفات الصوت والفيديو
- محركات أقراص فلاش المشتركة
- البريد الإلكتروني

أساسيات الفيروسات

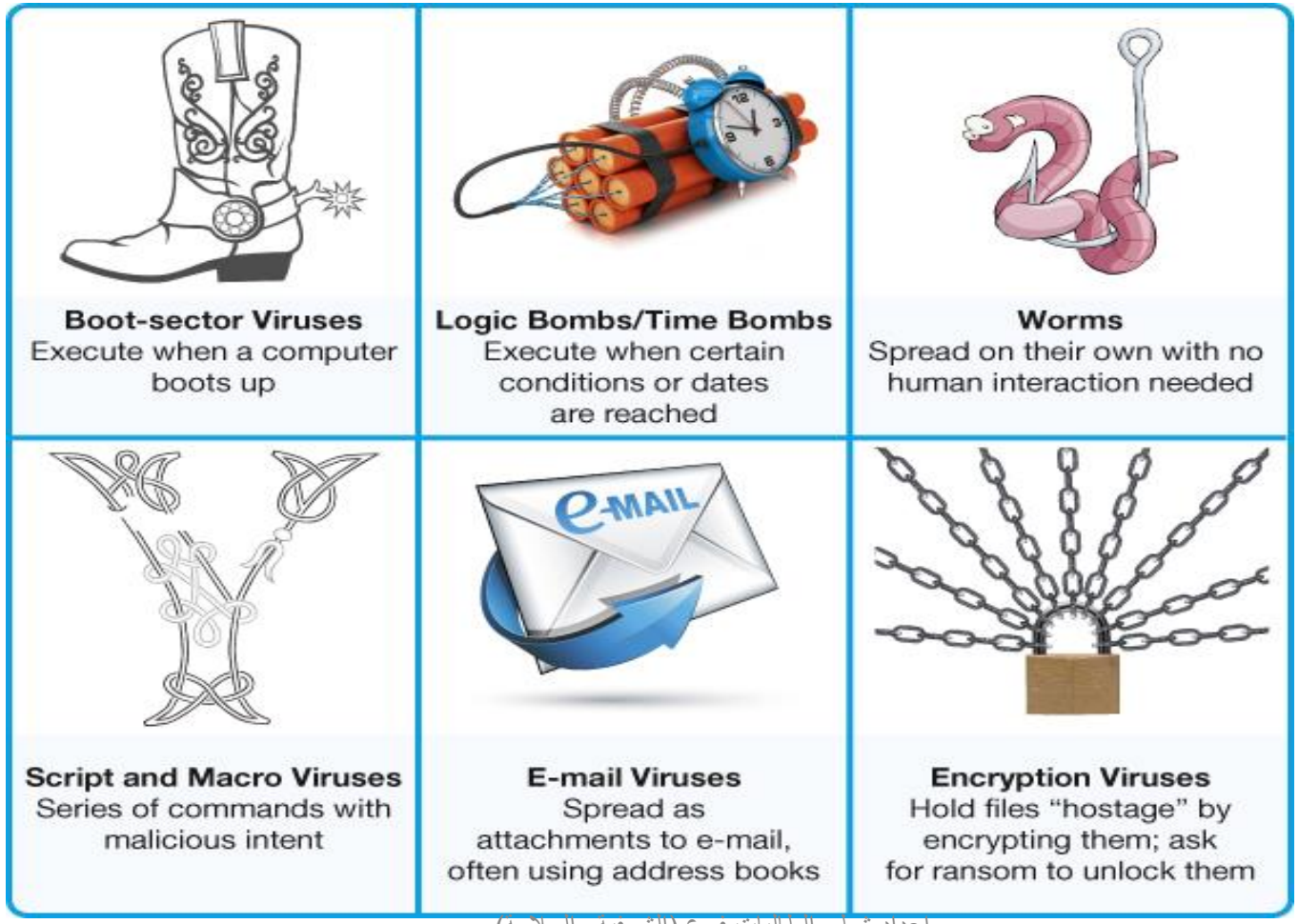


أساسيات الفيروسات

كيف يمكنني معرفة ما إذا كان يتم إصابة الكمبيوتر مع الفيروس؟

1. رموز البرامج الموجودة أو الملفات تختفي فجأة.
2. البدء في المتصفح الخاص بك ويأخذك إلى الصفحة الرئيسية غير عادية.
3. رسائل غريبة البوب يتم عرض صعودا أو الصور على الشاشة أو الموسيقى غريب أو اللعب الصوت.
4. تصبح ملفات البيانات تالفة.
5. توقف البرنامج يعمل بشكل صحيح.
6. إيقاف النظام الخاص بك بشكل غير متوقع.

أنواع الفيروسات



فيروسات قطاع الإقلاع

- تكرار نفسه في سجل التمهيد محرك الأقراص الرئيسي الثابت.
- **سجل التمهيد الرئيسي** هو برنامج التي تنفذ كلما تمهيد جهاز الكمبيوتر، وضمان أن الفيروس سيتم تحميل في الذاكرة على الفور، حتى قبل يمكن تحميل بعض البرامج الحماية من الفيروسات.
- وغالبا ما تنتقل فيروسات قطاع التمهيد من محرك أقراص فلاش متصلة بمنفذ USB.
- يحاول الكمبيوتر لتناول الغداء سجل التمهيد الرئيسي من محرك أقراص فلاش التي عادة ما تكون على الزناد للكشف عن الفيروس ليصيب القرص الصلب.

المنطق وقنبلة موقوتة

- **قنبلة المنطق** فيروس الكمبيوتر الذي يعمل عند تحقق مجموعة معينة من الظروف، مثل عندما يطلق البرنامج على عدد معين من المرات.
- **قنبلة موقوتة** فيروس هذا ما سببها مرور الوقت أو في تاريخ معين..

ديدان

- **ديدان** برنامج مستقل أن يضاعف نفسه عن طريق نسخ جزء من نفسه على كمبيوتر آخر

الديدان مقابل الفيروسات

فيروس	الفيروس المتنقل
تتطلب التفاعل البشري لنشر	الاستفادة من وسائل النقل ملف لنشر من تلقاء نفسها
تصيب ملف المضيف وينتظر حتى يتم تنفيذ هذا الملف لتكرار وتصيب نظام الكمبيوتر	العمل بشكل مستقل نشر نفسها ويمكن أن تولد الكثير من حركة المرور عند محاولة نشر

السيناريو وفيروسات الماكرو

النصي: قائمة من الأوامر التي يمكن تنفيذها على جهاز الكمبيوتر دون تدخل المستخدم أو المعرفة.

وغالبا ما تستخدم النصي لأداء وظيفة مشروعة مفيدة عن مواقع مثل جمع المعلومات من العملاء. ولكن بعض النصي والخبيثة.

فيروس ماكرو: هو الفيروس الذي تعلق نفسها على مستند يستخدم وحدات الماكرو.

دقيق: هو عبارة عن سلسلة قصيرة من الأوامر التي عادة بأتمتة المهام المتكررة.

فيروسات البريد الإلكتروني E

استخدام دفتر العناوين في نظام البريد ضحايا الإلكترونية ل **فيروسات البريد الإلكتروني E** توزيع الفيروس.

فيروسات التشفير

- انهم تشغيل برنامج الذي يبحث عن نوع شائع من الملفات، مثل **(الفدية)فيروسات التشفير** ملفات مايكروسوفت وورد، وضغط عليها باستخدام مفتاح التشفير المعقد الذي يجعل ملفاتك غير صالحة للاستعمال. ثم تظهر رسالة تطلب منك أن ترسل الدفعة إلى حساب إذا كنت ترغب في الحصول على برنامج فك تشفير الملفات الخاصة بك. العيب مع هذا النوع من الفيروس الذي يحفظه من كونها على نطاق واسع، هو أن المسؤولين عن إنفاذ القانون يمكن تتبع المدفوعات وقبض على الجناة.

تصنيف الفيروسات إضافية

الفيروسات يمكن تصنيفها بطرق خاصتك اتخاذها لتجنب الكشف عن طريق برامج مكافحة الفيروسات

- معظم **الفيروسات متعددة الأشكال** تغيير التعليمات البرمجية الخاصة به لتجنب الكشف. الفيروسات متعددة الأشكال تصيب نوع معين من الملفات.
- **الفيروسات متعدد الأجزاء** تم تصميم لتصيب أنواع الملفات متعددة في محاولة لخداع برامج مكافحة الفيروسات التي تبحث عن ذلك.
- **الفيروسات الشبح** محو مؤقتا مدوناتها من الملفات التي يقيمون فيها والاختباء في الذاكرة النشطة للكمبيوتر. هذا يساعد على تجنب كشف ما إذا كان يتم البحث فقط في القرص الصلب. برامج مكافحة الفيروسات الحالية الذاكرة بالاشعة وكذلك القرص الصلب. بحثا عن الفيروسات.

ادواري وبرامج التجسس :البرمجيات الخبيثة

- **البرمجيات الخبيثة:** هو البرامج الضارة التي تم إنشاؤها باستخدام القصد.
- **هناك ثلاثة أشكال أولية من البرامج الضارة:** ادواري، برامج التجسس، والفيروسات.

ادواري وبرامج التجسس :البرمجيات الخبيثة

ما هو ادواري؟

- **ادواري:** البرامج التي تعرض إعلانات ترعاها في قسم من نافذة المتصفح أو مربع منبثق كما.
- النظر في شرعية.
- وسائل توليد الدخل لأولئك المطورين الذين لا تهمة للبرمجيات أو المعلومات.

ادواري وبرامج التجسس :البرمجيات الخبيثة

ما هي برامج التجسس؟

- **برامج التجسس:** هو برنامج على الظهر الذي يقوم بتحميل عادة مع البرامج الأخرى غير المرغوب فيها تثبيت من الإنترنت ويعمل في خلفية النظام الخاص بك، من دون علمك.
- برامج التجسس ونقل المعلومات عنك مثل عادات تصفح الانترنت الخاص بك، وإلى صاحب البرنامج بحيث يمكن استخدام هذه المعلومات لأغراض تسويقية.
- تستخدم العديد من برامج التجسس وتتبع الكوكيز لجمع المعلومات .

ادواري وبرامج التجسس :البرمجيات الخبيثة

- **بسكويت:** ملفات نصية صغيرة يتم تخزينها على جهاز الكمبيوتر الخاص بك.
- **المفتاح المسجل:** مراقبين ضربات المفاتيح بقصد سرقة كلمات السر تسجيل الدخول معرفات أو معلومات بطاقة الائتمان.

ادواري وبرامج التجسس :البرمجيات الخبيثة

- **يمكنني منع برامج التجسس من التجسس على لي؟**
- يمكننا منع برامج التجسس عن طريق تثبيت برامج مكافحة التجسس.

بريد مؤذي

- **بريد مؤذي:** هو البريد الإلكتروني غير المرغوب فيه أو غير المرغوب فيه.
- **كيف يمكنني الأفضل تجنب البريد المزعج؟**
- الشركات التي ترسل الرسائل غير المرغوب فيها العثور على عنوان البريد الإلكتروني الخاص بك إما من قائمة التي يشترونها أو مع البرامج التي تبدو لعناوين البريد الإلكتروني على شبكة الانترنت.
- الرسائل الفورية غير المرغوب فيها هي أيضا شكل من أشكال البريد المزعج يسمى ***SPIM***.
- إذا كنت قد استخدمت عنوان البريد الإلكتروني الخاص بك لشراء أي شيء على الانترنت، فتح حساب عبر الإنترنت، أو المشاركة في الشبكات الاجتماعية مثل الفيسبوك عنوان البريد الإلكتروني الخاص بك وسوف تظهر في نهاية المطاف على واحدة من القوائم التي الاطر الحصول عليها.

