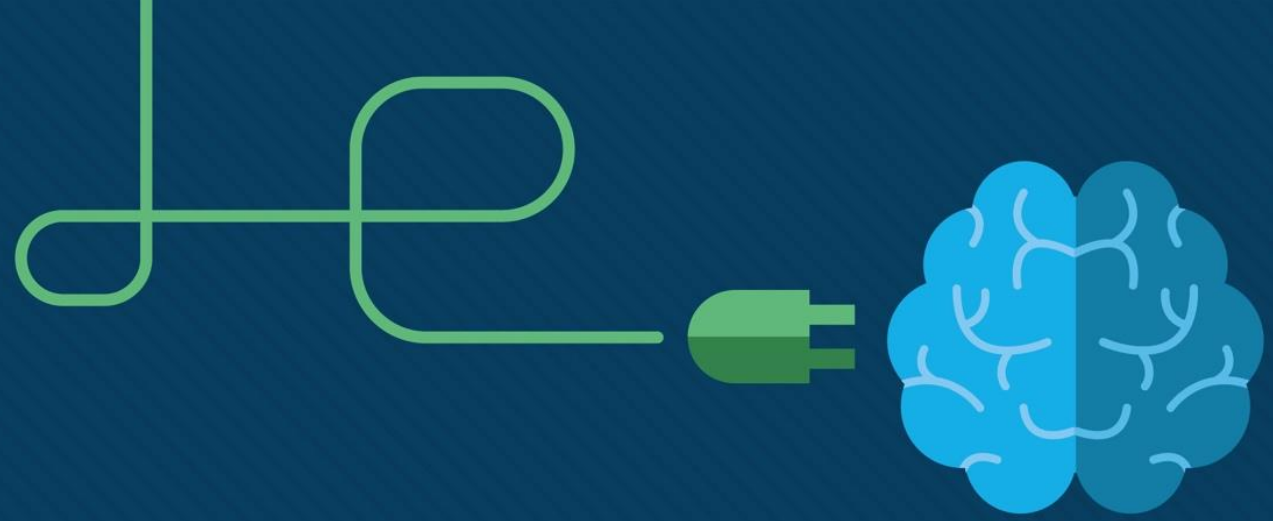
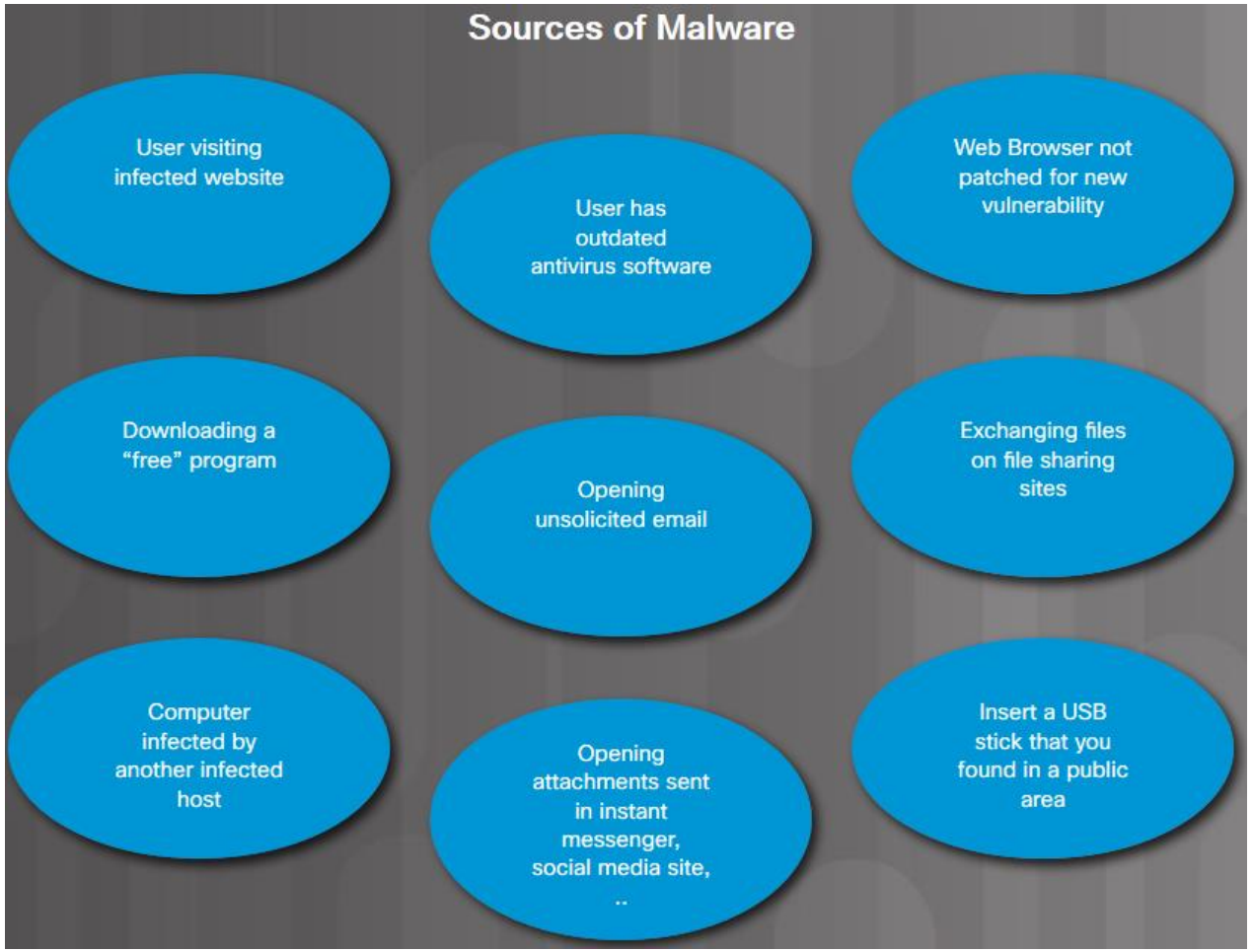


