الوحدة التدريبية الثامنة
أمن التطبيقات وضمان جودة التطبيق

رمز الوحدة
ADS-U8-CAVT

المتطلبات السابقة:

لا يوجد

نتاجات التعلم:

عند الانتهاء من دراسة هذه الوحدة واكتساب مهاراتها الأدائية والاتجاهات السلوكية الصحيحة والعلوم المهنية المرافقة من خلال التفاعل مع أنشطتها وخبراتها المختلفة ويصبح المتدرب قادرا على أداء نتاجات التعلم الأتية :

1- فهم أساسيات أمن المعلومات والتطبيقات وأهم التهديدات الأمنية لها .

2- تطبيق ممارسات حماية التطبيقات وأمنها من التهديدات والثغرات الأمنية.

3- فهم أساسيات التشفير وأنوع الخوارزميات المختلفة .

4- أكتساب المعرفة الكاملة بمفهوم النسخ الإحتياطي وأهميته .

الأنشطة التعليمية والتدريبية	مصادر التعلم
قراءة المعلومات النظرية	الوحدة التدريبية
البحث في المواقع الالكترونية التعليمية روابط التعليم الالكتروني	الشبكة العنكبوتية منصة الكلية التعليمية
تنفيذ التمارين العملية	المشغل / المختبر
التدريب الميداني	سوق العمل

روابط التعلم الإلكتروني

سيتم تزويد المتدربين بروابط التعلم الإلكتروني من خلال المدرب

- **أمن التطبيق وضمان جودته :**

من خلال مشاهدتك للصورة المجاورة :

- قم بتحليل الصورة وناقش أهميتها في العالم الرقمي اليوم، حيث تتزايد تهديدات الأمن السيبراني.
- شارك في مناقشة جماعية مع زملائك لتسليط الضوء على أهمية الوعي بالأمن السيبراني وأمن التطبيقات وضمان الجودة كما هو موضح في الصورة. وما هي التهديدات التي تتربص ببياناتنا وأنظمتنا؟

في عالم التطبيقات المتطور، يُعدّ ضمان أمان وجودة التطبيقات عنصرًا أساسيًا لنجاح أي مشروع برمجي. يتطلب ذلك من المطورين امتلاك مهارات وخبرات واسعة تشمل فهم المخاطر الأمنية، وتطبيق أفضل الممارسات البرمجية، واختبار التطبيقات بدقة، والتواصل الفعال مع العملاء. في هذه الوحدة، سنغوص في رحلة لفهم كيفية المساهمة في أمان التطبيق والتأكد من جودته، ونقدم الخطوات الأساسية التي يجب على المطورين اتباعها لضمان تقديم منتجات برمجية متميزة تلبي احتياجات العملاء وتُرضي توقعاتهم.

- **التهديدات الأمنية ونقاط الضعف :**

تتعرض أنظمتنا وبياناتنا لمخاطر متزايدة مع تطور التكنولوجيا. التهديدات الأمنية ونقاط الضعف تشكل تحديًا كبيرًا أمام أمن المعلومات. في هذه الوحدة، سنغوص في عالم التهديدات الأمنية لنفهم ماهيتها وكيف تتطور. سنتعرف على نقاط الضعف الشائعة في الأنظمة والبرامج وكيف يمكن للمهاجمين استغلالها .هدفنا الأساسي هو تمكينك من فهم هذه التهديدات ونقاط الضعف بشكل عميق .وذلك لأن هذا الفهم هو الخطوة الأولى لحماية أنظمتك وبياناتك من الاختراق. عند الانتهاء من هذه الوحدة، ستكون قادرًا على تحديد التهديدات المحتملة، وتقييم نقاط الضعف في نظامك، وبالتالي اتخاذ الإجراءات اللازمة لمنع الهجمات وحماية أصولك الرقمية.

- **التهديدات الأمنية Security Threats:**

أحداث أو أفعال يمكن أن تُلحق الضرر بنظام الحاسوب أو الشبكة أو البيانات.

- **نقاط الضعف Vulnerabilities:**

ثغرات في أنظمة الحاسوب أو الشبكات أو البرامج التي يمكن للمهاجمين استغلالها.

الشكل (1): صورة توضح بعض الثغرات السيبرانية التي يمكن أن تشكل تهديداً للأنظمة والتطبيقات

لماذا من المهم فهم التهديدات الأمنية ونقاط الضعف؟

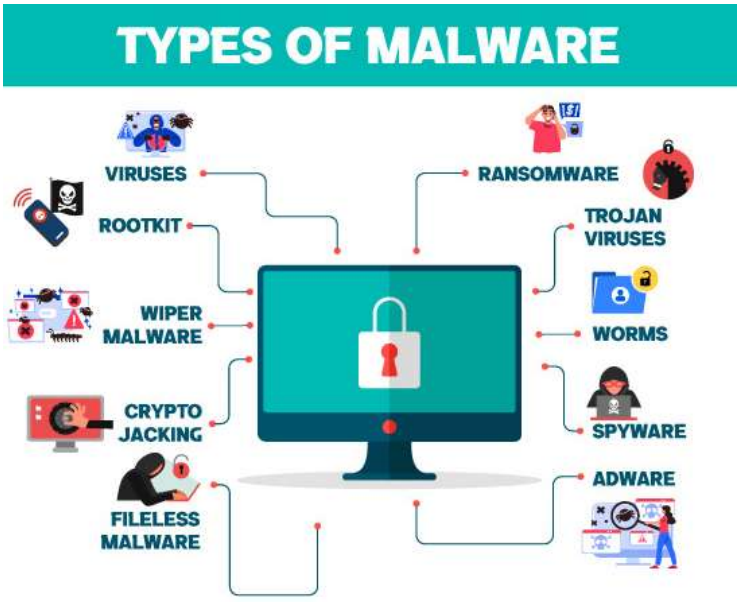
- لحماية أنظمة الحاسوب والشبكات والبيانات من الضرر.
- لمنع المهاجمين من سرقة البيانات أو تعطيل الخدمات أو إلحاق الضرر بالسمعة.
- لتحسين أمان التطبيقات والبرامج.

نشاط اثرائي 1: بالتنسيق مع المدرب :

تحدث عن أهمية فهم التهديدات الأمنية ونقاط الضعف من ناحية:

- حماية أنظمة الحاسوب والشبكات والبيانات من الضرر.
- منع المهاجمين من سرقة البيانات أو تعطيل الخدمات أو إلحاق الضرر بالسمعة.
- تحسين أمان التطبيقات والبرامج.

- **البرامج الضارة**: تُعدّ البرامج الضارة **Malware** من أخطر التهديدات التي تواجه مستخدمي أجهزة الحاسوب، حيث يمكنها إلحاق الضرر بالنظام والبيانات. تشمل الفيروسات، وبرامج التجسس، وبرامج الفدية، وغيرها من البرامج التي يمكن أن تُلحق الضرر بنظام الحاسوب. فيما يلي بعض أنواع البرامج الضارة الأكثر شيوعًا:



الشكل (2): صورة توضح بعض أنواع البرامج الضارة التي تشكل تهديد للأنظمة والتطبيقات

- **الفيروسات Viruses:** برامج ضارة قابلة للنسخ والتكاثر ذاتيًا، تُصيب أجهزة الحاسوب وتنتشر من خلال الملفات المُرفقة برسائل البريد الإلكتروني أو مواقع الويب المُصابة. تُلحق الضرر بالنظام والبيانات، مثل حذف الملفات أو تشفيرها، أو تعطيل وظائف النظام. بعض أنواع الفيروسات:
  - **فيروسات الملفات :** تكون هذه الفيروسات مُتخفية داخل الملفات، تنتشر من خلال إصابة الملفات القابلة للتنفيذ مثل ملفات.exe أو.doc. يكون سلاحها "التكاثر والانتشار" عند تشغيل الملف المُصاب، ينتشر الفيروس ويُصيب ملفات أخرى على الجهاز. أمثلة عليها Brain وMichelangelo.

الشكل (3): صورة توضح إصابة نظام بفيروس مايكل أنجلو

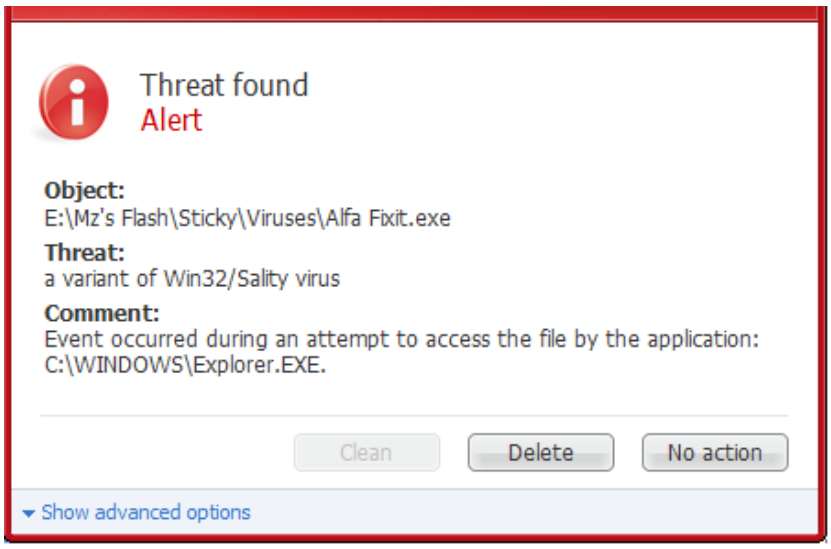
- **فيروسات التمهيد (Boot Sector Viruses)** : تُهاجم عند التشغيل وتُصيب هذه الفيروسات قطاع التمهيد على القرص الثابت، وتُنفذ نفسها عند بدء تشغيل الحاسوب. سلاحها "التحكم" تتحكم هذه الفيروسات في عملية التشغيل، مما قد يُعيق عمل البرامج أو يُلحق الضرر بالبيانات، أمثلتها: CIH وStoned Boot.