بريد مؤذي

هناك عدة طرق للمساعدة على تجنب البريد المزعج:

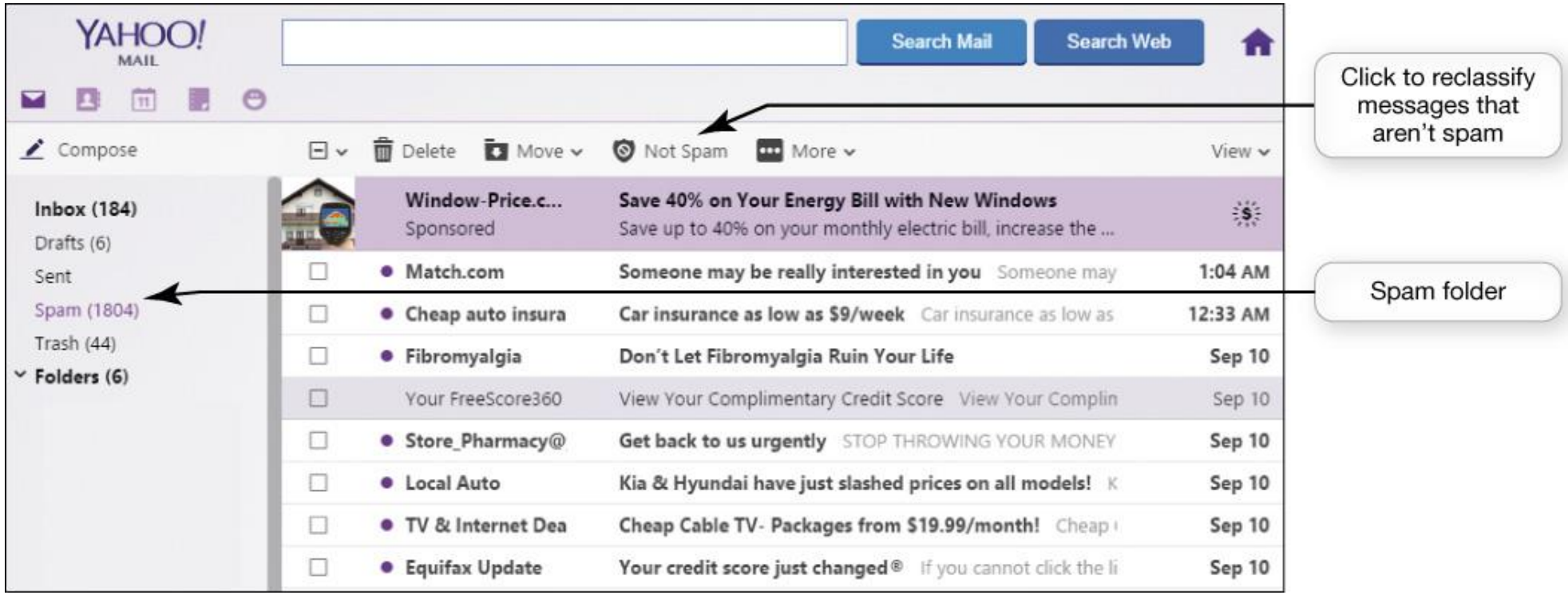
- إنشاء عنوان بريد إلكتروني مجاني.
- هو خيار يمكنك تحديد في حساب بريدك الإلكتروني أن أماكن)مرشحات البريد المزعج البريد غير "أو "البريد المزعج"معروفة أو يشتبه البريد المزعج في مجلد خاص يسمى "المرغوب فيه").
- شراء برامج من طرف ثالث.
- تصنيف رسائل البريد الإلكتروني التي تم أخطأ في التعرف بأنها غير مرغوب فيها.

بريد مؤذي

كيف مرشحات البريد المزعج العمل؟

- ٪ من البريد المزعج 95يمكن مرشحات البريد المزعج وبرامج تصفية التقاط ما يصل إلى عن طريق التحقق من عناوين البريد الإلكتروني الواردة ضد قاعدة بيانات من البريد المزعج معروفة.
- مرشحات البريد المزعج أيضا فحص البريد الإلكتروني الخاص بك لأنماط البريد المزعج أكثر من "21" و "مجانا"وكثيرا ما تستخدم كلمات مثل".
- فلتر البريد المزعج ليست مثالية، ويجب عليك مراجعة مجلد الرسائل غير المرغوب فيها قبل حذف محتوياته بسبب البريد الإلكتروني الشرعي قد ينتهي هناك عن طريق الخطأ.

بريد مؤذي


YAHOO! MAIL
Search Mail
Search Web
Compose
Delete
Move
Not Spam
More
View
Inbox (184)
Drafts (6)
Sent
Spam (1804)
Trash (44)
Folders (6)
Window-Price.c...
Sponsored
Save 40% on Your Energy Bill with New Windows
Save up to 40% on your monthly electric bill, increase the ...
Match.com
Someone may be really interested in you Someone may
1:04 AM
Cheap auto insura
Car insurance as low as $9/week Car insurance as low as
12:33 AM
Fibromyalgia
Don't Let Fibromyalgia Ruin Your Life
Sep 10
Your FreeScore360
View Your Complimentary Credit Score View Your Complin
Sep 10
Store_Pharmacy@
Get back to us urgently STOP THROWING YOUR MONEY
Sep 10
Local Auto
Kia & Hyundai have just slashed prices on all models! K
Sep 10
TV & Internet Dea
Cheap Cable TV- Packages from $19.99/month! Cheap
Sep 10
Equifax Update
Your credit score just changed® If you cannot click the li
Sep 10
Click to reclassify messages that aren't spam
Spam folder

بريد مؤذي

كيف يمكنني منع البريد المزعج

1. قبل التسجيل في موقع على شبكة الانترنت قراءة سياسة الخصوصية الخاصة بها لمعرفة الكيفية التي يستخدم البريد الإلكتروني الخاص بك.
2. عدم الرد على البريد المزعج.
3. هذه الخدمات versaforward.com الاشتراك في البريد الإلكتروني خدمة الشحن مثل الشاشة رسائل البريد الإلكتروني الخاصة بك الشحن فقط تلك الرسائل التي تعين على أنها بخير لقبوله.

بسكويت

ما هي الكوكيز؟

الكوكيز عبارة عن ملفات نصية صغيرة أن بعض المواقع تخزن تلقائيا على القرص الصلب الخاص بك عند زيارتهم.

كيفية عمل الكوكيز الإنترنت؟

- عند تسجيل الدخول إلى موقع على شبكة الانترنت يستخدم ملفات تعريف الارتباط ملف تعريف الارتباط بتعيين رقم معرف لجهاز الكمبيوتر الخاص بك.
- ويهدف معرف فريد لجعل زيارتك العودة إلى موقع على شبكة الانترنت أكثر كفاءة.
- في كل مرة تقوم بتسجيل الدخول إلى الموقع، الموقع يمثل زيارتك وبتتبع ذلك في قاعدة البيانات الخاصة به.

بسكويت

ماذا تفعل المواقع بمعلومات الكوكيز؟

- ويمكن أن توفر المواقع مع معلومات عن عادات التصفح الخاص بك، مثل الإعلانات التي قد فتحت، والمنتجات كنت قد نظرت، والوقت ومدة زياراتك.
- الشركات تستخدم هذه المعلومات لتحديد تدفق حركة المرور من خلال موقعه على الانترنت وفعالية استراتيجية التسويق الخاصة بهم.

بسكويت

يمكن الحصول على شركة معلوماتي الشخصية عندما أزور مواقعهم؟

المعلومات الشخصية .الكوكيز لا تذهب من خلال القرص الصلب بحثا عن معلومات شخصية
.الوحيدة الكعكة الحصول على هي المعلومات التي تقدمها عند ملء الاستمارات على الانترنت

بسكويت

هل توجد مخاطر الخصوصية مع الكوكيز؟

- يمكن لمواقع الويب تستخدم الكوكيز لجمع وبيع المعلومات الشخصية لأطراف ثالثة.
- يمكن أن المواقع على شبكة الإنترنت تتبع سلوك التصفح وادراك التعادل لتعريف المستخدم الخاص بك.

بسكويت

يجب أن حذف ملفات تعريف الارتباط من القرص الصلب؟

- الكوكيز لا تشكل أي تهديد أمني لأنه يكاد يكون من المستحيل إخفاء فيروس أو برنامج من البرامج الضارة في ملف تعريف الارتباط.
- على القرص الصلب الخاص بك، ونقدم لكم الراحة صغيرة على littlieلأنها تحتل غرفة زيارات العودة إلى المواقع على شبكة الإنترنت، ليس هناك سبب وجيه لحذفها حذف الملفات الكوكيز الخاصة بك في الواقع يمكن أن تسبب لك الإزعاج من إعادة دخول البيانات التي قمت بإدخالها بالفعل في موقع الكتروني.

بسكويت

الكوكيز نظرة عامة:

- مساعدة الشركات على تحديد فعالية التسويق.
- لا محرك بحث عن المعلومات الشخصية.
- قد تغزو خصوصيتك.
- لا تشكل أي تهديد أمني.

هندسة اجتماعية

ما هي الهندسة الاجتماعية؟

- أي أسلوب يستخدم المهارات الاجتماعية لتوليد التفاعل البشري الذي الحيل الأفراد للكشف عن معلومات حساسة.
- الهندسة الاجتماعية في كثير من الأحيان لا تنطوي على استخدام الكمبيوتر أو وجها لوجه التفاعل.

اجتماعي هندسة

ماذا جرعة اجتماعي هندسة عمل؟

- معظم الهندسة الاجتماعية تستخدم ذريعة لاستدراج ضحاياهم.
- **بالتستر:** فعل خلق سيناريو اخترع لإقناع شخص ما لإفشاء المعلومات.

الخداع وتزوير العناوين

كيف يتم التصيد مخططات أجريت؟

- **التصيد:** عملية إرسال رسائل البريد الإلكتروني لجذب مستخدمي الإنترنت في الكشف عن المعلومات الشخصية مثل بطاقة الائتمان أو أرقام الضمان الاجتماعي أو غيرها من المعلومات الحساسة التي يمكن أن تؤدي إلى سرقة الهوية.
- التصيد هو هجوم عبر الانترنت يستخدم البريد الإلكتروني متنكرا في زي سلاح.
- والهدف من ذلك هو لخداع المتلقي البريد الإلكتروني إلى الاعتقاد بأن الرسالة هي شيء يريدونه أو في حاجة إلى طلب من حساباتهم المصرفية، على سبيل المثال، أو مذكرة من شخص ما في شركاتهم وفوق ارتباط أو تحميل مرفق.

الخداع وتزوير العناوين

وتزوير العناوين نوع من التصيد احتيال؟

- **تزوير العناوين:** زرع الشيفرات الخبيثة على جهاز كمبيوتر يعمل يغير قدرة المتصفح للبحث عن عناوين الويب ويوجه المستخدمين إلى مواقع زائفة.
- تزييف أكثر غدرا من الخداع.

الخداع وتزوير العناوين

كيف يمكنني تجنب الوقوع بواسطة الخداع وتزوير العناوين الحيل؟

- أبدا الرد مباشرة على أي بريد إلكتروني يطلب منك معلومات شخصية.
- تحقق مع شركة يطلبون المعلومات وتعطي إلا إذا كان لديك معلومات مؤكدة الحاجة إليه.
- لا تنقر على وصلة في البريد الإلكتروني للذهاب إلى موقع على شبكة الانترنت.
- أبدا إعطاء المعلومات الشخصية عبر الإنترنت إلا إذا كنت تعرف أن الموقع آمن.
- استخدام عامل تصفية الخداع.

برامج الرعب

ما هي برامج الرعب؟

وهناك نوع من البرمجيات الخبيثة التي يتم تحميلها على جهاز الكمبيوتر الخاص بك ويحاول اقناع لكم أن جهازك مصاب بفيروس أو أي نوع آخر من البرامج الضارة.

برامج الرعب

كيف أحمي نفسي ضد برامج الرعب؟

- تثبيت برامج مكافحة الفيروسات وبرمجيات مكافحة البرمجيات الخبيثة.
- قد تكون مصابة جهاز الكمبيوتر "أبدا انقر على شعار الموقع أو مربعات منبثقة التي تقول الخاص بك، انقر هنا لمسح الملفات".

حماية الملكية الرقمية الخاصة بك

- تقييد الوصول إلى الأصول الرقمية الخاصة بك
- حفظ البيانات الخاصة بك آمنة
- حماية لديك الحاسبات البدنية الأصول

تقييد الوصول إلى الأصول الرقمية الخاصة بك

- **حفظ الفيروسات وقراصنة الكمبيوتر بعيدا عن جهاز الكمبيوتر الخاص بك عن طريق:**
  - (عادة من خلال الاتصال بالإنترنت)منعهم من الوصول إلى جهاز الكمبيوتر الخاص بك
  - باستخدام تقنيات لمنع العدوى بالفيروس من الوصول إلى حساب الخاص بك.
  - حماية المعلومات الرقمية الخاصة بك في مثل هذه الطريقة التي لا يمكن الوصول إليها (مثل كلمات السر)
  - إخفاء الأنشطة الخاصة بك من أعين المتطفلين

الجدران النارية

ما هو جدار الحماية؟

- هو برنامج حاسوبي أو جهاز مصمم لحماية الكمبيوتر من المتسللين
- هو جدار الحماية المصممة خصيصا لشبكة منزلية **:جدار الحماية الشخصية**
  - إلى الغزاة وربما (مسارات الاتصالات)باستخدام أنه يمكنك إغلاق الموانئ منطقية المفتوحة جعل جهاز الكمبيوتر الخاص بك غير مرئية إلى أجهزة الكمبيوتر الأخرى.

الجدران النارية

الذي هو أفضل برنامج جدار حماية أو جدار حماية الأجهزة؟

- نوع واحد هو ليس أفضل من الآخر.
- يجب عليك أن تنظر تركيب على حد سواء لأقصى قدر من الحماية كما ارتداء طبقات متعددة من الملابس في فصل الشتاء لإبقاء لكم أكثر دفئا من طبقة واحدة.

أنواع من الجدران النارية

ما برامج جدران الحماية هناك؟

- Windows وOS X جدار الحماية التي يمكن الاعتماد عليها، ويأتي مع نظام التشغيل كما (جدار حماية ويندوز).
- وتشمل الأجنحة الأمن برنامج جدار الحماية مثل مكافي لأمن الإنترنت، الأمن نورتون وجناح الأمن ترنت مايكرو الإنترنت.
  - مثل نظام الرصد التي)الجدران النارية المدرجة في الأجنحة الأمنية غالبا ما تأتي مع ميزات إضافية ينبهك إذا كان جهاز الكمبيوتر الخاص بك هو تحت الهجوم)
- لا يمكنك تشغيل اثنين من جدار الحماية في الوقت نفسه لأنها يمكن أن تتعارض مع بعضها البعض، وتسبب الكمبيوتر إلى إبطاء أو تجميد ما يصل
  - وهذا ما حدث عندما كنت تستخدم جناح الأمن يتضمن جدار الحماية، يجب جناح تعطيل جدار الحماية التي تأتي مع نظام التشغيل الخاص بك.