الفصل السادس عشر: التهديدات الأمنية

أساسيات تكنولوجيا المعلومات v7.0

البرامج الضاره

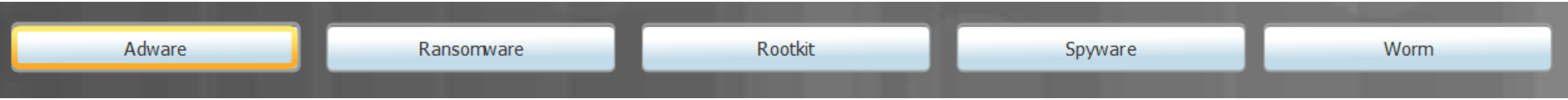


- هناك العديد من أنواع التهديدات التي تم إنشاؤها لتعطيل أجهزة الكمبيوتر والشبكات .
  - التهديد الأكبر والأكثر شيوعا لأجهزة الكمبيوتر والبيانات الواردة عليها هو البرمجيات الخبيثة .
- عادة ما يتم تثبيت البرامج الضارة على جهاز كمبيوتر دون معرفة المستخدم .بمجرد إصابة المضيف، يمكن للبرامج الضارة:
  - تغيير تكوين الكمبيوتر.
  - حذف الملفات أو محركات الأقراص الثابتة الفاسدة.
  - جمع المعلومات المخزنة على الكمبيوتر دون موافقة المستخدم.
  - افتح نوافذ إضافية على الكمبيوتر أو أعد توجيه المتصفح.

الفيروسات وأحصنة طروادة

- النوع الأول والأكثر شيوعا من البرامج الضارة الكمبيوتر هو **الفيروس** .
  - الفيروسات تتطلب العمل البشري لنشر وإصابة أجهزة الكمبيوتر الأخرى .
  - يخفي الفيروس عن طريق إرفاق نفسه برمز الكمبيوتر أو البرامج أو المستندات الموجودة على الكمبيوتر .عند فتحه، ينفذ الفيروس الكمبيوتر ويصيبه .
- مجرمي الإنترنت أيضا استخدام **أحصنة طروادة** للتنازل عن المضيفين .
  - حصان طروادة هو البرنامج الذي يبدو مفيدا ولكن أيضا يحمل التعليمات البرمجية الخبيثة .
  - وغالبا ما يتم توفير أحصنة طروادة مع برامج مجانية على الانترنت مثل ألعاب الكمبيوتر .

أنواع البرامج الضارة



- **Adware** يمكن عرض الإعلانات غير المرغوب فيها باستخدام نوافذ متصفح الويب المنبثقة أو أشرطة الأدوات الجديدة أو إعادة توجيه صفحة ويب بشكل غير متوقع إلى موقع ويب مختلف.
- **Ransomware** عادةً ما يمنع المستخدم من الوصول إلى ملفاته عن طريق تشفير الملفات ثم عرض رسالة تطالب بفدية لمفتاح فك التشفير.
- **Rootkits** من الصعب الكشف عنها وتستخدم من قبل مجرمي الإنترنت للحصول على مستوى المشرف الوصول إلى جهاز كمبيوتر.
- **Spyware** يشبه Adware ولكن يستخدم لجمع المعلومات عن المستخدم وإرسالها مرة أخرى إلى مجرمي الإنترنت.
- **Worms** هي برامج ذاتية النسخ المتماثل التي تنتشر تلقائيًا دون إجراء المستخدم عن طريق استغلال نقاط الضعف في البرامج.