الشكل (4): صورة توضح إصابة نظام بفيروس قام بتعطيل النظام

- **فيروسات الماكرو**: تُختبئ في لغات البرمجة: تُصيب هذه الفيروسات لغات البرمجة مثل Visual Basic أو Excel، وتنتشر من خلال الماكرو. سلاحها "الأتمتة" تُنفذ هذه الفيروسات أوامر برمجية ضارة بشكل تلقائي، مما قد يُسبب أضرارًا للنظام أو البيانات. أمثلتها: فيروس Melissa وMacro.

الشكل (5): صورة تحذر من أمكانية إصابة النظام بفيروس مايكرو

- **فيروسات المُتصفحات**: تُهاجم عالم الإنترنت: تُصيب هذه الفيروسات مُتصفحات الويب مثل Internet Explorer أو Chrome، وتنتشر من خلال مواقع الويب المُصابة. سلاحها "التجسس والتحكم" قد تُسجل هذه الفيروسات كلمات المرور وبيانات بطاقات الائتمان، أو تُعيد توجيه المستخدم إلى مواقع ويب ضارة. أمثلتها: فيروس W32/Silly وJS. Trojan.Banker.



الشكل (6): صورة توضح إصابة المتصفح بفيروس تجسس

- **فيروسات المُشفرات**: تهديد لبياناتك: تُشفّر هذه الفيروسات بيانات المستخدم، وتطالبه بدفع فدية لاستعادتها. سلاحها " الابتزاز" تُهدد هذه الفيروسات بفقدان البيانات الدائمة إذا لم يتم دفع الفدية، مما يُسبب خسائر مالية كبيرة. أمثلتها: فيروس WannaCry وPetya.

الشكل (7): صورة توضح إصابة نظام وتعطل بسبب تشفير فايروس للبيانات

هذه أمثلة قليلة من أنواع الفيروسات التي تُهدد أمان أجهزة الحاسوب. مع تطور التكنولوجيا، تظهر تهديدات جديدة بشكل مستمر، مما يتطلب من المستخدمين اليقظة والحذر الدائم.

- **برامج التجسس Spyware**: تمثل تهديداً كبيراً لخصوصية المستخدمين، حيث تقوم هذه البرامج الخبيثة بالتسلل إلى أجهزة الحاسوب والهواتف الذكية، لتراقب أنشطة وسلوك المستخدمين وتهدد خصوصيتهم، وتمكّن المطورين من سرقة المعلومات الحساسة مثل كلمات المرور وبيانات بطاقات الائتمان، دون علم أو موافقة المستخدمين.

بعض أنواع برامج التجسس:

- **برامج التجسس التقليدية**: تُثبت يدويًا: يتم تثبيت هذه البرامج على جهاز الضحية يدويًا، غالبًا من خلال خداعه بفتح ملف مُرفق مُصاب برسالة بريد إلكتروني أو تنزيل تطبيق ضار. مُهامها: تُراقب هذه البرامج أنشطة الضحية مثل الضغطات على لوحة المفاتيح، ولقطات الشاشة، وسجلات الدردشة، ورسائل البريد الإلكتروني، والملفات، وكاميرا الهاتف. أمثلتها: SpyEye و The Rat.

الشكل (8): صورة توضح إصابة نظام بفيروس SpyEye

- **برامج التجسس المُتقدمة:** تُثبت عن بُعد: تُستغل هذه البرامج ثغرات الأمان في البرامج أو أنظمة التشغيل لتثبيت نفسها على جهاز الضحية دون علمه أو موافقته. مُهامها: تُنفذ نفس مُهام برامج التجسس التقليدية، بالإضافة إلى إمكانية التحكم عن بُعد بجهاز الضحية، وتشغيل الكاميرا والميكروفون، وسرقة كلمات المرور، والبيانات المالية. أمثلتها: FinFisher وPegasus.

الشكل (9): صورة توضح إصابة نظام بفيروس Pegasus

- **برامج التجسس المُتخصصة:** تُستهدف مجموعات مُحددة: تُصمم هذه البرامج لاستهداف مجموعات مُحددة من الأشخاص، مثل المعارضين السياسيين أو النشطاء أو رجال الأعمال. مُهامها: تُنفذ نفس مُهام برامج التجسس التقليدية، بالإضافة إلى إمكانية الوصول إلى معلومات حساسة مثل رسائل البريد الإلكتروني المشفرة ورسائل الدردشة المُشفرة. أمثلتها: DarkMatter و NSO Group.

الشكل (10): صورة توضح رسائل نصية مخادعة متضمنة رابط يحتوي فايروس

- **برامج التجسس المُتخفية**: تُخفي نفسها بذكاء: تُصمم هذه البرامج لإخفاء نفسها عن برامج مكافحة الفيروسات وأدوات الأمان، مما يجعل من الصعب اكتشافها وإزالتها. مُهامها: تُنفذ نفس مُهام برامج التجسس التقليدية، بالإضافة إلى إمكانية تعطيل برامج الأمان وإعادة تثبيت نفسها بعد إزالتها. أمثلتها: Agent.btz و Uroboros.

الشكل (11): صورة توضح إصابة نظام بفيروس Agent.btz للتجسس وتعطيل إعدادات الأمان

- **برامج التجسس المُحمولة**: تُصيب الأجهزة المحمولة: تُصمم هذه البرامج خصيصًا لاستهداف الأجهزة المحمولة مثل الهواتف الذكية والأجهزة اللوحية. مُهامها: تُنفذ نفس مُهام برامج التجسس التقليدية، بالإضافة إلى إمكانية الوصول إلى سجلات المكالمات والرسائل النصية وبيانات الموقع الجغرافي. أمثلتها: Trilogy Mobile Spy وFlexiSPY.

الشكل (12): صورة توضح إصابة نظام بفيروس Agent.btz للتجسس وتعطيل إعدادات الأمان

هذه أمثلة قليلة من أنواع برامج التجسس التي تُهدد خصوصية المستخدمين. مع تطور التكنولوجيا، تظهر تهديدات جديدة بشكل مستمر، مما يتطلب من المستخدمين اليقظة والحذر الدائم.

- **برامج الفدية Ransomware**: برامج تُشفّر بيانات المستخدم وتطالبه بدفع فدية لاستعادتها. تُسبب خسائر مالية كبيرة للمستخدمين، وتُعطل عمل الشركات والأفراد. بعض أنواع برامج الفدية:

- **برامج الفدية المُشفّرة**: يعتبر هذا النوع من أكثر الأنواع شيوعًا؛ تُشفّر هذه البرامج جميع البيانات على جهاز الضحية، مما يجعلها غير قابلة للاستخدام. تنتشر هذه البرامج من خلال رسائل البريد الإلكتروني المُرفقة بالملفات المُصابة، أو مواقع الويب المُخترقة، أو روابط التنزيل الضارة. أمثلتها: WannaCry وPetya وRyuk.

الشكل (13): صورة توضح إصابة نظام بنوع من فيروسات الفدية التي تشفر بيانات الضحية

- **برامج الفدية المُقيدة**: تُعيق الوصول إلى البيانات؛ لا تُشفّر هذه البرامج البيانات، لكنها تمنع الضحية من الوصول إليها. تنتشر هذه البرامج من خلال نفس طرق برامج الفدية المُشفّرة. أمثلتها: Locky وCryptoLocker وJigsaw.

الشكل (14): صورة توضح إصابة نظام بنوع من فيروسات الفدية التي تعيق وصول الضحية لبياناته

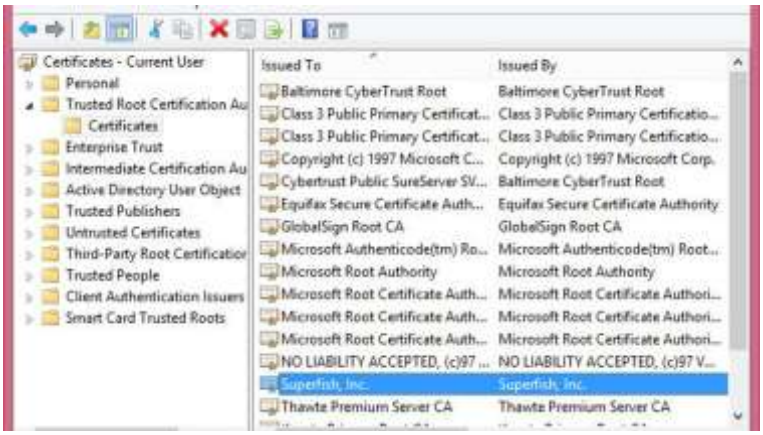
- **برامج الفدية المُزدوجة**: مزيج من التشفير والتقييد: تُشفّر هذه البرامج البيانات وتمنع الضحية من الوصول إليها في نفس الوقت. تنتشر هذه البرامج من خلال نفس طرق برامج الفدية المُشفّرة. أمثلتها: Dharma وMaze وSodinokibi.

