مبادئ عامة في السلامة الرقمية

الشريحة المُستهدَفة:
ذوو الاحتياجات الخاصة
المكفوفون

المبادرة الوطنية للسلامة الرقمية

حقوق الملكية الفكرية

المادة مملوكة للوكالة الوطنية للأمن السيبراني في دولة قطر، وكافَّة حقوق الملكية الفكرية التي تشمل حقّ المُؤلّف وحقوق التأليف والنشر والطباعة، كُلّها مكفولة للوكالة الوطنية للأمن السيبراني في دولة قطر.

وعليه فجميع الحقوق محفوظة للوكالة، ولا يجوز إعادة نشر أيّ أجزاء من هذا الكُتَيّب، أو الاقتباس منه، أو نَسْخ أي جزء منه، أو نقله كليًّا أو جزئيًّا في أي شكلٍ وبأي وسيلة، سواء بطُرق إلكترونية أو آلية، بما في ذلك التصوير الفوتوغرافي، أو التسجيل، أو استخدام أي نظام من نُظُم تخزين المعلومات واسترجاعها، سواءٌ من الأنظمة الحالية أو المُبتكَرة في المستقبل؛ إلا بعد الرجوع إلى الوكالة، والحصول على إذنٍ خَطّي منها.

ومَنْ يُخالِف ذلك يُعرّض نفسه للمُساءَلة القانونية.

الفهرس

- **تمهيد**

- **حماية الحسابات وكلمات المرور**
  - مفهوم السلامة الرقمية
  - ما هو الأمن السيبراني؟
  - التهديدات السيبرانية الشائعة
  - أهمية كلمة المرور
  - خصائص كلمة المرور القوية
  - أخطاء يجب تجنُّبها في كلمات المرور
  - أدوات إدارة كلمات المرور
  - المصادقة الثنائية (2FA)
  - تسجيل الخروج الآمِن
  - حماية كلمة المرور من السَّرقة
  - نصائح خاصة لإدارة كلمات المرور

- ماذا تفعل إذا نسيت كلمة المرور؟
- السؤال التفاعلي الأول
- السؤال التفاعلي الثاني

- **التصيد الاحتيالي**
  - ما هو التصيُّد الاحتيالي؟
  - أشكال التصيُّد الاحتيال
  - مؤشرات الرسائل الاحتيالية
  - الهندسة الاجتماعية
  - مخاطر شبكات Wi-Fi العامة
  - التصرُّف الصحيح عند الشَّك بالاحتيال
  - تطبيقات وهمية للاحتيال
  - الهجمات عبر الإعلانات
  - كيف تحمي نفسك من الاحتيال؟
  - السؤال التفاعلي الثالث
  - السؤال التفاعلي الرابع

- **الهجمات السيبرانية والبرمجيات الضارَّة وطرق الوقاية**
  - ما هي الهجمات السيبرانية؟
  - الفيروسات
  - ديدان الحاسوب
  - فيروس حصان طروادة
  - برمجيات الفدية (Ransomware)
  - برمجيات التجسُّس (Spyware)
  - الفرق بين الفيروس وبرمجية الفدية
  - كيف تكتشف الإصابة ببرمجيات ضارة؟
  - طرق الوقاية من البرمجيات الخبيثة
  - أهمية النَّسخ الاحتياطي

- السؤال التفاعلي الخامس
- السؤال التفاعلي السادس

- **إجابات الأسئلة التفاعلية**

تمهيد

السَّـلامة الرقميَّة ركيزة أسـاسـيَّة لضـمان أمن المعلومات، وحماية الأفراد والمجتمعات من التهديدات السيبرانية المتزايدة باستمرار.

تمَّ تصميم هذا الكُتَيِّب بهدف توعية ذوي الاحتياجات الخاصَّة -المكفوفين- بمبادئ السلامة الرقمية، وأفضل الممارسات التي تساعدهم على تفادي المخاطر السيبرانية؛ حيث يهدف هذا الكُتَيّب إلى تعزيز وعيهم بأبرز هذه التهديدات؛ مثل التصيد الاحتيالي، وسرقة الهوية الرقمية، والبرمجيَّات الضَّارَّة؛ ممَّا يجعل السلامة الرقمية أولويةً حيويةً لهم.

وتُعدّ هذه الجهود جزءًا من المبادرة الوطنية للسلامة الرقمية التي تُنظّمها الوكالة الوطنية للأمن السيبراني، لبناء بيئة رقمية آمِنَة لجميع فئات المجتمع.

المبادرة الوطنية للسلامة الرقمية

تعريف المبادرة

مجموعة من فعاليات التوعية في مجال السلامة الرقمية والأمن السيبراني؛ تستهدف المجتمع المحليّ على اختلاف الشرائح العُمرية والاجتماعية والقطاعات المهنية.

وتعمل على نشر الوعي بالسلامة الرقمية والاستخدام الآمِن لشبكة الإنترنت والتطبيقات التكنولوجية المختلفة، وتوضيح المخاطر المحتمَلة؛ وذلك بهدف بناء مجتمع آمِن سيبرانيًّا ومُتمكّن تكنولوجيًّا.