أنواع من الجدران النارية

ما هي الجدران النارية الأجهزة؟

- وتشمل العديد من الموجهات يباع الشبكة المنزلية جدار الحماية
- الإعداد لجدران الحماية الأجهزة ليست سوى مثل برامج جدران الحماية الذي صمم للمبتدئين والتكوين الافتراضي في معظم الموجه حفاظ على الموانئ منطقية غير المستخدمة مغلقة.
- يمكن ثائق التوجيه المرافق مساعدة المستخدمين الأكثر خبرة في ضبط الإعدادات للسماح بالوصول إلى منافذ معينة إذا لزم الأمر.

كيف الجدران النارية العمل

الجدران النارية المصممة لتقييد الوصول إلى الشبكة وحواسيبها.

كيف الجدران النارية حمايتك من المتسللين؟

- من خلال منع الوصول إلى الموانئ منطقية
- عن طريق الحفاظ على عنوان شبكة أمان الكمبيوتر

كيف الجدران النارية العمل

كيف منع الوصول إلى الموانئ جدار الحماية المنطقية؟

- **لمنع الوصول إلى الموانئ منطقية** جدار الحماية فحص حزم البيانات التي يرسل جهاز الكمبيوتر الخاص بك ويستقبل.

  حزم البيانات تحتوي على معلومات مثل عنوان من أجهزة الكمبيوتر إرسال واستقبال وميناء المنطقي الذي سيتم استخدام الحزمة.
- **تصفية الحزم** الجدران النارية بتصفية الحزم المرسلة إلى الموانئ منطقية محددة
- **حجب ميناء منطقي** الجدران النارية تجاهل الطلبات التي تأتي من الإنترنت طلب الوصول إلى منافذ معينة.

  الموانئ منطقية: هي بوابات الاتصالات الافتراضية أو المسارات التي تسمح الكمبيوتر لتنظيم طلبات من الشبكات أو أجهزة الكمبيوتر الأخرى

كيف الجدران النارية العمل

كيف الجدران النارية الحفاظ على عنوان الشبكة الخاصة بك آمنة؟

- كل جهاز كمبيوتر عنوان فريد يسمى **IP (عنوان بروتوكول الإنترنت)**.
- الخاص بك لشبكة منزلك إلى جهاز التوجيه الخاص بك عن طريق IP يتم تعيين عنوان **مزود خدمة الانترنت** الخاص **(ISP).**
- لكن كل جهاز على الشبكة المنزلية الخاصة بك أيضا لديه عنوان IP.
- لتعيين **عناوين (NAT):** الجدران النارية تستخدم عملية تسمى **ترجمة عنوان الشبكة** والتي يمكن أن تستخدم فقط على) **الداخلية الخاصة بك** على الشبكة **IP العام** إلى **IP** (شبكة الاتصال الداخلية، لذلك لا يمكن الكشف عنها من قبل قراصنة).

مع العلم الكمبيوتر الخاص بك هو آمن

- **كيف يمكنني معرفة ما إذا كان جدار حماية بلدي حماية جهاز الكمبيوتر الخاص بي؟**
- زيارة المواقع التي تقدم خدمات مجانية والتي تختبر ضعف جهاز الكمبيوتر الخاص بك.
  - زيارة مؤسسة البحوث جيبسون(grc.com)
    - نظام ليست عرضة للهجمات **:تقرير واضح**
    - اكتشاف الثغرات المحتملة **:لا تقرير نظيفة**
- **ما إذا كنت لا تحصل على تقرير نظيف من برنامج الاختبار؟**
- تثبيت جدار الحماية في أقرب وقت ممكن :لم يكن لديك جدار الحماية
- راجع وثائق :هل لديك جدار الحماية ولكن يتم تحديد المنافذ المشتركة بأنها عرضة جدار الحماية الخاص بك للحصول على تعليمات حول كيفية إغلاق أو تقييد الوصول إلى هذه المنافذ

مع العلم الكمبيوتر الخاص بك هو آمن

- موانئ المنطقية المشتركة

FIGURE 9.18

Common Logical Ports

PORT NUMBER	PROTOCOL USING THE PORT
21	FTP (File Transfer Protocol) control
23	Telnet (unencrypted text communications)
25	SMTP (Simple Mail Transfer Protocol)
53	DNS (domain name system)
80	HTTP (Hypertext Transfer Protocol)
443	HTTPS (HTTP with Transport Layer Security [TLS] encryption)

منع فيروس العدوى
برامج مكافحة الفيروسات

ما هو أفضل وسيلة لحماية بلدي الفيروسات شكل الأجهزة؟

1. تثبيت مكافحة الفيروسات.
2. الحفاظ على هذا البرنامج حتى الآن.

ما هو أفضل وسيلة لحماية الأجهزة من الفيروسات؟

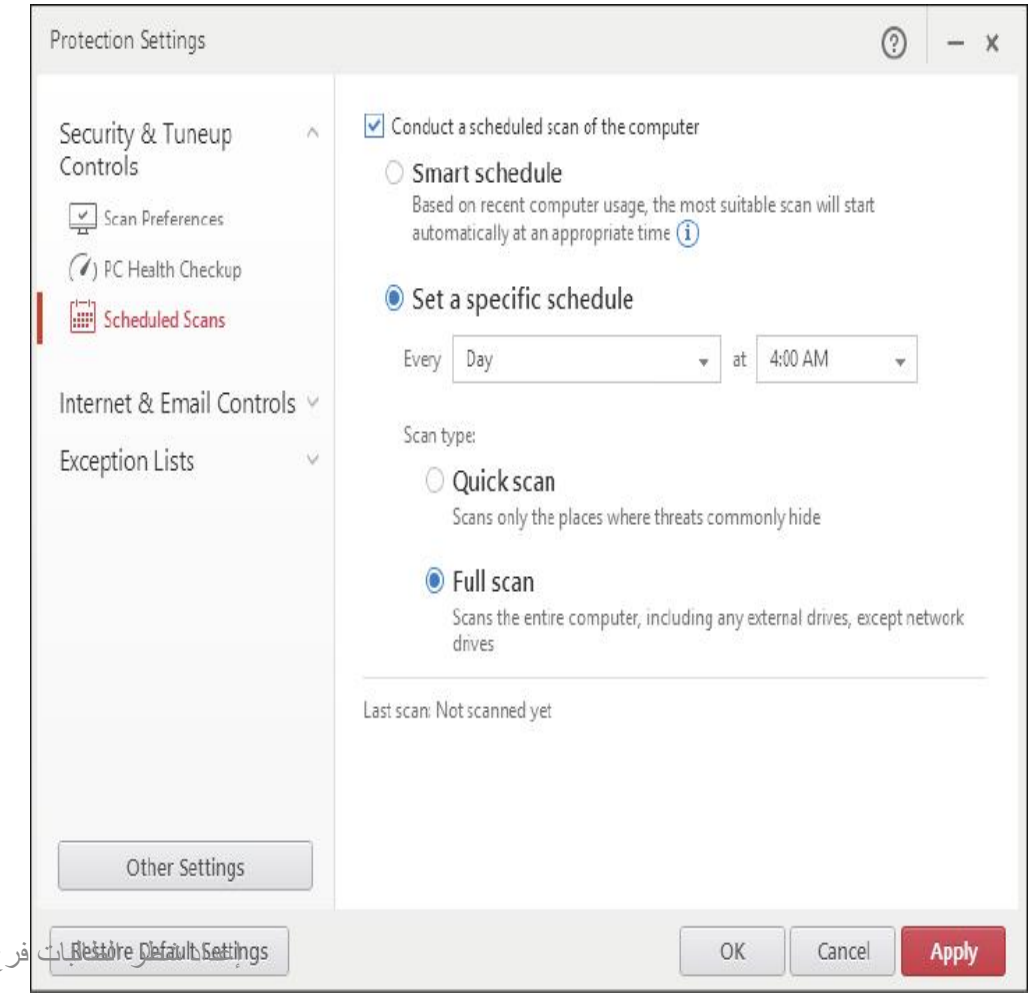
- **برامج مكافحة الفيروسات:** بالكشف عن الفيروسات ويحمي جهاز الكمبيوتر والملفات الخاصة بك من الأذى.
- ، ومكافي هي من بين الشركات التي تقدم درجات عالية AVGسيمانتيك، كاسبيرسكي، حزم برامج مكافحة الفيروسات.

برامج مكافحة الفيروسات

- **عدد المرات التي أحتاجها لتشغيل برنامج مكافحة الفيروسات؟**
  - يجب عليك تشغيل مسح الفيروسات نشطة على النظام بأكمله مرة واحدة على الأقل في الأسبوع.
  - برامج مكافحة الفيروسات الحالية تعمل بالاشعة في الخلفية عندما لا يتم استخدام وحدة المعالجة المركزية الخاصة بك بشكل كبير.
    - يمكنك تكوين البرنامج لتشغيل المسح في بعض الأحيان عندما لا تستخدم النظام الخاص بك (كنت النوم الخاصة بك ولكن ولكن جهاز الكمبيوتر في وضع التشغيل.
  - إذا كنت تشك في وجود المشكلة، يمكنك اطلاق المسح الضوئي وتشغيله على الفور.

برامج مكافحة الفيروسات

- ترينـد مايكرو لأمن الإنترنت



برامج مكافحة الفيروسات

كيف تعمل برامج مكافحة الفيروسات؟

1. **كشف**
   - برامج مكافحة الفيروسات بالبحث عن تواقيع الفيروسات في ملفات
   - هو جزء من شفرة الفيروس هذا فريدة من نوعها لفيروس كمبيوتر :فيروس التوقيع معين

برامج مكافحة الفيروسات

2. وقف تنفيذ فيروس

- إذا كان يكتشف برامج مكافحة الفيروسات توقيع الفيروسات أو أي نشاط مشبوه، فإنه يتوقف تنفيذ الملفات والفيروسات ويعلمك أنه قد الكشف عن فيروس.
- إجراء من شأنه أن يضع الفيروس في منطقة آمنة على القرص الصلب :كما تفعل الحجر الصحي الخاص بك بحيث أنها لن تنتشر إلى ملفات أخرى
- تعطيك خيار حذف أو إصلاح الملف المصاب
  - للأسف، وبرامج مكافحة الفيروسات لا يمكن دائما إصلاح الملفات المصابة لجعلها صالحة للاستعمال مرة أخرى.
  - الاحتفاظ بنسخ احتياطية من الملفات الهامة.

برامج مكافحة الفيروسات

3. منع العدوى في المستقبل

- سوف البرمجيات معظم الفيروسات أيضا محاولة لمنع العدوى عن طريق **بتلقيح** الملفات الرئيسية على جهاز الكمبيوتر الخاص بك.
- برنامج الحماية من الفيروسات يسجل السمة الرئيسية حول ملفات جهاز الكمبيوتر الخاص بك **:تلقيح** مثل حجم الملف والبيانات التي تم إنشاؤها وتحافظ هذه الإحصاءات في مكان آمن على القرص الصلب الخاص بك
- عند مسح بحثا عن الفيروسات، ومكافحة الفيروسات برنامج يقارن سمات الملفات مع السمات التي سجلت سابقا للمساعدة في الكشف عن محاولات من قبل برامج الفيروسات لتعديل الملفات.

برامج مكافحة الفيروسات

هل برامج مكافحة الفيروسات دائما وقف الفيروسات؟

- المصيد الفيروسات المعروفة على نحو فعال
- فيروسات في كل وقت (غير معروفة)يتم كتابة جديدة
  - برامج مكافحة الفيروسات الحديثة البحث عن الأنشطة مثل فيروس المشبوهة وكذلك تواقيع الفيروسات
  - حافظ على برامج مكافحة الفيروسات الخاص بك حتى الآن.