الشكل (15): صورة توضح إصابة نظام بنوع من فيروسات الفدية التي تشفروتعيق وصول الضحية لبياناته

- **برامج الفدية المُستهدفة**: تُستهدف مجموعات مُحددة: تُصمم هذه البرامج لاستهداف مجموعات مُحددة من الأشخاص، مثل الشركات الكبيرة أو المؤسسات الحكومية. تنتشر هذه البرامج من خلال هجمات التصيد المُستهدف أو هجمات خرق أنظمة المعلومات. أمثلتها: SamSam وGandCrab وBitPaymer.
- **برامج الفدية المُتخصصة**: تُستهدف أنظمة التشغيل: تُصمم هذه البرامج لاستهداف أنظمة التشغيل المُحددة، مثل أنظمة التشغيل الصناعية أو أنظمة الرعاية الصحية. طرق انتشارها: تنتشر هذه البرامج من خلال هجمات خرق أنظمة المعلومات المُخصصة. أمثلتها: Chakrabortty وLockerGoga وRansack.

- **برامج الإعلانات المُتطفلة Adware:** تُعدّ برامج الإعلانات المُتطفلة من أكثر البرامج المُزعجة التي تُواجه مستخدمي أجهزة الحاسوب. هذه البرامج تُظهر إعلانات مُزعجة بشكل مُفرط على شاشة الحاسوب، وتُبطئ أداءه، مما يُسبب إزعاجًا للمستخدم ويُستهلك موارد النظام، وقد تُوجهه إلى مواقع ويب ضارة. فيما يلي بعض أنوع الإعلانات المُتطفلة:

- **برامج الإعلانات المُنثورة:** تُدمج هذه البرامج في البرامج المجانية أو المُقرصنة، وتُظهر إعلانات مُزعجة عند تشغيل البرنامج أو استخدامه. أمثلتها: Toolbar Babylon و Superfish.



الشكل (16): صورة توضح إصابة سجلات النظام بنوع من البرامج الضارة

- **برامج الإعلانات المُنفذة:** يتم تثبيت هذه البرامج على جهاز الضحية يدويًا، غالبًا من خلال خداع الضحية بفتح ملف مُرفق مُصاب برسالة بريد إلكتروني أو تنزيل تطبيق ضار. أمثلتها: Adware Agent و PopUpMonster.

الشكل (17): صورة توضح إصابة النظام بنوع من البرامج المزعجة التي تظهر بشكل مستمر ومزعج على شاشة الضحية

- **برامج الإعلانات المُتغيرة**: تُغير هذه البرامج إعدادات المتصفح لتُظهر إعلانات مُزعجة على جميع مواقع الويب التي يزورها الضحية. أمثلتها: MyWebSearch وSearchDefender.
- **برامج الإعلانات المُتتبعة**: تُراقب هذه البرامج سلوك المستخدم على الإنترنت وتُظهر إعلانات مُستهدفة بناءً على اهتماماته. أمثلتها: Weborama وDotomi.
- **برامج الإعلانات المُتلاعبة**: تُنزل هذه البرامج برامج ضارة أخرى على جهاز الضحية، مثل برامج التجسس أو برامج الفدية. أمثلتها: Zlob وWin32.Agent. Trojan.Downloader.

- **برامج الخداع Phishing**: تُعدّ برامج الخداع من أخطر التهديدات التي تواجه مستخدمي أجهزة الحاسوب. هذه البرامج تُظهر رسائل وهمية تُحاكي برامج شرعية مثل مواقع التواصل الاجتماعي، وتطالب المستخدم بدفع المال أو إدخال معلومات حساسة مثل كلمات المرور أو بيانات بطاقات الائتمان.

اثر ائي 2: بالتنسيق مع المدرب

ناقش أنواع برامج الخداع التي تُهدد أمننا.

:

الشكل (18): صورة تظهر شكل مو اقع التواصل الاجتماعي "فيسبوك" ولكن غير حقيقي

- **برامج مكافحة الفيروسات الوهمية**: تُعرض هذه البرامج رسائل وهمية تُحاكي برامج مكافحة الفيروسات الشرعية، وتزعم اكتشاف فيروسات على جهاز المستخدم. تُطالب هذه البرامج المستخدم بدفع المال لشراء برنامج مكافحة الفيروسات الوهمي لحل المشكلة المُختلقة. أمثلتها: Fake Antivirus Pro وSystemCare AntiVirus.

الشكل (19): صورة تظهر شكل نافذة برنامج مكافحة فيروسات، ولكن غير حقيقي

- **برامج دعم الحاسوب الوهمية**: تُعرض هذه البرامج رسائل وهمية تُحاكي برامج دعم الحاسوب الشرعية، وتزعم وجود مشكلات في جهاز المستخدم. تُطالب هذه البرامج المستخدم بدفع المال للحصول على دعم فني لحل المشكلة المُختلقة. أمثلتها: Tech Support Pro وPC Repair Tech.
- **برامج الرسائل الوهمية**: تُرسل هذه البرامج رسائل وهمية تُحاكي رسائل البريد الإلكتروني أو رسائل SMS من مؤسسات شرعية مثل البنوك أو شركات بطاقات الائتمان. تُطالب هذه البرامج المستخدم بإدخال معلومات حساسة مثل كلمات المرور أو بيانات بطاقات الائتمان. أمثلتها: Phishing emails from fake banks or credit card companies.
- **برامج المو اقع الإلكترونية الوهمية**: تُنشئ هذه البرامج مواقع ويب وهمية تُحاكي مواقع الويب الشرعية مثل مواقع البنوك أو المتاجر الإلكترونية. تُطالب هذه البرامج المستخدم بإدخال معلومات حساسة مثل كلمات المرور أو بيانات بطاقات الائتمان عند تسجيل الدخول إلى الموقع الوهمي. أمثلتها: Fake banking websites or online shopping websites.

- **برامج التطبيقات الوهمية**: تُنشئ هذه البرامج تطبيقات وهمية تُحاكي التطبيقات الشرعية الموجودة على متاجر التطبيقات. تُطالب هذه البرامج المستخدم بإدخال معلومات حساسة مثل كلمات المرور أو بيانات بطاقات الائتمان عند استخدام التطبيق الوهمي. أمثلتها: Fake banking apps or mobile shopping apps.

- **أنواع أخرى من البرامج الضارة**. لا تقتصر التهديدات على أنواع البرامج الضارة التي تم تناولها سابقًا. فهناك العديد من الأنواع الأخرى التي تُهدد أمن أجهزة الحاسوب والهواتف الذكية ونطاقات العمل الرقمي.

- **برامج ضارة تُستهدف أجهزة الهاتف المحمول**: تُصمم هذه البرامج خصيصًا لاستهداف أجهزة الهاتف الذكية التي تعمل بنظام Android أو iOS. تنتشر هذه البرامج من خلال تطبيقات ضارة تم تحميلها من متاجر التطبيقات غير الرسمية أو من خلال رسائل SMS أو البريد الإلكتروني المُحتوية على روابط ضارة. أمثلتها: Trilogy Mobile Spy وFlexiSPY وLocket.

الشكل (20): صورة تظهر رسالة نصية احتيالية تستهدف الهواتف الذكية

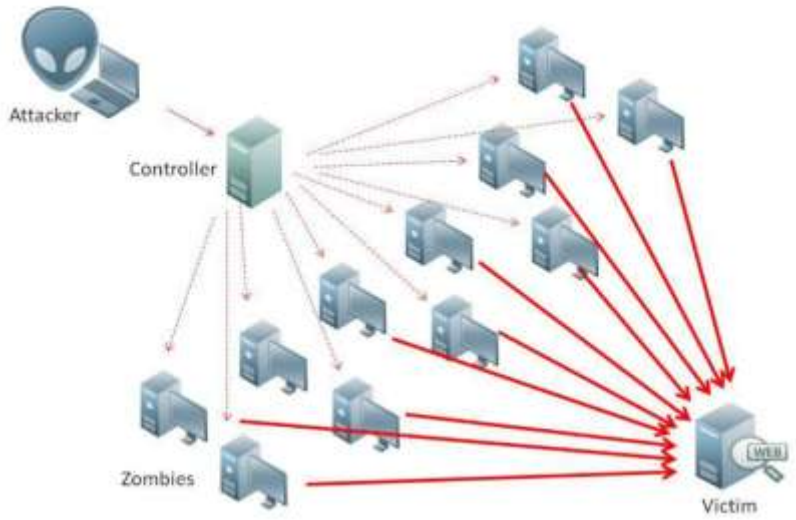
- **برامج تُستخدم لسرقة العملات الرقمية**: تُصمم هذه البرامج لاستهداف العملات الرقمية Digital Currencies مثل Bitcoin وEthereum. تُستغل هذه البرامج ثغرات الأمان في أجهزة الحاسوب أو تتسلل إلى أنظمة التعدين لاستخراج العملات الرقمية دون علم أو موافقة المستخدم. أمثلتها: Cryptojacking malware وMinergate و CoinHive.