برامج مكافحة البرامج الضارة

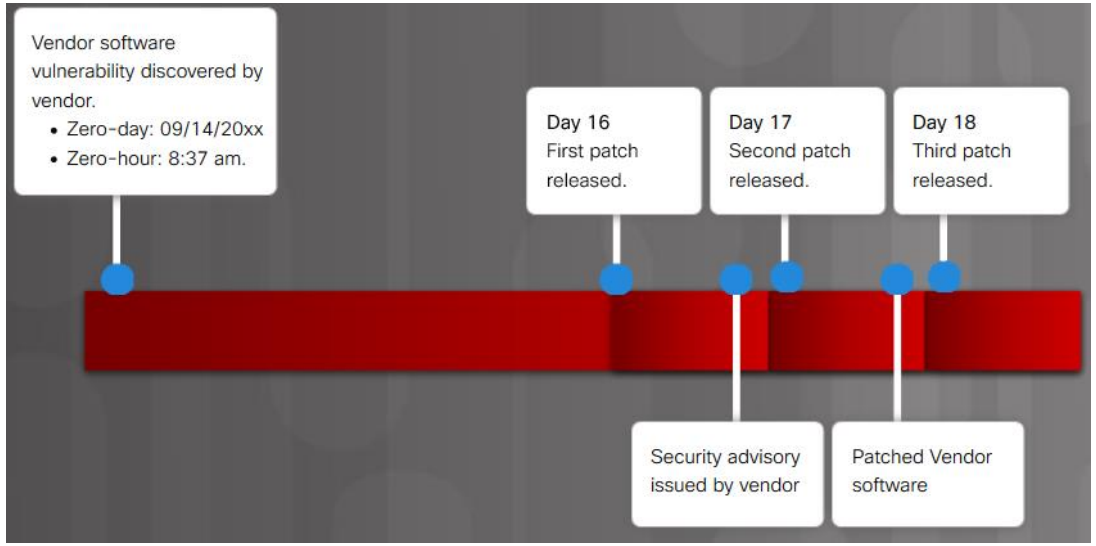
- من المهم أن تقوم بحماية أجهزة الكمبيوتر والأجهزة المحمولة باستخدام برامج مكافحة الفيروسات ذات السمعة الطيبة .
- اليوم ، ويشار إلى برامج مكافحة الفيروسات عادة باسم برامج مكافحة البرامج الضارة
  - برامج مكافحة البرمجيات الخبيثة يمكن الكشف عن ومنع ransomware, spyware, Trojans, rootkits, keyloggers, و adware
  - برامج مكافحة البرامج الضارة تبحث باستمرار عن أنماط معروفة ضد قاعدة بيانات من التوقيعات الخبيثة المعروفة .
  - يمكنهم أيضًا استخدام تقنيات تحديد البرامج الضارة الاستدلالية التي يمكنها اكتشاف سلوك محدد مرتبط ببعض أنواع البرامج الضارة .