برامج مكافحة الفيروسات

وجاء جهاز الكمبيوتر الخاص بي الجديد مع برامج مكافحة الفيروسات تثبيت، لذلك لا ينبغي أن سبق لي أن تكون محمية؟

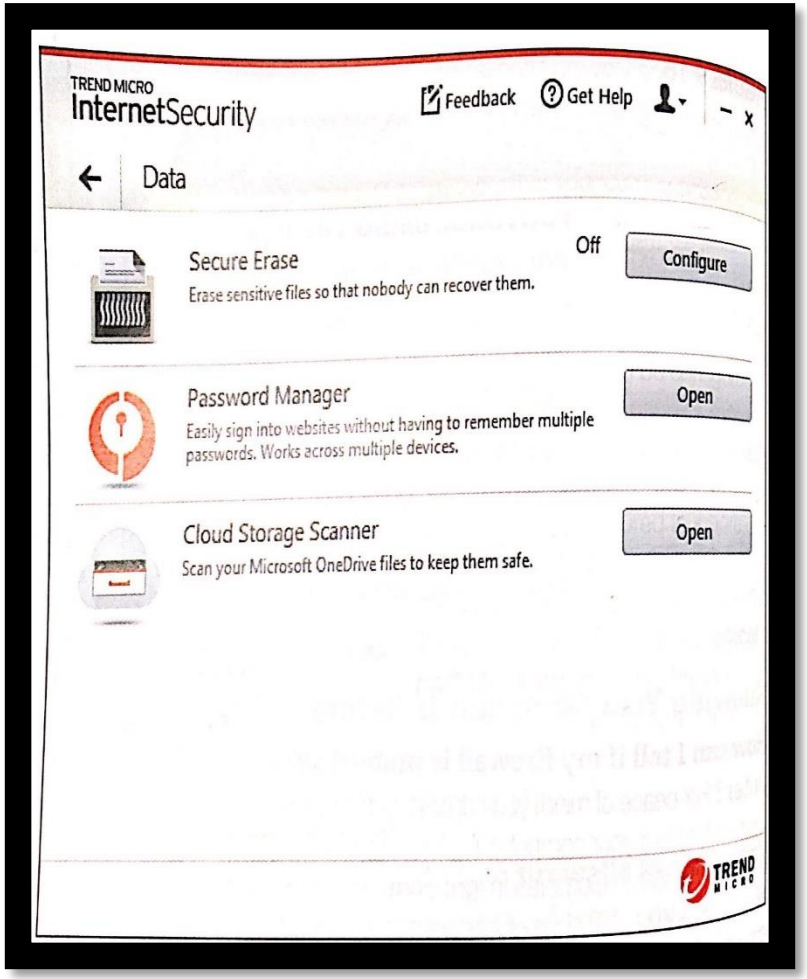
- هذه عادة ما تكون الإصدارات التجريبية التي توفر تحديثات البرنامج لفترة محدودة من الزمن(يوما 180أو 90).
- لديك شراء النسخة الكاملة من البرنامج للتأكد من أنك لا تزال محمية من الفيروسات الجديدة
- ، إذا كان هناك أي برامج مكافحة الفيروسات طرف ثالث مثبتة، والمدافع 10في ويندوز النوافذ تكون نشطة افتراضيا.

برامج مكافحة الفيروسات

كيف أتأكد من بلدي برامج مكافحة الفيروسات هو حتى الآن؟

- معظم برامج مكافحة الفيروسات لديها ميزة التحديث التلقائي في كل مرة تذهب على الانترنت
- عادة ما يظهر حالة الاشتراك التحديث.
- العديد من حزم الإنترنت توفر ميزات مكافأة مثل الماسحات الضوئية سحابة التخزين ومديري كلمة السر لتوفير لكم مع حماية إضافية.

برامج مكافحة الفيروسات



برامج مكافحة الفيروسات

ماذا علي أن أفعل إذا أعتقد أن إصابة جهاز الكمبيوتر الخاص بي مع الفيروس؟

- تمهيد الكمبيوتر باستخدام قرص التثبيت مكافحة الفيروسات
  - إذا قمت بتنزيلها من الإنترنت DVDنسخ الملفات برامج مكافحة الفيروسات ل.
- إذا كان البرنامج بالكشف عن الفيروسات، قد البحث فيها أيضا على تحديد ما إذا كنت سوف تحتاج إلى اتخاذ خطوات يدوية إضافية للقضاء على الفيروسات.
  - تحتوي على أرشيف Symantecمعظم المواقع الإلكترونية للشركة مكافحة الفيروسات مثل موقع للمعلومات عن الفيروسات وتقدم خطوة خطوة حلول لإزالتها

برامج مكافحة الفيروسات

- **كيف يمكنني حماية هاتفي من الفيروسات؟**
  - مجرمو الإنترنت يختبئون الآن الفيروسات في تطبيقات تبحث المشروعة للتحميل على الأجهزة النقالة
  - برامج الحماية من الفيروسات المصممة خصيصا للأجهزة النقالة
    - عرض المنتجات الخالية فعالة لحماية أجهزة أندرويد Google Playفي متجر (أفاست الأمن موبايل، 360 و الأمن).
  - توفر أيضا الحماية من البرامج الضارة مثل القدرة على مسح محتويات الهاتف الخاص بك إذا فقدت أو سرقت.

تحديثات البرنامج

لماذا تحديث برنامج نظام التشغيل الخاص بي مساعدة في حماية لي من الفيروسات؟

- العديد من الفيروسات استغلال نقاط الضعف في أنظمة التشغيل.
- يمكن تعيين المواقع الخبيثة تصل لمهاجمة جهاز الكمبيوتر **تدفع من قبل هجوم التنزيل:** الخاص بك عن طريق تحميل برامج ضارة على جهاز الكمبيوتر الخاص بك.
  - صفحات الويب 1000في 1حملة عن طريق التحميل يؤثر ما يقرب من.
- تأكد من نظام التشغيل الخاص بك هو حتى الآن وتحتوي على أقل تصحيحات الأمان.

تحديثات البرنامج

هل تحديثات نظام التشغيل يحدث فقط تلقائيا؟

- Microsoft.، والآن تحميل التحديثات تلقائيا كلما يتم توفيرها من قبل 10في ويندوز
  - لجدولة تلقائيا إعادة تشغيل الكمبيوتر لتطبيق التحديثات أو اختيار وقت Windowsلديك خيار للسماح إعادة تشغيل أكثر ملاءمة يدويا.
- OS Xماك لديه فائدة مماثلة لجمع التحديثات.
- توفر بعض الخيارات الأخرى مثل القدرة Windows Updateالشاشة خيارات متقدمة ل Microsoftعلى الحصول على التحديثات لمنتجات الأخرى(MS مكتب).

تحديثات البرنامج

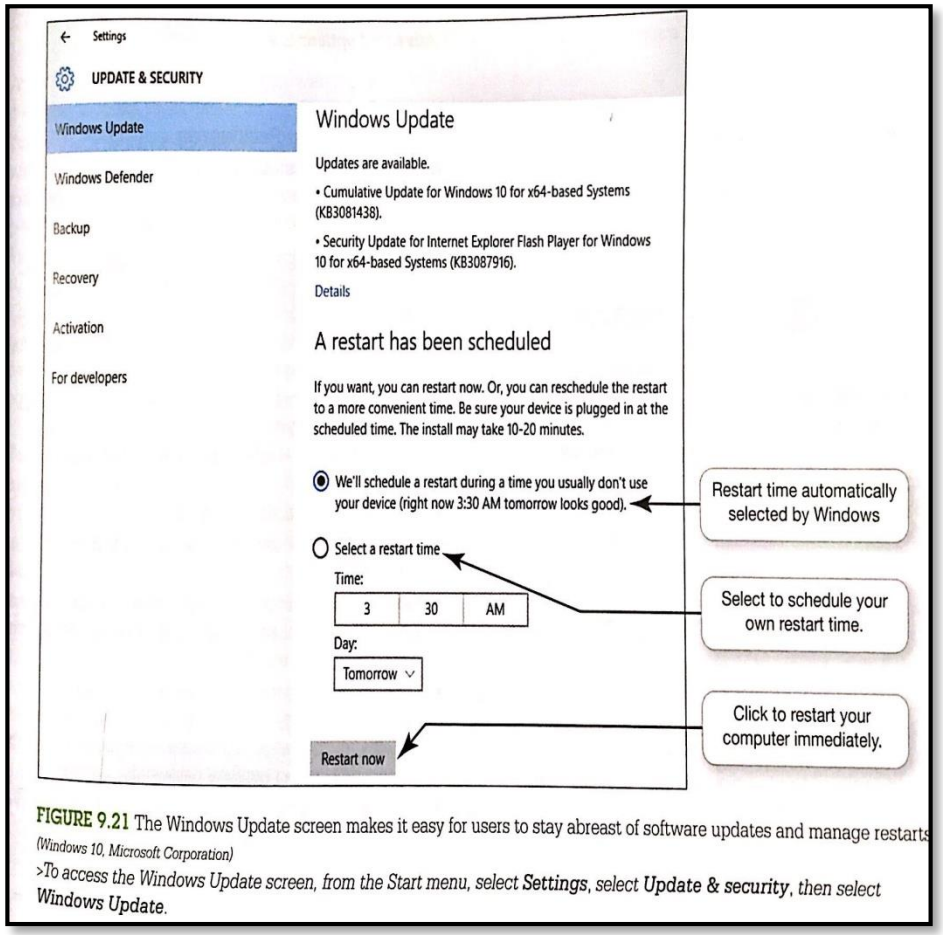


FIGURE 9.21 The Windows Update screen makes it easy for users to stay abreast of software updates and manage restarts *(Windows 10, Microsoft Corporation)*

>*To access the Windows Update screen, from the Start menu, select* ***Settings****, select* ***Update & security****, then select* ***Windows Update****.*

تحديثات البرنامج

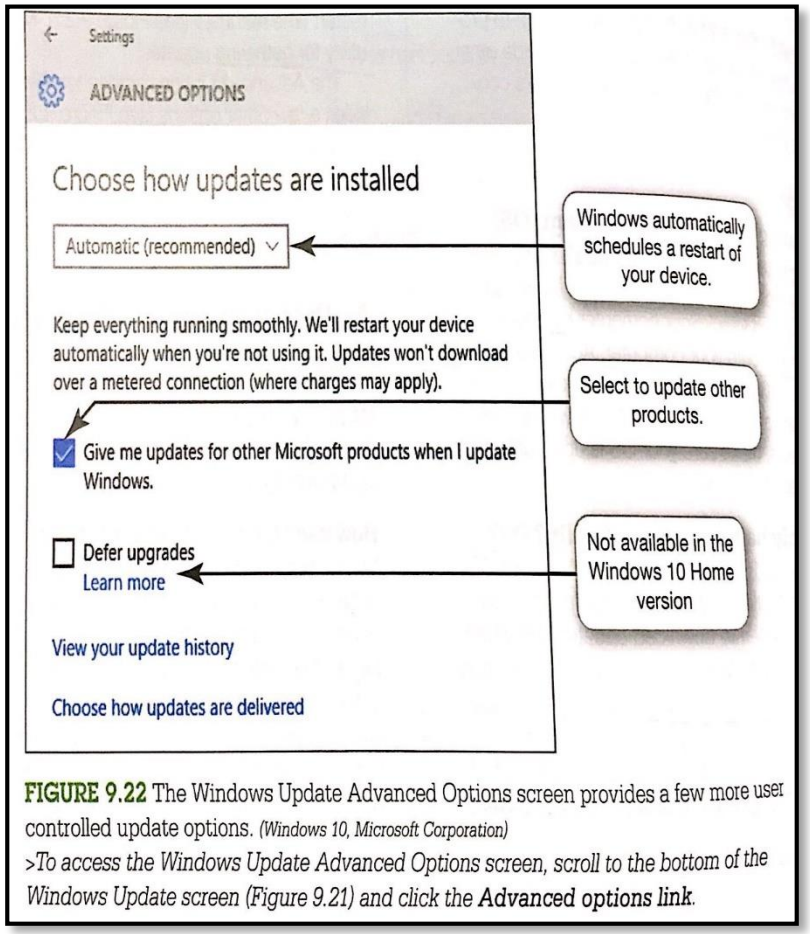


FIGURE 9.22 The Windows Update Advanced Options screen provides a few more user controlled update options. *(Windows 10, Microsoft Corporation)*

>To access the Windows Update Advanced Options screen, scroll to the bottom of the Windows Update screen (Figure 9.21) and click the ***Advanced options link****.*

كلمات المرور والقياسات الحيوية :المصادقة

كيف يمكنني أفضل كلمات السر باستخدام لحماية جهاز الكمبيوتر الخاص بي؟

- تلك التي يصعب على القراصنة تخمين هو أكثر أهمية من أي (آمنة)خلق قوية كلمات السر وقت مضى.
- قراصنة يهاجمون مواقع الدفاع عنهم ضعيفا لكلمات السر لأن الكثير من الناس استخدام نفس كلمة السر لكل موقع يستخدمونها.
  - لذا، إذا يمكن للقراصنة الحصول على كلمة السر الخاصة بك من موقع الألعاب سيئة المضمون، لأنها قد تكون قادرة على الوصول إلى حسابك المصرفي مع نفس كلمة السر.