- **برامج تُستخدم لإنشاء شبكات بوتنت**: تُصمم هذه البرامج لإنشاء شبكات بوتنت botnet networks، وهي مجموعات من أجهزة الحاسوب المُصابة التي يتم التحكم بها عن بُعد من قبل مُطور البرامج الضارة. تُستغل هذه البرامج ثغرات الأمان في أجهزة الحاسوب وتُثبت عليها برامج ضارة دون علم أو موافقة المستخدم. أمثلتها: Mirai وPbot و Conficker.

هذه أمثلة قليلة من أنواع أخرى من البرامج الضارة التي تُهدد أمن أجهزة الحاسوب والهواتف الذكية ونطاقات العمل الرقمي. مع تطور التكنولوجيا، تظهر تهديدات جديدة بشكل مستمر، مما يتطلب من المستخدمين اليقظة والحذر الدائم.

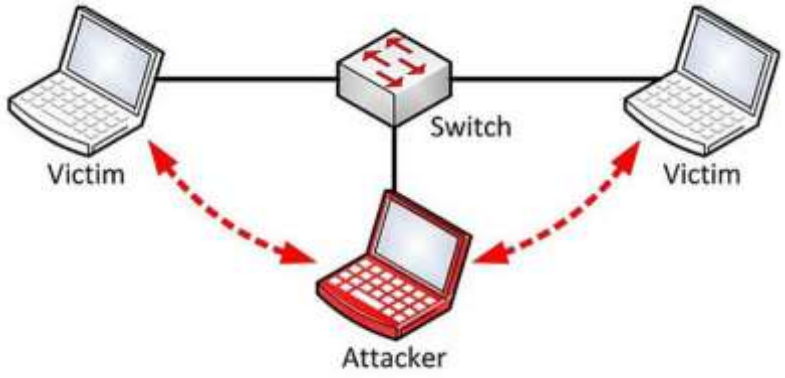
- **هجمات الشبكة Network Attacks:** تُعدّ هجمات الشبكة من أخطر التهديدات التي تواجه الشركات والأفراد. هذه الهجمات تُستهدف شبكات الحاسوب والأنظمة الإلكترونية بهدف تعطيل الخدمات أو سرقة البيانات أو إلحاق الضرر بالنظام. تشمل هجمات رفض الخدمة، واختراق الشبكة، وهجمات الرجل في المنتصف، وغيرها من الهجمات التي يمكن أن تُعطل الخدمات أو تسرق البيانات. دعونا بعض الأمثلة الشائعة:

- **هجمات رفض الخدمة (DoS):** هدفها إغراق خوادم الشبكة بطلبات زائفة، مما يُعيق عملها ويمنع المستخدمين الشرعيين من الوصول إلى الخدمات. أمثلتها: هجمات DDoS (Distributed Denial-of-Service) وSmurf attacks وPing floods.



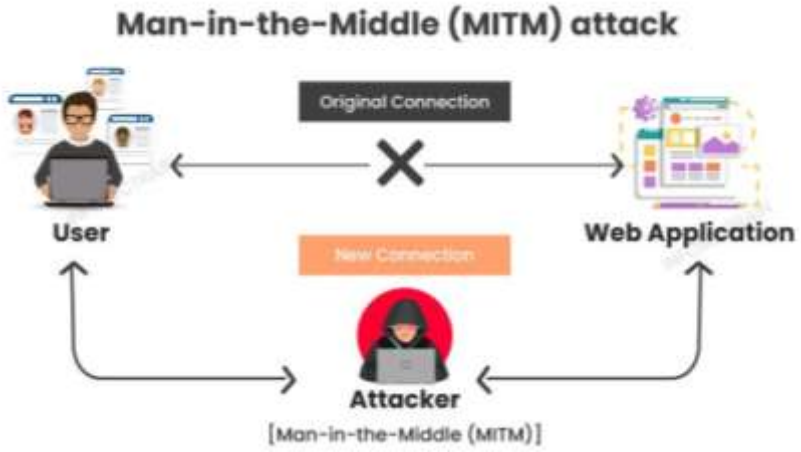
الشكل (21): صورة تظهر هجوم رفض الخدمة DDoS

- **هجمات اختراق الشبكة:** هدفها اختراق أنظمة الحاسوب والشبكات للوصول إلى البيانات الحساسة أو نشر برامج ضارة. استغلال ثغرات الأمان في البرامج أو أنظمة التشغيل، أو استخدام تقنيات الهندسة الاجتماعية لخداع المستخدمين. أمثلتها: هجمات SQL injection و Cross-site scripting (XSS) وRansomware attacks.



الشكل (22): صورة توضح اختراق الأنظمة من خلال ربط الموزع الداخلي للوصول إلى البيانات الحساسة

- **هجمات الرجل في المنتصف:** هدفها اعتراض الاتصالات بين جهازين على الشبكة، وسرقة البيانات أو تغييرها. استخدام نقاط Wi-Fi العامة غير الآمنة أو إعداد شبكات وهمية. أمثلتها: Man-in-the-browser attacks و Man-in-the-middle attacks (MitM).



الشكل (23): صورة توضح شكل هجمات الرجل في المنتصف

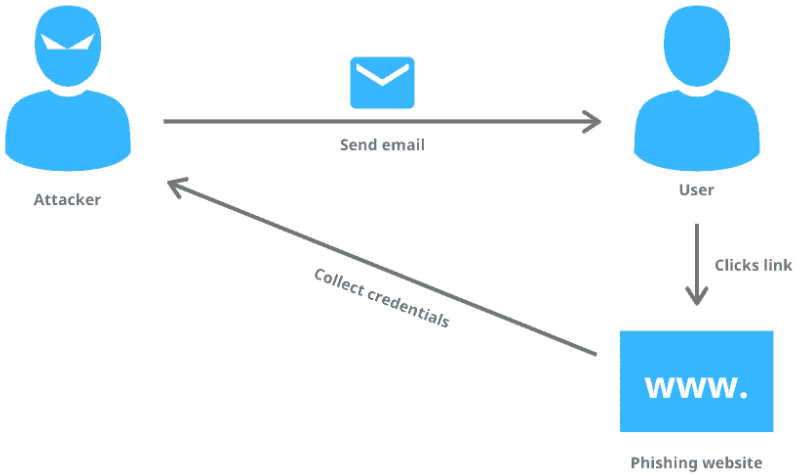
- **هجمات التجسس:** هدفها مراقبة أنشطة المستخدمين على الشبكة وسرقة البيانات الحساسة مثل كلمات المرور وبيانات بطاقات الائتمان. استخدام برامج التجسس أو تقنيات الهندسة الاجتماعية لخداع المستخدمين. أمثلتها: Keylogging attacks وSpyware attacks و Phishing attacks.

- **هجمات برامج الفدية:** هدفها تشفير البيانات على جهاز الضحية، وطالبه بدفع فدية لاستعادتها. إرسال بريد إلكتروني مُرفق بملف مُصاب أو استغلال ثغرات الأمان في البرامج أو أنظمة التشغيل. أمثلتها: WannaCry وPetya وRyuk.

- **هجمات الهندسة الاجتماعية Social Engineering Attacks:** تُعدّ هجمات الهندسة الاجتماعية من أخطر التهديدات التي تواجه الأفراد والشركات. هذه الهجمات تعتمد على خداع الضحية نفسياً لإقناعه بالكشف عن معلومات حساسة أو اتخاذ إجراءات غير آمنة. تشمل الاحتيال عبر البريد الإلكتروني، والتصيد الاحتيالي، وهجمات هندسة اجتماعية أخرى. أمثلة على هجمات الهندسة الاجتماعية:

- **الاحتيال عبر البريد الإلكتروني (Phishing):** هدفه إرسال رسائل بريد إلكتروني وهمية تُحاكي رسائل من مؤسسات شرعية مثل البنوك أو شركات بطاقات الائتمان، بهدف خداع الضحية للكشف عن معلومات حساسة مثل كلمات المرور أو بيانات بطاقات الائتمان.