أنواع هجمات TCP/IP

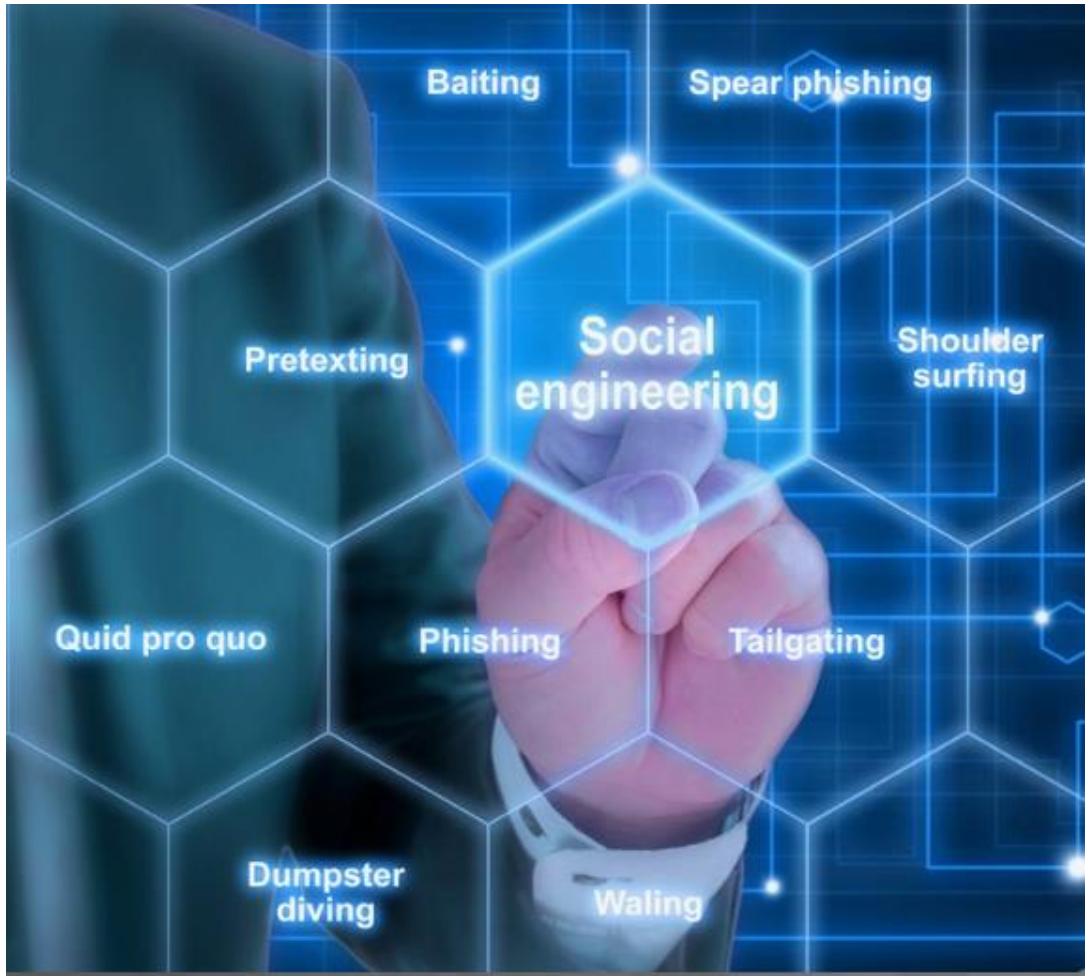
- **رفض الخدمة (DoS)** هو هجوم حيث يطغى المهاجم تمامًا على جهاز مستهدف بطلبات خاطئة لإنشاء رفض الخدمة للمستخدمين الشرعيين.
- **Distributed DoS** هجوم DoS مكبر باستخدام العديد من المضيفين المصابين يسمى الكسالى لتطغى على الهدف.
- **Man-in-the-Middle** هو هجوم حيث يقوم المهاجم باعتراض الاتصال بين مضيفين.

Zero-Day

- يتم استخدام المصطلحين التاليين بشكل شائع لوصف وقت اكتشاف تهديد:
  - **Zero-Day** - يشار إليها أحيانًا أيضًا بهجمات يوم الصفر أو تهديد يوم الصفر أو استغلال يوم الصفر .هذا هو اليوم الذي تم فيه اكتشاف ثغرة أمنية غير معروفة من قبل المورد .المصطلح هو إشارة إلى مقدار الوقت الذي كان لدى المورد لمعالجة مشكلة عدم الحصانة .
  - **Zero-hour -** هذه هي اللحظة التي يتم فيها اكتشاف الاستغلال .
- يمكن استغلال البرنامج حتى يتم توفير تصحيح يعالج مشكلة عدم الحصانة .



الهندسة الاجتماعية



- يستخدم مجرمو الإنترنت تقنيات الهندسة الاجتماعية لخداع الأهداف المطمئنة للكشف عن معلومات سرية.
- الهندسة الاجتماعية هي هجوم الوصول الذي يحاول التلاعب الأفراد في أداء الأعمال أو الكشف عن المعلومات السرية .
- يعتمد المهندسون الاجتماعيون في كثير من الأحيان على الطبيعة البشرية ورغبة الناس في أن يكونوا مفيدين.
- **ملاحظه** وغالبا ما تستخدم الهندسة الاجتماعية بالتزامن مع هجمات الشبكة الأخرى.

تقنيات الهندسة الاجتماعية

- **Pretexting** - يتظاهر المهاجم بأنه بحاجة إلى بيانات شخصية من أجل تأكيد هوية المستلم.
- **Phishing** - يرسل المهاجم بريدًا إلكترونيًا احتياليًا متنكرًا على أنه من مصدر موثوق به.
- **Spear Phishing** -يقوم المهاجم بإنشاء هجوم تصيد مستهدف لفرد أو مؤسسة معينة.
- **Spam** -البريد الإلكتروني غير المرغوب فيه الذي يحتوي في كثير من الأحيان على روابط ضارة أو برامج ضارة أو محتوى خادع.
- **Something for Something** -عندما يطلب المهاجم معلومات شخصية مقابل شيء ما.
- **Baiting** - المهاجم يترك محرك أقراص فلاش المصابة البرمجيات الخبيثة في موقع عام.
- **Impersonation** - يتظاهر المهاجم بأنه شخص ليسوا عليه.
- **Tailgating** -يتبع المهاجم شخصًا مصرحًا له إلى منطقة آمنة.
- **Shoulder surfing** -مهاجم ينظر على كتف شخص ما لسرقة المعلومات.
- **Dumpster Diving** -يبحث المهاجم عن معلومات سرية من خلال المهملات.