كلمات المرور والقياسات الحيوية :المصادقة

كيفية إنشاء كلمة مرور قوية؟

- كلمات مرور قوية وصعبة لشخص تخمينها.
- **القواعد الارشادية:**
  - لا تستخدم مكونات استخلاصه بسهولة المتعلقة بالحياة الخاصة بك(الاسم، العنوان،...)
  - لا يقل عن 14 حرفا.
  - هل كلمات لا تستخدم موجودة في القاموس
  - مزيج العليا والسفلى الحروف والرموز.
  - لم تخبر أحدا كلمة المرور الخاصة بك أو تدونها في مكان قد يرى آخرون.
  - تغيير كلمة المرور الخاصة بك في أساس منتظم
  - لا تستخدم نفس كلمة السر لكل حساب لديك.
- هناك العديد من مولد كلمة السر متاح مجانا لمساعدتك على إنشاء كلمات مرور آمنة. (strongpasswordgenerator.com)

كلمات المرور والقياسات الحيوية :المصادقة

Strong and Weak Password Candidates

PASSWORD	RATING	GOOD POINTS	BAD POINTS
Joysmithl022	Poor	• Contains upper- and lowercase letters • Contains letters and numbers	• Less than 14 characters • Contains name and birth date
test44drive6car	Mediocre	• 15 characters in length	• Contains three words found in the dictionary • Numbers repeated consecutively
8$RanT%5ydTTtt&	Better	• Good length • Contains upper- and lowercase letters • Contains symbols	• Upper- and lowercase letters repeated consecutively • Still contains one dictionary word (rant)
7R3m3mB3R$5%y38	Best	• All good points from above • Dictionary word (remember) has 3s instead of Es	• None

كلمات المرور والقياسات الحيوية :المصادقة

كيف يمكنني التحقق من مدى قوة كلمة المرور الخاصة بي؟

- استخدام الانترنت اختبار قوة كلمة المرور، مثل عداد كلمة (passwordmeter.com)

كيف يمكنني تقييد الوصول إلى جهاز الكمبيوتر الخاص بي؟

- أخرى كلمة السر أو رمز مرور لحماية OS، ومعظم OS X، Windowsقد بنيت في نظام التشغيل الملفات وكذلك سطح المكتب بأكمله.
- جهاز الكمبيوتر الخاص بك تلقائيا كلمة المغلقة بعد فترة معينة من الوقت الضائع.
- لك استخدام كلمات السر الصورة في العمل بوصفه طريقة إضافية للوصول إلى جهاز WSنوافذ ألو الكمبيوتر الخاص بك.
  - اختار صورة ثم رسم ثلاثة بحركات على أنه إما الخطوط المستقيمة والدوائر أو الصنابير.
  - إذا كنت قد نسيت الإيماءات، يمكنك الوصول إلى جهاز الكمبيوتر الخاص بك دائما عبر كلمة السر التقليدية.

كلمات المرور والقياسات الحيوية :المصادقة

FIGURE 9.25 Drawing three gestures (a swipe and two circles) on this image (and repeating them once) sets your picture password options in Windows. *(Windows 10, Microsoft Corporation)*

إدارة كلمات السر الخاصة بك

كيف يمكنني تذكر كل كلمات السر الخاصة بي معقدة؟

- أدوات إدارة كلمة المرور(البرامج).

أين يمكنني الحصول على برنامج إدارة كلمة المرور؟

- معظم أجنحة أمن الإنترنت الحالية ومتصفحات الويب تجعل من السهل تتبع كلمة المرور عن طريق توفير أدوات إدارة بكلمة مرور(البرامج).
  - على سبيل المثال: مايكروسوفت سوف حافة تذكر كلمات السر الخاصة بك بالنسبة لك.
- هناك بعض كلمات المرور التي يجب أن لا يكون متصفحك أن نتذكر، مثل كلمة المصرفية عبر الانترنت.

إدارة كلمات السر الخاصة بك

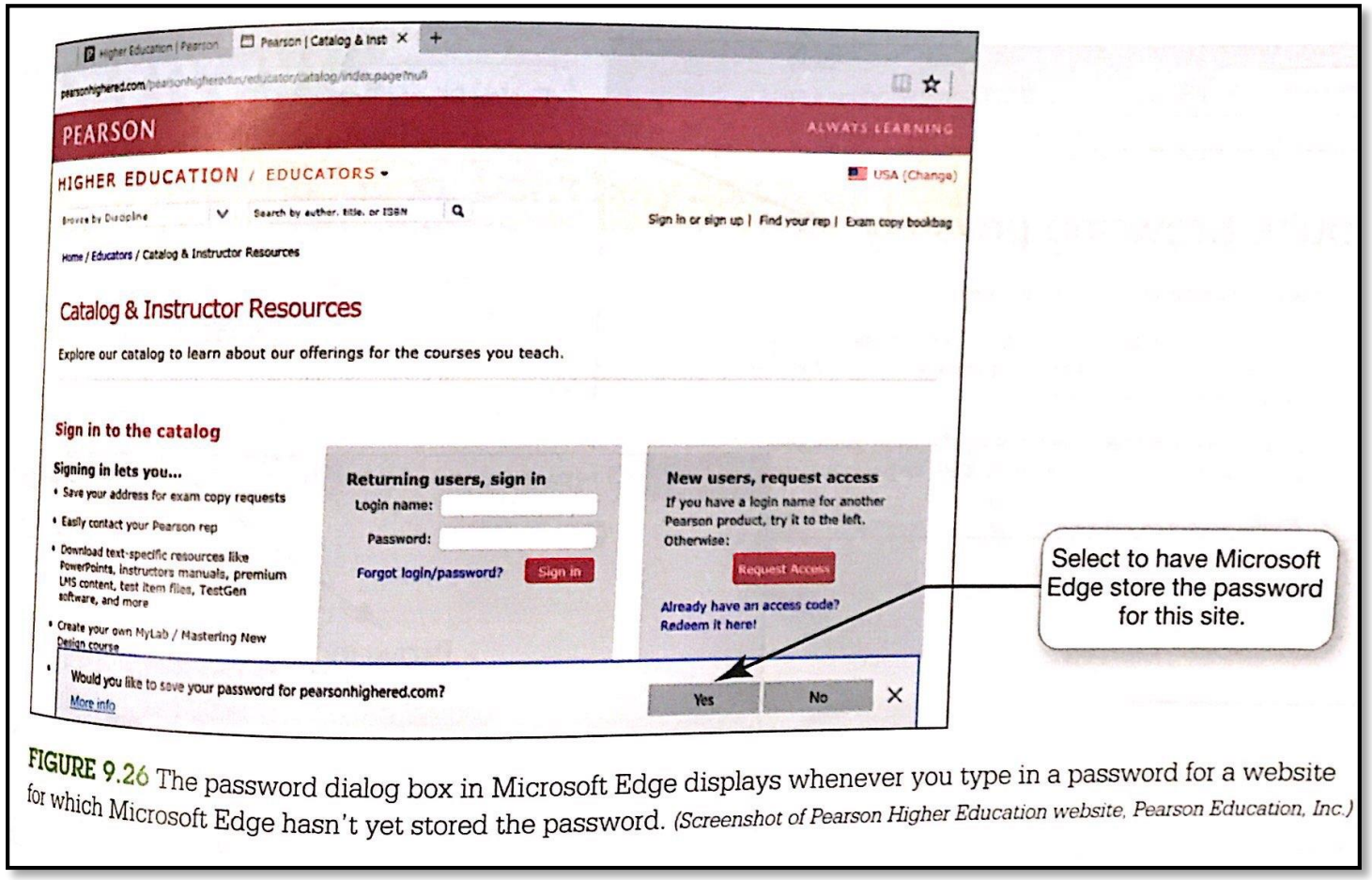


FIGURE 9.26 The password dialog box in Microsoft Edge displays whenever you type in a password for a website for which Microsoft Edge hasn't yet stored the password. *(Screenshot of Pearson Higher Education website, Pearson Education, Inc.)*

بصمات أجهزة مصادقة

بجانب كلمات السر، وإلا كيف يمكن أن تحد من استخدام جهاز الكمبيوتر الخاص بي؟

- **البيومترية جهاز المصادقة:** هو الجهاز الذي يقرأ سمة شخصية فريدة مثل بصمات الأصابع أو نمط القزحية في العين وتحويل نمطها إلى رمز رقمي.
- وتوفر هذه الأجهزة مستوى عال من الأمن لأنه لا يوجد اثنين من الناس لديهم نفس الخصائص البيولوجية.
- أنها تقضي على الأخطاء البشرية التي يمكن أن تحدث في حماية كلمة السر.
  - مثلا، اي فون وسامسونج غالاكسي الهواتف وقارئ بصمات الأصابع ونظم الجوائز الوجه.

كلمات المرور والقياسات الحيوية :المصادقة

- بصمة
- نمط قزحية العين في
- المصادقة صوت
- التعرف على الأنماط وجهه
- توفير مستوى عال من الأمن

إخفاء عن أعين المتطفلين :مجهول بتصفح الإنترنت

يجب أن أقلق من تصفح الإنترنت على جهاز الكمبيوتر المشتركة العام أو العمل؟

- أنت لا تعرف أبدا ما قد تم تركيب أدوات الشائنة من قبل قراصنة على أجهزة الكمبيوتر العامة
- العديد من أرباب العمل بشكل روتيني مراجعة تاريخ تصفح الإنترنت من الموظفين لضمان حصول العمال يقضون وقتهم على الإنترنت بشكل مثمر.

إخفاء عن أعين المتطفلين :مجهول بتصفح الإنترنت

ما هي الأدوات التي يمكنني استخدامها للحفاظ على أنشطة تصفح بلدي خاصة عند تصفح الإنترنت؟

- وتشمل الإصدارات الحالية من موزيلا فايرفوكس، مايكروسوفت إيدج وجوجل كروم أدوات الاشتراكات، والتستر على التوالي InPrivateوتسمى التصفح الخاص،)الخصوصية).
- إذا اخترت لتصفح المجهول:
  - سوف إصدار خاص من نوافذ المتصفح المفتوحة.
  - أيضا .لا تظهر كل السجلات إذا المواقع التي تزورها وملفات قمت بتحميلها في تاريخ شبكة الإنترنت يتم حذف أي ملفات مؤقتة ولدت في هذا الاستعراض عند الخروج من نافذة خاصة.

إخفاء عن أعين المتطفلين :مجهول بتصفح الإنترنت

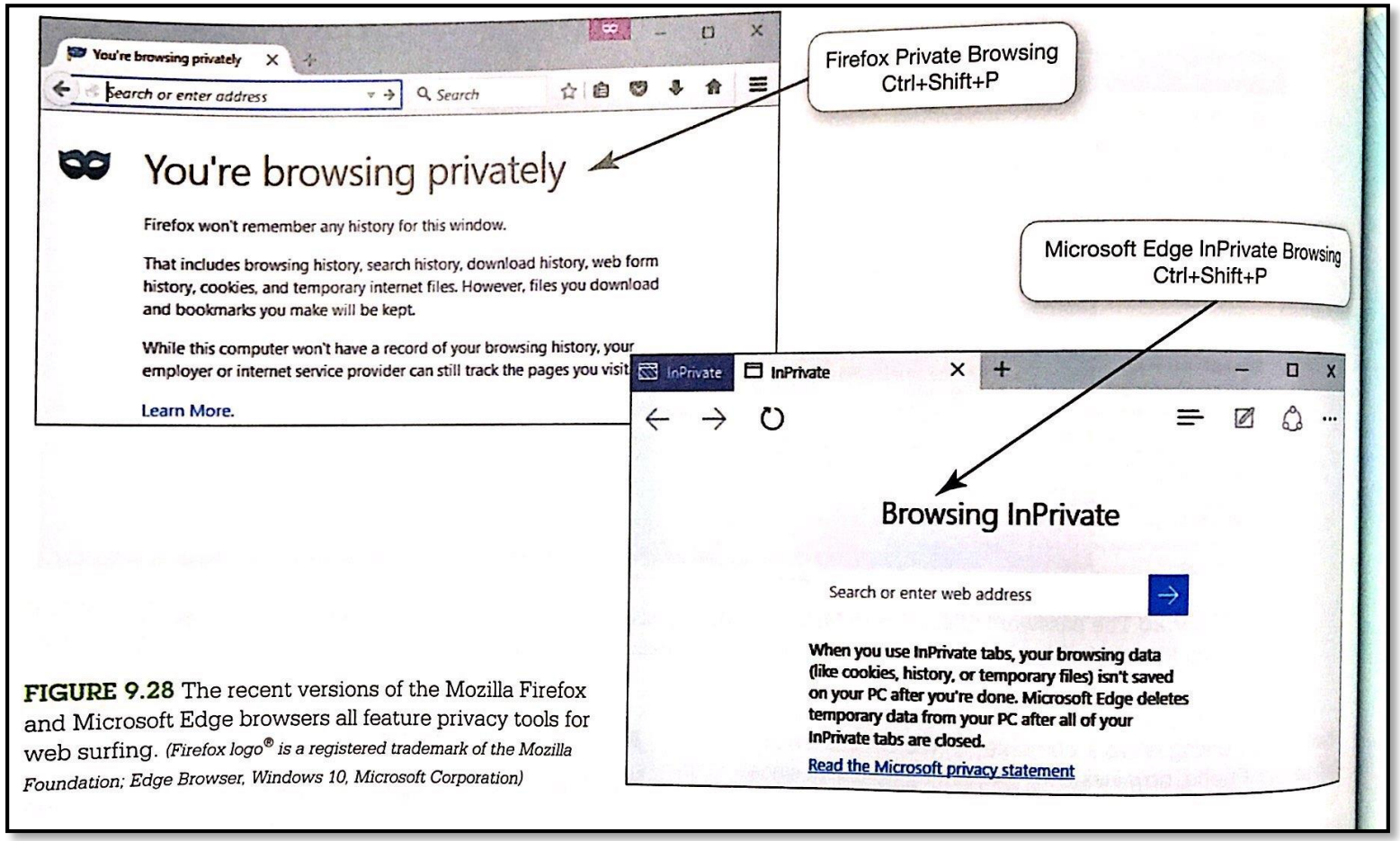


FIGURE 9.28 The recent versions of the Mozilla Firefox and Microsoft Edge browsers all feature privacy tools for web surfing. *(Firefox logo® is a registered trademark of the Mozilla Foundation; Edge Browser, Windows 10, Microsoft Corporation)*

إخفاء عن أعين المتطفلين :مجهول بتصفح الإنترنت

هل هناك أي أدوات أخرى يمكنني أن استخدامها لحماية الخصوصية؟

- الشخصية محركات الأقراص فلاش Ironkeyالأجهزة المحمولة مثل الخصوصية (ironkey.com)
- سيتم تخزين كافة ملفات إنترنت الحساسة، مثل الكوكيز، وكلمات السر، تاريخ الإنترنت، ومخابئ متصفح على الجهاز الخصوصية، وليس على جهاز الكمبيوتر الذي تستخدمه.
- الخاص بك من أعين المتطفلين IPحماية عنوان.
- هل لديك أدوات إدارة كلمة المرور التي تخزين كل معلومات تسجيل الدخول الخاصة بك وتشفيرها.