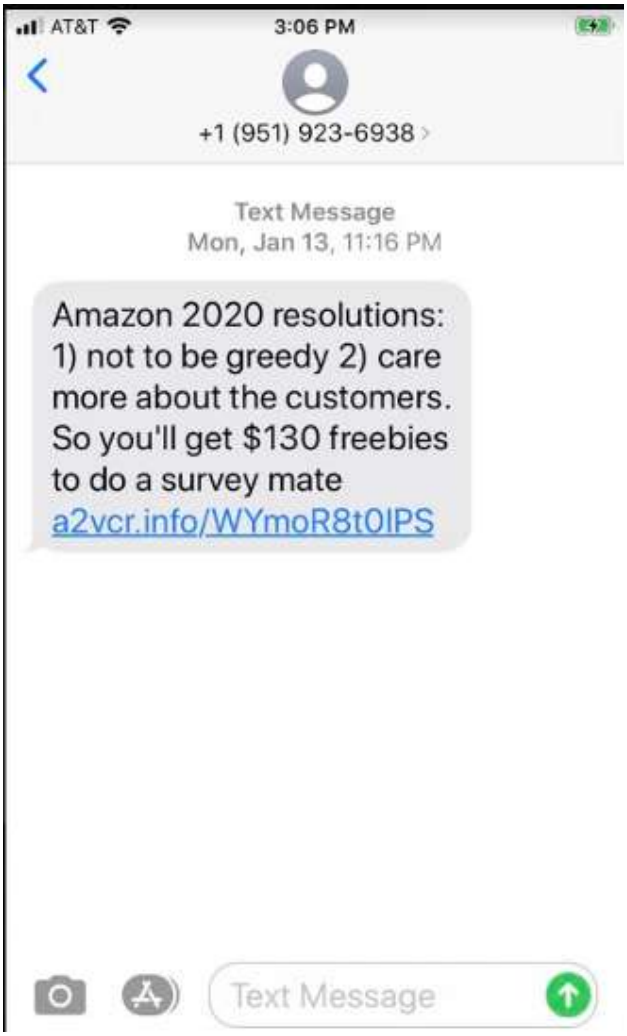
أمثله: رسائل بريد إلكتروني وهمية من بنوك مزيفة أو مواقع تسوق إلكترونية.



الشكل (24): صورة توضح طريقة الاحتيال عبر البريد الإلكتروني Phishing

- **التصيد الاحتيالي (Smishing):** هدفه إرسال رسائل SMS وهمية تُحاكي رسائل من مؤسسات شرعية مثل البنوك أو شركات الاتصالات، بهدف خداع الضحية للكشف عن معلومات حساسة مثل كلمات المرور أو بيانات بطاقات الائتمان.

أمثله: رسائل SMS وهمية من بنوك مزيفة أو شركات اتصالات.



الشكل (25): صورة توضح طريقة الاحتيال الاحتيالي Smishing

- **هجمات التحويل (Vishing):** هدفها استخدام مكالمات هاتفية وهمية تُحاكي مكالمات من مؤسسات شرعية مثل البنوك أو شركات الاتصالات، بهدف خداع الضحية للكشف عن معلومات حساسة مثل كلمات المرور أو بيانات بطاقات الائتمان.

أمثله: مكالمات هاتفية وهمية من بنوك مزيفة أو شركات اتصالات.

- **هجمات الابتزاز Extortion Attacks:** هدفها إرسال رسائل تهديد أو ابتزاز للضحية، بهدف إجباره على دفع مبالغ مالية أو الكشف عن معلومات حساسة. طرقها استخدام معلومات شخصية مسروقة أو تهديد بنشر معلومات محرجة. أمثلتها: هجمات Ransomware وDoxing attacks.

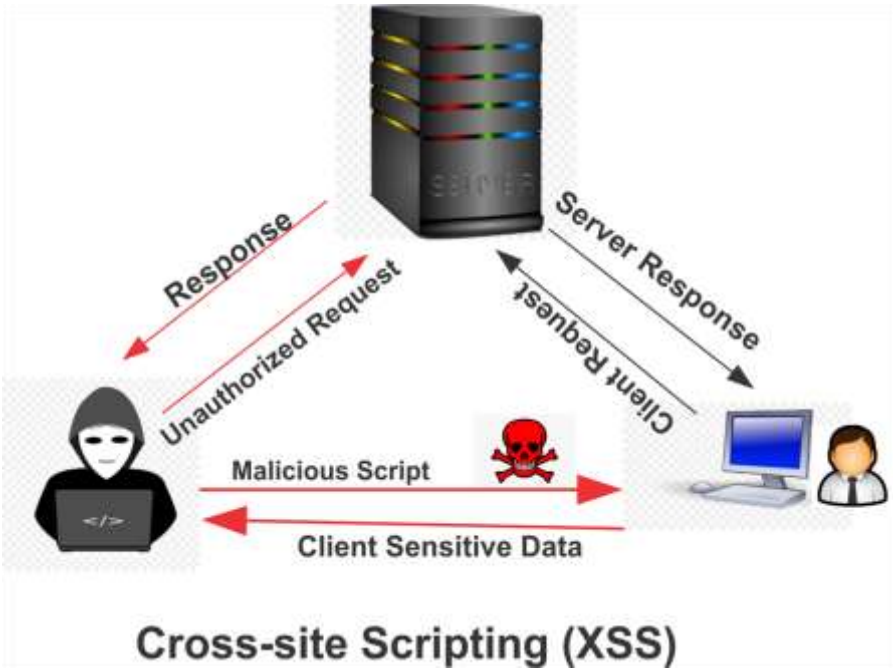
- **هجمات التحويل الاجتماعي Social Conversion Attacks**: هدفها خداع الضحية شخصيًا لبناء الثقة معه، ثم إقناعه بالكشف عن معلومات حساسة أو اتخاذ إجراءات غير آمنة. طرقها استخدام أساليب التملق أو التهديد أو التلاعب النفسي. أمثلتها: هجمات Tailgating وPretexting attacks.

- **الثغرات الأمنية في البرامج:** تُعدّ ثغرات البرامج الأمنية من أخطر التهديدات التي تواجه المستخدمين والشركات. هذه الثغرات هي عبارة عن أخطاء في البرمجة تُتيح للمهاجمين الوصول إلى بيانات حساسة أو السيطرة على النظام. تشمل الأخطاء في البرمجة التي يمكن للمهاجمين استغلالها للوصول إلى البيانات أو السيطرة على النظام. بعض الأمثلة على ثغرات البرامج الأمنية الشائعة:

- **ثغرات حقن التعليمات البرمجية (SQL Injection)**: مكان حدوثها قواعد البيانات. طريقة استغلالها يُدخل المهاجم تعليمات برمجية ضارة في استعلامات SQL، مما يُمكنه من سرقة البيانات أو تعديلها أو حذفها. أمثلتها: استغلال ثغرات حقن SQL في مواقع الويب أو التطبيقات.

الشكل (26): صورة توضح أسلوب فتح ثغرات عن طريق حقن التعليمات البرمجية

- **ثغرات البرامج النصية عبر المواقع (XSS)**: مكان حدوثها صفحات الويب. طريقة استغلالها يُدخل المهاجم تعليمات برمجية ضارة في مدخلات المستخدم، مما يُمكنه من سرقة معلومات حساسة مثل كلمات المرور أو بيانات بطاقات الائتمان. أمثلتها: استغلال ثغرات XSS في مواقع الويب أو التطبيقات عبر الإنترنت.



الشكل (27): صورة توضح أسلوب فتح ثغرات عن طريق البرامج النصية عبر المو اقع

- **ثغرات سرقة البيانات الحساسة:** مكان حدوثها البرامج والتطبيقات. يُستغل المهاجم ثغرة في البرنامج للوصول إلى بيانات حساسة مثل كلمات المرور أو بيانات بطاقات الائتمان. أمثلتها: استغلال ثغرات سرقة البيانات الحساسة في البرامج المصرفية أو برامج إدارة كلمات المرور.
- **ثغرات التصعيد (Privilege Escalation):** مكان حدوثها أنظمة التشغيل والبرامج. يُستغل المهاجم ثغرة في النظام للوصول إلى مستوى أعلى من الأذونات، مما يُمكنه من التحكم في النظام أو سرقة البيانات. أمثلتها: استغلال ثغرات التصعيد في أنظمة التشغيل Windows أو Linux.
- **ثغرات التنفيذ عن بعد (RCE):** مكان حدوثها داخل البرامج والتطبيقات. يُرسل المهاجم تعليمات برمجية ضارة إلى البرنامج، مما يُمكنه من تشغيلها على جهاز الضحية. أمثلتها: استغلال ثغرات RCE في برامج Adobe Flash Player أو Microsoft Office.

هذه أمثلة قليلة من ثغرات البرامج الأمنية التي تُهدد أمان المستخدمين والشركات. مع تطور التكنولوجيا، تظهر ثغرات جديدة بشكل مستمر، مما يتطلب من المستخدمين والشركات اليقظة والحذر الدائم. إنّ فهم أنواع ثغرات البرامج الأمنية وأضرارها أمر ضروري لحماية أمانك الشخصي وأمان شركتك. باتباع الإرشادات المذكورة أعلاه، يمكنك تقليل مخاطر التعرض لهذه الثغرات والحفاظ على سلامة بياناتك.

- **معايير الأمان و أفضل الممارسات المتبعة لتحقيق أمن التطبيقات :**

- **استخدام كلمات مرور قوية وفريدة من نوعها.**

مواصفات كلمات المرور القوية؟

الشكل (28): صورة تظهر الفرق بين كلمة المرور الضعيفة والقوية

- **طويلة**: تتكون من 12 حرفًا على الأقل.
- **معقدة**: تتضمن مزيجًا من الأحرف الكبيرة، والصغيرة، والأرقام، والرموز.
- **لا يمكن تخمينها بسهولة**: لا تتضمن معلومات شخصية مثل اسمك أو تاريخ ميلادك أو عنوانك.
- **فريدة من نوعها**: لا تستخدم نفس كلمة المرور لأكثر من حساب واحد.

- **تثبيت تحديثات الأمان بانتظام**. تُعدّ التحديثات الأمنية ضرورية لحماية أجهزتنا وبياناتنا من التهديدات الإلكترونية المتطورة. تُصدر الشركات المصنعة للبرامج وتطبيقات أنظمة التشغيل تحديثات أمان بانتظام لإصلاح الثغرات الأمنية التي قد يستغلها المتسللون للوصول إلى أجهزتنا أو سرقة بياناتنا.

لماذا من المهم تثبيت تحديثات الأمان بانتظام؟

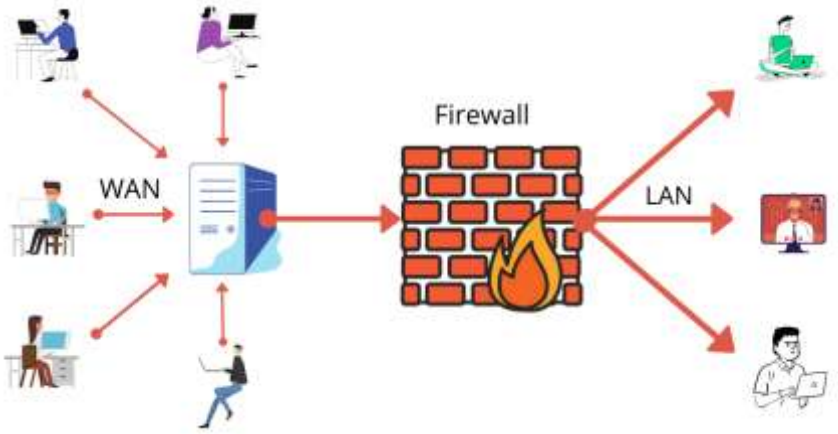
- **لإصلاح الثغرات الأمنية:** تُصدر الشركات المصنعة تحديثات أمان لإصلاح الثغرات الأمنية في البرامج وتطبيقات أنظمة التشغيل. قد يستغل المتسللون هذه الثغرات للوصول إلى أجهزتنا أو سرقة بياناتنا.
- **لحماية أنفسنا من البرامج الضارة:** تُصدر الشركات المصنعة تحديثات أمان لحماية أجهزتنا من البرامج الضارة الجديدة. قد تُلحق البرامج الضارة الضرر بجهازنا أو تسرق بياناتنا.
- **لحماية خصوصيتنا:** تُصدر الشركات المصنعة تحديثات أمان لحماية خصوصيتنا من خلال إصلاح الثغرات الأمنية التي قد تسمح للمتسللين بالوصول إلى بياناتنا الشخصية.

- **تعليمات لتثبيت تحديثات الأمان بانتظام:**

- **قم بتمكين التحديث التلقائي:** يُمكنك تمكين التحديث التلقائي على جهازك، بحيث يتم تثبيت التحديثات الأمنية تلقائيًا فور إصدارها.
- **تحقق من وجود تحديثات يدويًا:** إذا لم تكن قد قمت بتمكين التحديث التلقائي، فتأكد من التحقق من وجود تحديثات يدويًا بشكل منتظم.
- **قم بتثبيت التحديثات فور إصدارها:** لا تُؤجل تثبيت تحديثات الأمان، فكلما أسرعت في تثبيتها، زادت حماية جهازك من التهديدات الإلكترونية.
- **استخدم برامج مكافحة الفيروسات وبرامج مكافحة البرامج الضارة:** تُساعدك برامج مكافحة الفيروسات وبرامج مكافحة البرامج الضارة في حماية جهازك من البرامج الضارة الجديدة.
- **كن على دراية بعمليات الاحتيال عبر الإنترنت:** توخّ الحذر من رسائل البريد الإلكتروني أو المكالمات الهاتفية المشبوهة التي تطلب منك تثبيت تحديثات الأمان. تأكد من التحقق من صحة المصدر قبل تثبيت أي تحديثات.

- **استخدام جدارناري وبرامج مكافحة الفيروسات.** تُعدّ جدران الحماية وبرامج مكافحة الفيروسات أدوات ضرورية في عالم التهديدات الرقمية لحماية أجهزتنا وبياناتنا من التهديدات الإلكترونية المتطورة. تعمل هذه الأدوات كمُرشّحات لتحديد ووقف البرامج الضارة والتهديدات الأخرى قبل أن تُلحق الضرر بأجهزتنا.

- **ما هو جدار النار Firewall؟**



الشكل (29): صورة تظهر استخدام أنظمة الجدار الناري لحماية وفصل المستخدمين الداخليين عن المستخدمين الاخرين

- **هو بمثابة درع واقٍ:** حيث يعمل جدار النار كدرع واقٍ بين جهازك والإنترنت، ويُراقب جميع الاتصالات الواردة والصادرة.
- **يمنع البرامج الضارة:** يُمكن لجدار النار منع البرامج الضارة من الوصول إلى جهازك عن طريق حظر الاتصالات الضارة.
- **يُحمي معلوماتك الشخصية:** يُمكن لجدار النار حماية معلوماتك الشخصية من السرقة عن طريق حظر المتسللين من الوصول إلى جهازك.

ما هو برنامج مكافحة الفيروسات؟

- **يُكافح البرامج الضارة:** يُساعد برنامج مكافحة الفيروسات في مكافحة البرامج الضارة الموجودة على جهازك بالفعل.
- **يُكشف عن التهديدات:** يُمكن لبرنامج مكافحة الفيروسات فحص جهازك بحثًا عن التهديدات المعروفة، مثل الفيروسات وبرامج التجسس وبرامج الفدية.

- **يُحمي جهازك في الوقت الفعلي**: يُمكن لبرنامج مكافحة الفيروسات حماية جهازك في الوقت الفعلي من التهديدات الجديدة.

- **إرشادات لاستخدام جدار ناري وبرامج مكافحة الفيروسات:**

- **استخدم جدار ناري وبرامج مكافحة الفيروسات من شركات موثوقة**: تأكد من استخدام جدار ناري وبرامج مكافحة الفيروسات من شركات موثوقة ذات سمعة طيبة.
- **تأكد من تحديث جدار ناري وبرامج مكافحة الفيروسات بشكل منتظم**: تُصدر الشركات المصنعة تحديثات بانتظام لمنتجاتها لضمان حمايتها من أحدث التهديدات.
- **قم بإجراء فحص منتظم لجهازك باستخدام برنامج مكافحة الفيروسات**: قم بإجراء فحص منتظم لجهازك باستخدام برنامج مكافحة الفيروسات للكشف عن أي تهديدات موجودة.
- **احرص على تمكين الحماية في الوقت الفعلي**: تأكد من تمكين الحماية في الوقت الفعلي في برنامج مكافحة الفيروسات لحماية جهازك من التهديدات الجديدة.
- **كن على دراية بعمليات الاحتيال عبر الإنترنت**: توخّ الحذر من رسائل البريد الإلكتروني أو المكالمات الهاتفية المشبوهة التي تطلب منك تنزيل أو تثبيت جدار ناري أو برنامج مكافحة الفيروسات. تأكد من التحقق من صحة المصدر قبل تنزيل أو تثبيت أي برامج.
- **كن حذرًا بشأن ما تنقر عليه وتنزيله.** يُعدّ الحذر بشأن ما تنقر عليه وتنزيله أمرًا ضروريًا لحماية نفسك من المخاطر عبر الإنترنت. قد تحتوي الروابط والملفات المرفقة في رسائل البريد الإلكتروني أو مواقع الويب على برامج ضارة أو فيروسات يمكن أن تُلحق الضرر بجهازك أو تسرق بياناتك.

- **توجيهات للمواظبة لكي تكون آمنًا على الإنترنت:**

- **توخّ الحذر عند فتح رسائل البريد الإلكتروني:** لا تفتح رسائل البريد الإلكتروني من مرسلين غير معروفين، ولا تنقر على الروابط أو المرفقات المشبوهة.
- **كن حذرًا عند تصفح الإنترنت:** تجنب زيارة المواقع الإلكترونية المشبوهة أو غير الموثوقة.
- **تحقق من الروابط قبل النقر عليها:** قم بوضع الماوس على الرابط قبل النقر عليه للتأكد من وجهة الرابط الفعلية.
- **قم بتنزيل البرامج والتطبيقات من مواقع موثوقة:** تأكد من تنزيل البرامج والتطبيقات من مواقع الويب الرسمية للشركات المصنعة.
- **استخدم برامج مكافحة الفيروسات وبرامج مكافحة البرامج الضارة:** تُساعدك برامج مكافحة الفيروسات وبرامج مكافحة البرامج الضارة في حماية جهازك من البرامج الضارة والفيروسات.
- **كن على دراية بعمليات الاحتيال عبر الإنترنت:** توخّ الحذر من رسائل البريد الإلكتروني أو المكالمات الهاتفية المشبوهة التي تطلب منك إدخال معلومات حساسة أو تنزيل برامج.
- **لا تشارك معلومات حساسة مع أي شخص لا تعرفه.** تُعدّ خصوصيتنا أمرًا بالغ الأهمية. يجب علينا توخي الحذر بشأن المعلومات التي نشاركها مع الآخرين، خاصةً مع الأشخاص الذين لا نعرفهم.