إخفاء عن أعين المتطفلين :مجهول بتصفح الإنترنت

هل هناك أي شيء آخر يمكنني القيام به للحفاظ على البيانات الخاصة بي آمنة على جهاز الكمبيوتر مشترك؟

- خذ نظام لينكس معك على محرك أقراص فلاش، وتجنب استخدام الكمبيوتر الصورة OS العامة أو العمل.
  - **مزايا استخدام نظام التشغيل لينكس:**
    - لأن تمهيد الكمبيوتر من محرك أقراص فلاش يلغي تماما أي تفاعل مع نظام التشغيل الخاص بالكمبيوتر. والحد بشكل كبير من التقاط الفيروسات والبرامج الضارة الأخرى.
    - الفيروسات والقرصنة ضد لينكس عالبريد اقل عرضة بكثير من الهجمات ضد ويندوز.
    - كنت لا تترك آثار النشاط الخاص وراء لأنك تجنب القراءة والكتابة إلى القرص الصلب لجهاز الكمبيوتر.
  - Pendrivelinux.com مصدرا ممتازا التي تقدم إصدارات مختلفة من لينكس.
  - لMac OS توزيعة الابتدائية لونا لينكس يوفر مفهوم تقريبي لOS X.

إخفاء عن أعين المتطفلين :مجهول بتصفح الإنترنت

كيف يمكنني أن أحمي نقل بيانات حساسة إذا كان لدي لاستخدام الشبكة اللاسلكية العامة؟

- **شبكة خاصة افتراضية** هي شبكات آمنة التي يتم وضعها باستخدام البنية التحتية للإنترنت العامة.
  - البيانات المرسلة آمنة كما) .باستخدام البرمجيات المتخصصة والخوادم وبروتوكولات نقل البيانات (إرساله على شبكة اتصال خاصة

حماية الملكية الرقمية الخاصة بك

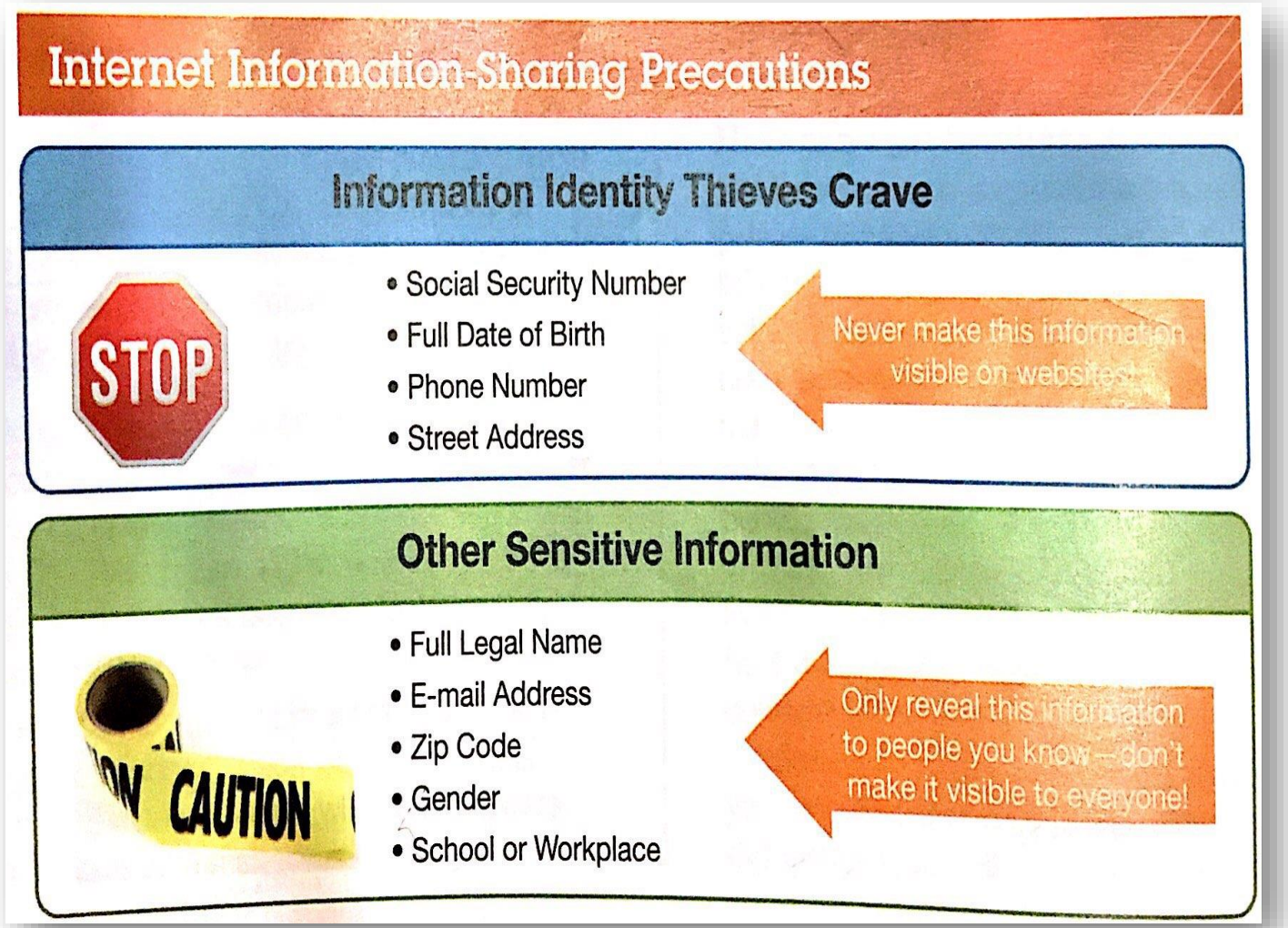
1. تقييد الوصول إلى الأصول الرقمية الخاصة بك
2. حفظ البيانات الخاصة بك آمنة
3. حماية لديك الحاسبات البدنية الأصول

حماية المعلومات الشخصية الخاصة بك

- مع جرائم الإنترنت مثل سرقة الهوية متفشية، تحتاج إلى اتخاذ خطوات لحماية المعلومات الشخصية الخاصة بك.
- **ما هي المعلومات التي يجب أن لا مشاركة على المواقع؟**
  - الكشف عن معلومات أقل قدر ممكن، وخصوصا إذا كانت المعلومات ستكون متاحة للجميع.
  - **أربعة مفاتيح المعلومات** اللازمة لالصلب الهوية:
    - رقم الحماية الاجتماعية
    - رقم الهاتف
    - تاريخ الولادة
    - عنوان الشارع

حماية المعلومات الشخصية الخاصة بك

- المبادئ التوجيهية جيدة:



حماية المعلومات الشخصية الخاصة بك

- **كيف يمكنني معرفة ما الذي يمكن أن يرى معلوماتي على الشبكة الاجتماعية؟**

تغيير إعدادات الخصوصية الافتراضية في ملفك الشخصي في الفيسبوك على سبيل المثال، للتأكد من أنك لا تبادل المعلومات على نطاق أوسع مما يجب.

- **كيف يمكنني حماية المعلومات الخاصة بي في الفيسبوك؟**
  - تغيير إعدادات الخصوصية في ملفك الشخصي
    - تعيين معظم الخيارات في قسم معلومات أساسية لملفك الشخصي للأصدقاء أو بي فقط.
    - في قسم معلومات الاتصال، والحد من هذه المعلومات فقط للأصدقاء أو لنفسك أمر حتمي.

النسخ الاحتياطي البيانات الخاصة بك

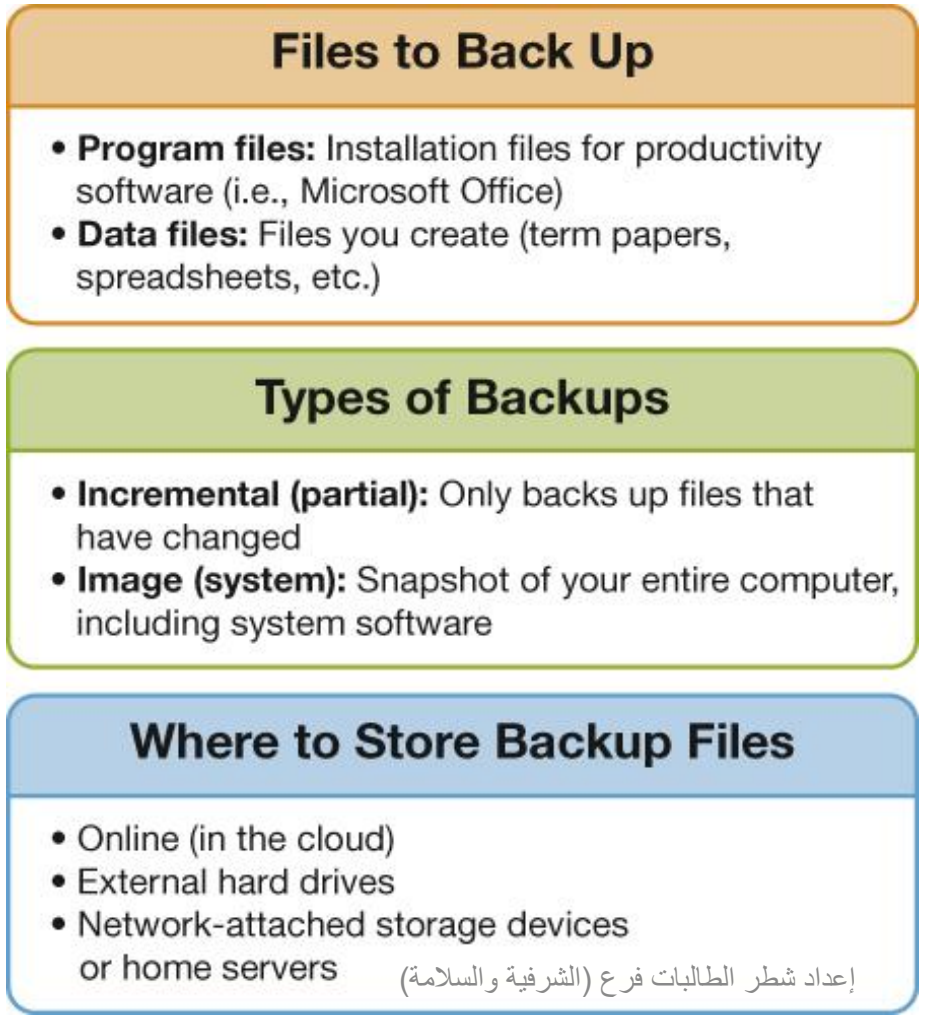
- **كيف يمكن أن تلحق الضرر البيانات الموجودة على جهاز الكمبيوتر الخاص بي؟**
- ثلاثة تهديدات الرئيسية التي تواجه البيانات الموجودة على جهاز الكمبيوتر الخاص بك:
  - دخول غير مرخص
  - العبث
  - تدمير

قد تفقد البيانات الخاصة بك عن غير قصد:

- الملفات المحذوفة عن طريق الخطأ
- إسقاط الكمبيوتر المحمول على الأرض.
- الفيروس من مرفق البريد الإلكتروني.
- تشتعل فيها النيران منزلك

النسخ الاحتياطي البيانات الخاصة بك

- استراتيجية النسخ الاحتياطي للملفات الخاصة بك



النسخ الاحتياطي البيانات الخاصة بك

- **النسخ الاحتياطي** هي نسخ من الملفات التي يمكنك استخدامها لتحل محل النسخ الأصلية لو انهم المفقودة أو التالفة.

أي نوع من الملفات أقوم بحاجة الى الدعم؟

1. **ملف البرنامج:** الملفات المستخدمة لتثبيت البرامج
   - DVD
   - تحميلها من الإنترنت.
2. **ملف البيانات :** الملفات التي قمت بإنشائها أو شراؤها)الأبحاث وجداول البيانات والموسيقى وملفات الصور وقوائم الاتصال، ودفاتر العناوين....