ما هي المعلومات الحساسة؟

- **معلومات شخصية:** مثل اسمك وعنوانك ورقم هاتفك وتاريخ ميلادك.
- **معلومات مالية:** مثل رقم بطاقتك الائتمانية أو معلومات حسابك المصرفي.
- **كلمات المرور:** كلمات المرور الخاصة بحساباتك عبر الإنترنت، مثل بريدك الإلكتروني وشبكات التواصل الاجتماعي.
- **صور شخصية:** أية صور أو مقاطع فيديو شخصية لك.

- **لماذا من المهم عدم مشاركة المعلومات الحساسة مع أشخاص لا تعرفهم؟**
  - **لمنع سرقة الهوية:** يمكن للمجرمين استخدام معلوماتك الشخصية لسرقة هويتك وفتح حسابات باسمك أو ارتكاب جرائم أخرى.
  - **لمنع الاحتيال:** يمكن للمجرمين استخدام معلوماتك المالية للاحتيال عليك أو سرقة أموالك.
  - **لمنع الابتزاز:** يمكن للمجرمين استخدام معلوماتك الشخصية أو صورك لابتزازك.
- **تعليمات لحماية معلوماتك الحساسة:**
  - **لا تشارك معلوماتك الحساسة مع أي شخص لا تعرفه:** لا تشارك معلوماتك الشخصية أو معلوماتك المالية أو كلمات المرور الخاصة بك مع أي شخص لا تعرفه أو لا تثق به.
  - **كن حذرًا بشأن ما تنشره عبر الإنترنت:** تجنب مشاركة معلوماتك الشخصية أو صورك الشخصية على مواقع التواصل الاجتماعي أو المنتديات العامة.
  - **استخدم كلمات مرورقوية وفريدة من نوعها:** استخدم كلمات مرور قوية وفريدة من نوعها لحساباتك عبر الإنترنت، ولا تشاركها مع أي شخص.
  - **تأكد من حماية أجهزتك بكلمة مرور:** تأكد من حماية أجهزتك بكلمة مرور قوية لمنع الوصول غير المصرح به.
  - **كن على دراية بعمليات الاحتيال عبر الإنترنت:** توخّ الحذر من رسائل البريد الإلكتروني أو المكالمات الهاتفية المشبوهة التي تطلب منك إدخال معلومات حساسة.
  - **استخدم التشفيرلحماية البيانات الحساسة.** باتت البيانات الحساسة أكثر عرضة للسرقة والوصول غير المصرح به. من هنا، تأتي أهمية التشفير كأداة أساسية لحماية هذه البيانات وضمان أمانها.

نشاط اثرائي 3: بالتنسيق مع المدرب

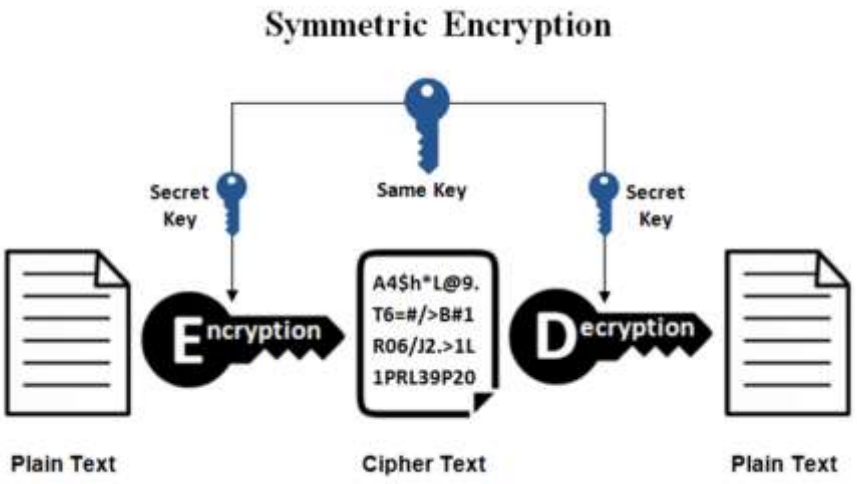
إشرح لماذا يعتبر "الحذر" مفتاح الأمان في العالم الرقمي .

- **التشفير (Encryption) :**

التشفير : هو عملية تحويل البيانات إلى شكل غير قابل للقراءة إلا باستخدام مفتاح فك التشفير الصحيح.

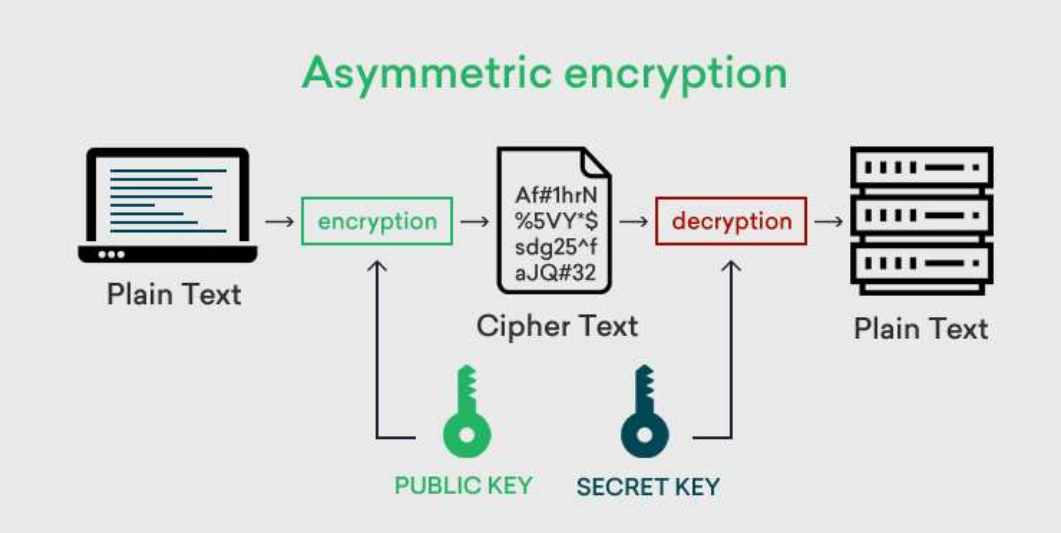
كيف يعمل التشفير؟

- **خوارزميات التشفير:** تُستخدم خوارزميات معقدة لتحويل البيانات إلى رموز لا يمكن فهمها بدون مفتاح فك التشفير.
- **مفاتيح التشفير:** تُستخدم مفاتيح التشفير لفك رموز البيانات المُشفّرة وتحويلها إلى شكلها الأصلي.
- **أنواع خوارزميات التشفير:**
  - **التشفير المتماثل:** يستخدم مفتاحًا واحدًا لكل من التشفير وفك التشفير.



الشكل (30): صورة تظهر نمط التشفير المتماثل

- **التشفير غير المتماثل Asymmetric Encryption:** يستخدم مفتاحين: مفتاحًا عامًا للتشفير ومفتاحًا خاصًا لفك التشفير.



الشكل (31): صورة تظهر نمط التشفير غير المتماثل

- **فوائد استخدام التشفير:**
  - **حماية البيانات الحساسة:** يُساعد التشفير على حماية البيانات الحساسة من السرقة أو الوصول غير المصرح به، حتى لو تم اختراق جهاز الحاسوب أو فقدان البيانات.
  - **ضمان الخصوصية:** يُحافظ التشفير على خصوصية بياناتك، ويمنع الآخرين من قراءتها دون موافقتك.
  - **الامتثال للقوانين واللوائح:** تُلزم العديد من القوانين واللوائح الشركات بحماية البيانات الحساسة للعملاء، والتشفير هو أحد أكثر الأدوات فعالية لتحقيق ذلك.
- **أمثلة على استخدامات التشفير:**
  - **حماية البيانات على أجهزة الحاسوب:** يمكن استخدام التشفير لحماية البيانات الموجودة على أجهزة الحاسوب المحمولة وأجهزة الحاسوب المكتبية من السرقة في حال فقدانها أو سرقتها.
  - **تأمين البيانات المُرسلة عبر الإنترنت:** يُستخدم التشفير لتأمين البيانات المُرسلة عبر الإنترنت، مثل كلمات المرور ومعلومات بطاقات الائتمان، ومنع المتسللين من اعتراضها.

- **حماية البيانات في التخزين السحابي**: يُستخدم التشفير لحماية البيانات المُخزّنة في التخزين السحابي، مثل Dropbox وGoogle Drive، من الوصول غير المصرح به.

- **تعليمات لإستخدام التشفير بفعالية:**

  - **استخدم برامج تشفير قوية:** تأكد من استخدام برامج تشفير موثوقة من شركات معروفة.
  - **احتفظ بمفاتيح التشفير الخاصة بك آمنة:** لا تشارك مفاتيح التشفير الخاصة بك مع أي شخص، واحرص على تخزينها في مكان آمن.
  - **تحديث برامج التشفير بانتظام:** تأكد من تحديث برامج التشفير الخاصة بك بانتظام للحصول على أحدث الحماية من التهديدات الأمنية.
  - **قم بإنشاء نسخ احتياطية من بياناتك بانتظام.** تُعدّ بياناتنا ثروة ثمينة. فقدانها قد يُسبب خسائر مادية ومعنوية كبيرة. لذلك، إنشاء نسخ احتياطية من بياناتك بانتظام هو أمر ضروري لحماية هذه البيانات وضمان استعادتها في حال حدوث أيّ خلل أو فقدان.