النسخ الاحتياطي البيانات الخاصة بك

ما نوع النسخ الاحتياطي يمكن أن أقوم بها؟

هناك خياران رئيسيان لالنسخ الاحتياطي للملفات:

1. **النسخ الاحتياطي الجزئي)نسخ احتياطي تزايدي):**
   - النسخ الاحتياطي للملفات التي تغيرت أو تم إنشاؤها منذ أن تم إجراء النسخ الاحتياطي الأخير فقط
   - توفيرا للوقت.
   - أكثر كفاءة من نسخة احتياطية الصورة.
2. **احتياطية للنظام)صورة احتياطية):**
   - وتدعم كل نظام، والتطبيق، وملفات بيانات تصل، وليس فقط الملفات التي تغيرت.
   - يضمن لك التقاط تغييرات على ملفات التطبيق مثل تحديثات البرامج التلقائي الذي قد لا التقاط نسخ احتياطي تزايدي.
   - مفيدة في مجموع فشل القرص الصلب، وتكوين جهاز الكمبيوتر الخاص بك وسوف يكون بالضبط ما كان عليه من قبل.

النسخ الاحتياطي البيانات الخاصة بك

- **أين يجب أن تخزين بلدي احتياطية؟**
  - يجب تخزينها بعيدا عن حيث يقع جهاز الكمبيوتر الخاص بك
  - يجب أن يتم تخزين اثنين على الأقل من أماكن مختلفة.
  - حيث لإجراء نسخ احتياطي:

1. (في سحابة)على الانترنت
2. محركات الأقراص الصلبة الخارجية
3. شبكة التخزين المرفقة **(NAS)** الأجهزة والخوادم المنزل.

حفظ البيانات الخاصة بك آمنة

النسخ الاحتياطي البيانات الخاصة بك

A Comparison of Typical Data Backup Locations

BACKUP LOCATION	PROS	CONS
Online (in the Cloud) 	• Files stored at a secure, remote location • Files/backups accessible anywhere through a browser	• Most free storage sites don't provide enough space for image backups
External Hard Drive 	• Inexpensive, one-time cost • Fast backups with USB 3.0 devices connected directly to your computer	• Could be destroyed in one event (fire/ flood) with your computer • Can be stolen • Slightly more difficult to back up multiple computers with one device
Network-Attached Storage (NAS) Device and Home Server 	• Makes backups much easier for multiple computing devices	• More expensive than a stand-alone external hard drive • Could be destroyed in one event (fire/ flood) with your computer • Can be stolen

النسخ الاحتياطي البيانات الخاصة بك

- 1. **على الانترنت(في سحابة):**
  - لا حاجة إلى أن يكون في المنزل أو مقبض حول القرص الصلب الخارجي.
  - أمنا.
  - مكان بعيد
  - أقل عرضة بكثير للكوارث البيانات.
  - Adrive (لا يكفي للنسخ الاحتياطي الصورة) مايكروسوفت مجانا ون درايف و.
  - Ibackup: كاربونايت و :مع رسوم الاشتراك (صورة احتياطية)المزيد من السعة التخزينية.

النسخ الاحتياطي البيانات الخاصة بك

2. محركات الأقراص الصلبة الخارجية:

- أو كبيرة ذاكرة فلاش سعة
- يمكن أن تفشل محركات الأقراص الصلبة الخارجية وفقدان البيانات الخاصة بك احتياطيا
- لمزيد من السلامة، وأفضل لاستخدام محركات الأقراص الصلبة الخارجية بالتزامن مع استراتيجية النسخ الاحتياطي عبر الإنترنت.

3. الأجهزة والخدمات المنزلية (NAS)التخزين المتصلة بالشبكة:

- هم أساسا محركات الأقراص الصلبة الكبيرة متصلا بشبكة من أجهزة الكمبيوتر بدلا من كمبيوتر واحد.
- أنها يمكن أن تستخدم لدعم أجهزة كمبيوتر متعددة في وقت واحد.
- ذات قدرة عالية لدعم التحديث تلقائيا وتبادل الملفات NASالخوادم الرئيسية بمثابة أجهزة.

النسخ الاحتياطي البيانات الخاصة بك

- **كم مرة يجب أن النسخ الاحتياطي للبيانات الخاصة بي؟**
  - من الصعب أن نتذكر)في كل مرة كنت إجراء تغييرات عليها(.
  - النسخ الاحتياطي البرمجيات يمكن تهيئتها لإجراء عمليات النسخ تلقائيا.
  - مثال: سجل ويندوز ملف فائدة.
- **كم مرة يجب أن خلق صورة احتياطية؟**
  - لأن ملفات البرنامج ونظام التشغيل الخاص بك لا تتغير كلما ملفات البيانات الخاصة بك، يمكنك تنفيذ عمليات النسخ الاحتياطي على صورة **وأقل تواترا** أساس.
  - يمكنك أن تفعل ذلك على أساس أسبوعي
  - ينبغي أن تؤدي بالتأكيد واحدة **بعد تثبيت** برامج جديدة.

النسخ الاحتياطي البيانات الخاصة بك

- صورة النظام أداة النسخ الاحتياطي

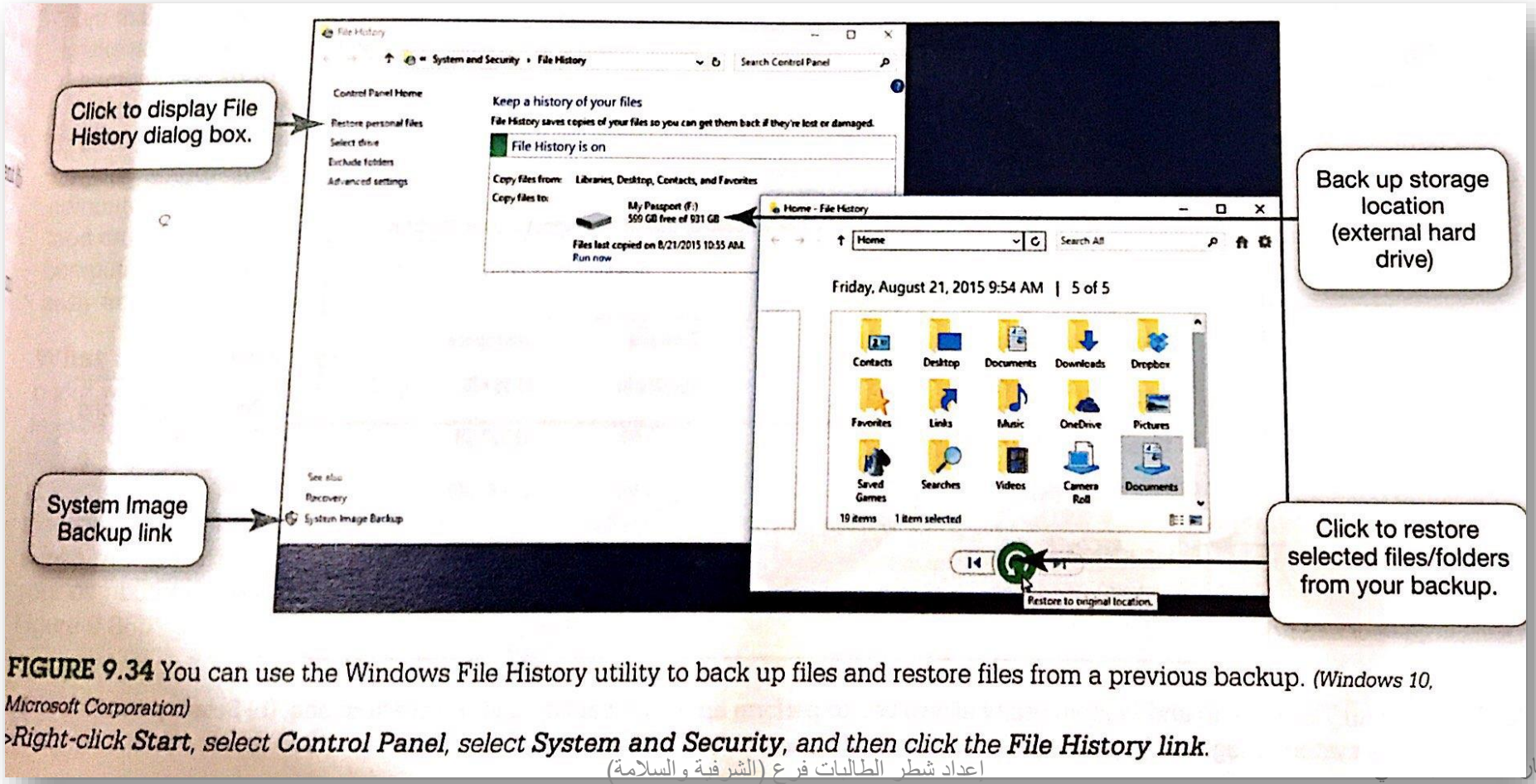


FIGURE 9.34 You can use the Windows File History utility to back up files and restore files from a previous backup. *(Windows 10, Microsoft Corporation)*

>Right-click ***Start****, select* ***Control Panel****, select* ***System and Security****, and then click the* ***File History*** *link.*

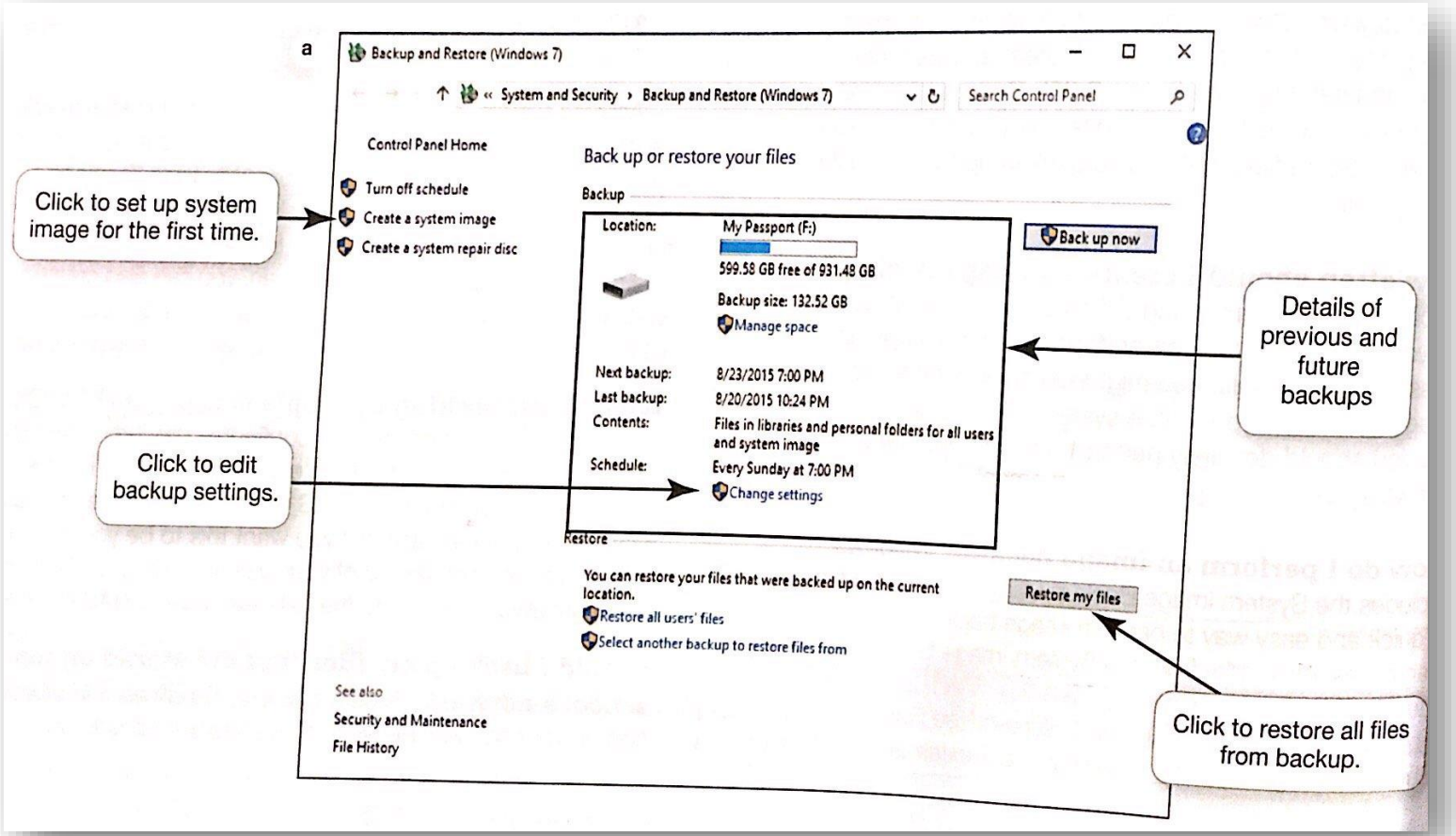
النسخ الاحتياطي البيانات الخاصة بك

- **كيف يمكنني إجراء نسخ احتياطي الصورة؟**
  - على نوافذ نظام صورة أداة النسخ الاحتياطي.
  - النسخ الاحتياطي والاستعادة (10ويندوز)من الشاشة التاريخ الملفات (7ويندوز)،.
  - أو الشبكة NASتحتاج قرص صلب خارجي أو جهاز.
  - خطوات:
    1. انقر على إنشاء رابط صورة النظام، حدد الموقع، انقر فوق التالي.
    2. نسخ احتياطي لكافة ملفات Windowsثم سيقوم .أقسام من جهاز الكمبيوتر الخاص بك لتكون احتياطيا /حدد محركات أقسام المحدد /البيانات وملفات النظام على كافة محركات.
    3. انقر احتياطية بداية لبدء صورة النظام الخاص بك .

  - بعد تشغيل صورة النظام لأول مرة، يمكنك ان ترى نتيجة النسخ الاحتياطي الأخير وتاريخ النسخ يمكنك إنشاء نظام**قرص إصلاح في حالة** التي .يمكنك تغيير الوقت .الاحتياطي المجدول التالي تحتوي على الملفات المستخدمة للإقلاع جهاز الكمبيوتر الخاص بك في حالة وجود خطأ Windows خطير.

النسخ الاحتياطي البيانات الخاصة بك

- النسخ الاحتياطي صورة النظام



النسخ الاحتياطي البيانات الخاصة بك

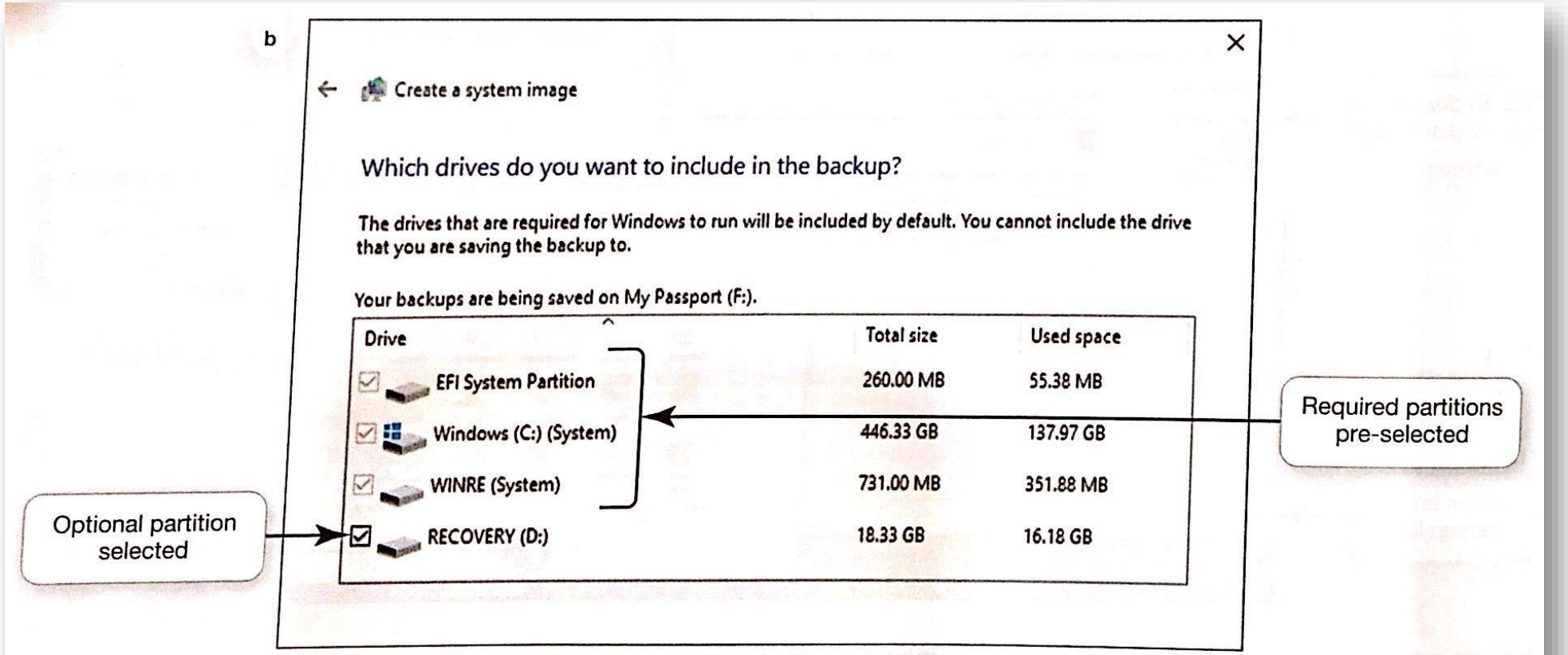


FIGURE 9.35 (a) The Backup and Restore utility allows you to perform an image backup and restore from one. (b) Select partitions to be included in the system image backup. *(Windows 10, Microsoft Corporation)*

النسخ الاحتياطي البيانات الخاصة بك

- **ماذا عن النسخ الاحتياطي كمبيوتر أبل؟**
  - من السهل جدا لتكوين.
  - بالكشف عن الوقت ميزة آلة عندما يتم توصيل ينحدر صلب خارجي إلى الكمبيوتر أو يتم توصيل جهازNAS بك الخاصة الشبكة إلى.
  - ثم سيطلب منك إذا كنت تريد أن يكون محرك النسخ الاحتياطي.
  - وأيد جميع الملفات حتى بما في ذلك ملفات نظام التشغيل إذا أجبت التي كتبهاYES.
- يجب أن النسخ الاحتياطي للملفات بلدي التي يتم تخزينها على شبكة مدرستي؟
  - إذا كنت يسمح لتخزين الملفات هناك، على الأرجح أنها مدعومة بشكل منتظم.
  - اطلب من مسؤول شبكة المدرسة.
  - فمن الأفضل للحفاظ على نسخ احتياطية من ملفاتك نفسك.

حماية لديك الحاسبات البدنية الأصول

- حماية جهاز الكمبيوتر الخاص بك المكونات، قرص أو الهواتف من:

1. العوامل البيئية
2. العواصف الطاقة وانقطاع الكهرباء
3. سرقة.

العوامل البيئية والطاقة العواصف

لماذا هو بيئة حيوية لعمليات بلدي أجهزة الحاسوب؟

أجهزة الكمبيوتر والأجهزة الحساسة، ويمكن أن تضررت من الآثار السلبية لسوء المعاملة أو بيئة فقيرة.

- إذا .يجلس الكمبيوتر على سطح مستو مسطح :حماية الكمبيوتر من حركة مفاجئة كما فشل من قبل كان جهاز الكمبيوتر المحمول، أنها تحمل في حالة وقائية.
- لا تترك في السيارة .الأجهزة الإلكترونية لا يحبون الحرارة الشديدة أو البرد.
- تأكد من .يحسب توليد الكثير من الحرارة، وهذا هو السبب في أنها تحتوي على مراوح التبريد وضع سطح المكتب الخاص بك حيث الفتحات تناول المروحة غير محظورة.
- إذا كان جهاز الكمبيوتر المحمول، واستخدام الحصير البرد التي تحتوي على مراوح التبريد.
- وضع الكمبيوتر في غرفة نظيفة قدر الإمكان.
- تستهلك المواد الغذائية والمشروبات بعيدا عن جهاز الكمبيوتر الخاص بك

العوامل البيئية والطاقة العواصف

ما هي قوة العواصف؟

السلطة عرام يحدث في الحالات التالية:

- يتم تزويد التيار الكهربائي ما يزيد على التيار الكهربائي العادي
- قديم أو خلل الأسلاك
- خطوط الكهرباء التي سقطت
- الصواعق
- أعطال في محطات شركة الكهرباء

العوامل البيئية والطاقة العواصف

- **تصاعد حامية**

هو الجهاز الذي يحمي الكمبيوتر من قوة العواصف

- استبدال كل 2-3 سنوات أو بعد زيادة كبيرة.
- شراء تصاعد حامية التي تشمل أضواء مؤشر.

وإلى جانب جهاز الكمبيوتر الخاص بي، ما الأجهزة الأخرى تحتاج إلى أن تكون متصلا تصاعد حامية؟

- استخدام مع جميع الأجهزة الإلكترونية التي تحتوي على مكونات الحالة الصلبة مثل التلفزيون، ستريو، والطابعات، والهواتف الذكية عند الشحن.
- أكثر ملاءمة للاستخدام **كلها حماة تصاعد منزل** التي تحمي جميع الأجهزة الكهربائية في المنزل

العوامل البيئية والطاقة العواصف

- البيت كله، تصاعد حامية

FIGURE 9.37 A whole-house surge protector is usually installed at the breaker panel or near the electric meter.

العوامل البيئية والطاقة العواصف

- **٪ آمنة عندما موصول تصاعد حامية؟100هي المعدات بلدي**
  - يمكن الصواعق تولد هذه الفولتية العالية التي يمكن أن تطغى تصاعد حامية.
  - فصل الأجهزة الإلكترونية أثناء عاصفة رعدية

منع ومعالجة سرقة

ما الذي أحتاجه للقلق إذا سرق جهاز الحوسبة بلدي؟

- المخاوف الأمنية للهواتف النقالة:
  1. وحفظ لهم من السرقة.
  2. حفظ البيانات آمنة في حال سرقتها.
  3. إذا سرق deiceالعثور على
  4. يتعافى بعد ومحو البيانات من جهاز المسروقة.

إنذار :حفاظ على سلامتهم

ما هو نوع من التنبيه يمكنني تثبيت على جهاز المحمول الخاص بي؟

برنامج المنبه إما بالكشف عن الحركة مثل جهازك الذي التقطت أو أصوات بالقرب خارقة ناقوس الخطر حتى تقوم بإدخال رمز -من جهازك ومن ثم ينطلق الأذن تعطيل.

أنواع برنامج المنبه يمكنك تثبيت:

- برنامج المنبه حركة جيدة وغير مكلفة سرقة رادع.
- مثال على البرمجيات الحرة:
  - Lalarm غير فعالة لأجهزة الكمبيوتر المحمولة.
  - Alarmomatic التطبيق مثل التنبيه الحركة و لباد وفون.

حفظ البيانات الأجهزة المحمولة الآمنة

كيف يمكنني تأمين البيانات على أجهزة الجوال؟

- تشفير البيانات على جهازك المحمول.
- مثال: آمنة هو التطبيق (للحصول على صورة والبيانات في اي فون، آي باد)
  بت والتي من الصعب جدا للقضاء 256، الذي يوفر تشفير
- مثال؛ صندوق قوي المحمول هو التطبيق مشابه لأجهزة الروبوت
- و منزل امن هي لأجهزة الكمبيوتر المحمول ل SensiGuard

توفير التشفير للملفات ومحركات الأقراص الصلبة بالكامل.

تنبيهات البرمجيات والمسحات البيانات

كيف يمكن أن جهاز الكمبيوتر الخاص بي يساعدني على التعافي عندما سرق؟

- جهاز تتبع سرقة السيارات المستخدمة في هو تتبع LoJackنظام مماثل ل البرنامج على النحو التالي:
  - تمكن جهاز :، جهاز الكمبيوتر هاتف المنزل، وماك هاتف المنزلLoJackمطلق الكمبيوتر الخاص بك لتنبيه السلطات إلى موقع الكمبيوتر إذا سرق.
  - iHound: التطبيق تتبع لأجهزة Androidو iOS.

حماية لديك الحاسبات البدنية الأصول

- إذا سرق الجهاز،
  - عن (نقل المعلومات تتبع)اتصل صناعة البرمجيات تتبع والتي سوف تتعقب جهازك طريقIPالموقع برج خلية أو ساخنة نقطة فاي واي ،.
  - سوف تساعد السلطات في تحديد مكان واستعادة الجهاز المحمول الخاص بك.

حماية لديك الحاسبات البدنية الأصول

ماذا لو اللصوص العثور على تتبع البرامج وحذفها؟

- ملفات تتبع البرامج والدلائل غير مرئية.
- وتتبع البرامج يمكن إعادة تثبيت نفسها بعد

عملية إعادة تهيئة.

ماذا لو جهازي لا يمكن استردادها من قبل السلطات؟

- حزم البرمجيات لتحقيق الانتعاش بعد وحذف الملفات.
- وهذه الميزات ويسمح لك لقفل الجهاز أو مسح محتوياته عن بعد عن طريق LoJackمطلق حذف جميع البيانات الخاصة بك
- البحث عن اي فون بلدي لجميع أجهزة دائرة الرقابة الداخلية التي هي جزء من على iCloud
- يرسل النص والرد حسب الموقع، التقاط) أين هو بلدي الروبوت لجميع أجهزة الروبوت الصور مع الجبهة أو الكاميرات الخلفية.

حماية لديك الحاسبات البدنية الأصول

كيف يمكنني التأكد من أنني قد غطت جميع جوانب حماية الأجهزة الرقمية الخاصة بي؟

دليل للتأكد من أنك لم تفوت الأوجه الأمنية الحساسة.

Computer Security Checklist

Firewall

- Do all your computers and tablets have firewall software installed and activated before connecting to the Internet?
- Is your router also able to function as a hardware firewall?
- Have you tested your firewall security by using the free software available at grc.com?

Virus and Spyware Protection

- Is antivirus and anti-spyware software installed on all your devices?
- Is the antivirus and anti-spyware software configured to update itself automatically and regularly?
- Is the software set to scan your device on a regular basis (at least weekly) for viruses and spyware?

Software Updates

- Have you configured your operating systems (Windows, OS X, iOS) to install new software patches and updates automatically?
- Is other software installed on your device, such as Microsoft Office or productivity apps, configured for automatic updates?
- Is the web browser you're using the latest version?

Protecting Your Devices

- Are all computing devices protected from electrical surges?
- Do your mobile devices have alarms or tracking software installed on them?