- **النسخ الاحتياطي**

هو عبارة عن عمل نسخة من بياناتك يتم تخزينها في مكان منفصل عن موقعها الأصلي. وتستخدم النسخ الاحتياطية لإستعادة البيانات في حال حدوث تلف في محرك الأقراص الثابتة، أو فقدان جهاز الحاسوب، أو سرقة البيانات، أو حدوث أيّ كارثة أخرى.

الشكل (32): شكل النسخ الاحتياطي من الأجهزة المختلفة الى وسائط التخزين من السيرفرات ومركز البيانات والتخزين السحابي

لماذا من المهم إنشاء نسخ احتياطية من بياناتك؟

- **لحماية بياناتك من الفقدان:** يُمكن أن تُفقد بياناتك لأسباب مختلفة، مثل تلف محرك الأقراص الثابتة أو سرقة جهاز الحاسوب أو حدوث هجمات إلكترونية. إنشاء نسخ احتياطية يُتيح لك استعادة بياناتك في حال حدوث أيّ من هذه الحوادث.
- **للاسترداد السريع:** في حال حدوث فقدان للبيانات، تُتيح لك النسخ الاحتياطية استعادة بياناتك بسرعة وسهولة دون الحاجة إلى بذل الكثير من الجهد أو تكبد تكاليف باهظة.
- **لتحقيق الأمان:** مع وجود نسخ احتياطية من بياناتك، ستتمتع براحة البال مع العلم أنه يمكنك استعادة بياناتك في حالة وقوع أي حادث.

- **أنواع النسخ الاحتياطي:**
  - **النسخ الاحتياطية الكاملة:** تشمل النسخة الاحتياطية الكاملة جميع بياناتك في وقت محدد.
  - **النسخ الاحتياطية التزايدية:** تشمل النسخة الاحتياطية التزايدية فقط الملفات التي تم تغييرها أو إضافتها منذ آخر نسخة احتياطية كاملة.
  - **النسخ الاحتياطية التفاضلية:** تشمل النسخة الاحتياطية التفاضلية فقط الملفات التي تم تغييرها منذ آخر نسخة احتياطية، سواء كانت جديدة أو مُعدّلة.
- **طرق إنشاء نسخ احتياطية:**
  - **على محركات الأقراص الثابتة الخارجية:** تُعدّ محركات الأقراص الثابتة الخارجية خيارًا شائعًا لإنشاء نسخ احتياطية من البيانات، فهي سهلة الاستخدام وميسورة التكلفة.
  - **على خدمات التخزين السحابي:** توفر خدمات التخزين السحابي، مثل Dropbox و Google Drive، مساحة تخزين عبر الإنترنت لإنشاء نسخ احتياطية من بياناتك.
  - **على برامج النسخ الاحتياطي:** تتوفر العديد من برامج النسخ الاحتياطي التي تُسهل عملية إنشاء النسخ الاحتياطية وإدارتها.
- **تعليمات لإنشاء نسخ احتياطية فعّالة:**
  - **حدد نوع النسخة الاحتياطية المناسبة لك:** اختر نوع النسخة الاحتياطية التي تناسب احتياجاتك وتفضيلاتك.
  - **حدد جدولًا زمنيًا للنسخ الاحتياطية:** حدد جدولًا زمنيًا منتظمًا لإنشاء نسخ احتياطية من بياناتك، مثل يوميًا أو أسبوعيًا أو شهريًا.
  - **اختبر نسخك الاحتياطية بانتظام:** تأكد من اختبار نسخك الاحتياطية بانتظام للتأكد من إمكانية استعادة بياناتك بنجاح.
  - **احتفظ بنسخك الاحتياطية في مكان آمن:** احرص على تخزين نسخك الاحتياطية في مكان آمن بعيدًا عن موقع جهاز الحاسوب، مثل محرك أقراص خارجي أو خدمة تخزين سحابي.

- **كن على دراية بأحدث التهديدات الأمنية.** التهديدات الأمنية متطورة بشكلٍ مُستمرّ، ممّا يُشكل خطرًا على بياناتنا وأجهزتنا.

- **فوائد معرفة التهديدات الأمنية :**

  - **لحماية بياناتك:** معرفة التهديدات الأمنية الحديثة يُساعدك على اتخاذ خطوات لمنعها من الوصول إلى بياناتك.
  - **لحماية أجهزتك:** معرفة التهديدات الأمنية الحديثة يُساعدك على حماية أجهزتك من البرامج الضارة والفيروسات والهجمات الأخرى.
  - **لحماية خصوصيتك:** معرفة التهديدات الأمنية الحديثة يُساعدك على حماية خصوصيتك من خلال تجنب الوقوع ضحية لعمليات الاحتيال والهجمات الإلكترونية.

نشاط اثرائي 4: بالتنسيق مع المدرب

أشرح لماذا من المهم أن تكون على دراية بأحدث التهديدات الأمنية؟

- **توجيهات للبقاء على دراية بأحدث التهديدات الأمنية :**

- **تابع أخبار الأمن الإلكتروني:** اقرأ المواقع الإلكترونية ومقالات المدونات التي تُغطي أخبار الأمن الإلكتروني.
- **اشترك في تنبيهات الأمن:** اشترك في تنبيهات من الشركات والمواقع الإلكترونية التي تستخدمها لتُعلمك بأيّ خروقات أمنية قد تحدث.
- **حافظ على تحديث برامجك:** تأكد من تحديث برامجك وتطبيقاتك ونظام التشغيل الخاص بك بانتظام لسد أية ثغرات أمنية قد يتم اكتشافها.
- **استخدم برامج مكافحة الفيروسات وبرامج مكافحة البرامج الضارة:** استخدم برامج مكافحة الفيروسات وبرامج مكافحة البرامج الضارة لحماية جهازك من البرامج الضارة والفيروسات.
- **كن حذرًا بشأن ما تنقر عليه وتنزيله:** كن حذرًا بشأن ما تنقر عليه وتنزيله من الإنترنت، وتجنب فتح المرفقات أو النقر على الروابط المشبوهة في رسائل البريد الإلكتروني.
- **كن قويًا في استخدام كلمات المرور:** استخدم كلمات مرور قوية وفريدة من نوعها لحساباتك عبر الإنترنت، ولا تشاركها مع أي شخص.
- **كن على دراية بعمليات الاحتيال عبر الإنترنت:** توخّ الحذر من رسائل البريد الإلكتروني أو المكالمات الهاتفية المشبوهة التي تطلب منك إدخال معلومات حساسة.

يمكنك البقاء على دراية بأحدث التهديدات الأمنية وحماية نفسك من المخاطر عبر الإنترنت. تذكر أنّ اليقظة هي مفتاح الأمان في عالم رقمي مُتغير.

- **فوائد المشاركة في البرامج التدريبية الخاصة بأمن البيانات والمعلومات :**
  - تساعد على رفع مستوى الوعي الأمني للأفراد والمنظمات.
  - تساعد الناس كيفية التعرف على التهديدات الأمنية وتجنبها.
  - تحسن قدرة المنظمات على حماية بياناتها وأنظمتها.

نشاط اثرائي 5: بالتنسيق مع المدرب

شاركنا تجاربك في التعامل مع التهديدات الأمنية!

الشكل (33): صورة تظهر أهمية رفع مستوى الوعي الأمني من خلال التدريب

- **تطوير وتنفيذ الضوابط الأمنية :**
  - الضوابط الأمنية هي تدابير يتم اتخاذها للحد من مخاطر التهديدات الأمنية.
  - تشمل أمثلة الضوابط الأمنية جدران الحماية، وبرامج مكافحة الفيروسات، والتحكم في الوصول، والتشفير.
  - من المهم تطوير وتنفيذ ضوابط أمان تتناسب مع احتياجات الأعمال الخاصة بك.

ملخص : إن فهم التهديدات الأمنية ونقاط الضعف ضروري لحماية أنظمة الحاسوب والشبكات والبيانات .يمكنك اتخاذ خطوات لتقليل مخاطر التهديدات الأمنية من خلال اتباع أفضل ممارسات الأمان والمشاركة في برامج التدريب وتطوير وتنفيذ الضوابط الأمنية ومن أهم تلك الممارسات :

- **حدد احتياجاتك**: ما هي البيانات التي تحتاج إلى حماية؟ ما هي المخاطر التي تواجهها؟
- **اختر الضوابط المناسبة**: جدران ناري، وبرامج مكافحة الفيروسات، والتحكم في الوصول، والتشفير، وغيرها.
- **نفّذ بذكاء**: تأكد من تنفيذ الضوابط بشكل صحيح وفعال.
- **راقب وحافظ**: راقب الضوابط بانتظام وقم بتحديثها عند الحاجة.