الشرائح المُستهدَفة

تستهدف المبادرة مختلف شرائح المجتمع، مع تركيزها في السنة الأولى على الشرائح الآتية:

كبار القَدْر

المرأة والأسرة

ذوو الاحتياجات الخاصة

طلبة الجامعات

العمالة الوافدة

مؤسسات المجتمع المدني

القطاع المالي والمصرفي

أدوات التوعية

تعتمد المبادرة على أدوات توعية متنوّعة ومتكاملة، تشمل الآتي:

- دليل السلامة الرقمية
- كُتَيّبات توعية
- ألعاب سيبرانية
- فيديوهات توعية
- ألعاب تعليمية مُبتكَرة
- وِرَش توعية

حماية الحسابات وكلمات المرور

مفهوم السلامة الرقمية

السلامة الرقمية هي ممارسات تساعدنا على استخدام الإنترنت والتكنولوجيا بطريقة آمِنة، تحمينا من المخاطر وتُحافظ على خصوصيَّتنا.

- تساعد السلامة الرقمية على حماية معلوماتنا الشخصية من السرقة أو الاستخدام غير المُصرَّح به.
- تُمكِّننا من التفاعل على الإنترنت دون الوقوع في شِباك الاحتيال الإلكتروني أو التصيُّد.
- تشمل استخدام أدوات الأمان، مثل: كلمات المرور والمصادقة الثنائية.
- تُعزّز ثقة المستخدِم في استخدام البريد الإلكتروني والخدمات الإلكترونية المختلفة.
- تضمن بيئةً رقميةً أكثر أمانًا لذوي الإعاقة البصرية، خصوصًا عند الاعتماد على قارئات الشاشة.

ما هو الأمن السيبراني؟

الأمن السيبراني هو مجموعة من السياسات والتقنيات والإجراءات التي تهدف إلى حماية المعلومات الرقمية والأجهزة والشبكات من الهجمات السيبرانية.

- يعمل الأمن السيبراني على منع المُتَسلّلين من الوصول إلى بياناتك الخاصة أو تعديلها أو سرقتها.
- يتضمَّن مراقبة الأنظمة وتحديثها بشكلٍ دَوريّ لسَدّ الثغرات الأمنية.
- يشمل الدفاع ضد أنواع متعددة من التهديدات، مثل: الفيروسات والتصيُّد والابتزاز الإلكتروني.
- كل مستخدِم، حتى إن لم يكن خبيرًا، يجب أن يكون على دِراية بأساسيات هذا المجال لحماية نفسه.

التهديدات السيبرانية الشائعة

التهديدات السيبرانية هي محاولات لإلحاق الضَّرر بالمُستخدِم أو الجهاز أو البيانات، وتُشكِّل خطرًا حقيقيًّا على كل مَن يستخدم الإنترنت، ومن أبرزها ما يلي:

- التصيّد الاحتيالي هو أسلوب مخادع لخداع الضحية، ودفعه للكشف عن معلومات حسَّاسة، مثل: كلمات المرور أو بيانات بطاقات الائتمان.
- الفيروسات والبرمجيات الخبيثة قد تتسبَّب في تلف الجهاز، أو سرقة الملفات المهمَّة، أو تعطيل النظام بشكلٍ كاملٍ.
- الهندسة الاجتماعية تعتمد على استغلال مشاعر الناس كالثّقة أو الخوف للحصول على بياناتهم دون استخدام أدوات تقنية.
- هجمات الشبكات، مثل: اختراق شبكة Wi-Fi، تُتيح للمهاجمين التجسُّس على كل ما تفعله على الإنترنت.
- البرامج المزيَّفة قد تُقنع المستخدِم بتحميلها، لتبدأ بعدها بسرقة بياناته أو السيطرة على جهازه.

أهمية كلمة المرور

كلمة المرور هي المفتاح الرئيسي للدخول إلى حساباتك، ويجب أن تكون قويَّة؛ لأنها الحاجز الأول ضد أي محاولات اختراق.

- من دون كلمة مرور جيّدة، يمكن لأي شخص الدخول إلى بريدك أو ملفاتك أو حتى حسابك البنكي.
- كلمة المرور القوية تمنع الوصول غير المُصرَّح به إلى معلوماتك الحسَّاسة.
- كثير من المخترِقين ينجحون فقط لأنّ المستخدِمين يستخدمون كلمات مرور ضعيفة أو مكرَّرة.
- استخدام كلمة مرور مميَّزة لكل حساب يُقلّل من الخطر في حال اختراق أحد الحسابات.
- حماية كلمة المرور تعني حماية الهوية الرقمية بشكلٍ كاملٍ.

خصائص كلمة المرور القوية

كلمة المرور القوية ليست مجرد كلمة طويلة، بل يجب أن تكون صعبة التوقُّع، ويصعب كسرها بالبرمجيات الخبيثة أو التخمين اليدوي.

- يجب أن تحتوي على 12 حرفًا على الأقل؛ لتجعل عملية كسرها صعبة تقنيًّا.
- من الأفضل أن تتضمَّن مزيجًا من الحروف الكبيرة والصغيرة لتزيد من تنوُّع الاحتمالات.
- وجود أرقام ضمن الكلمة يُعزّز تعقيدها، ويُصعّب على المخترقين تخمينها.
- إضافة رموز مثل: ! و@ و# يجعل الكلمة أكثر أمانًا، ويضيف طبقة حماية إضافية.
- تجنُّب الكلمات أو الأسماء المعروفة، مثل: اسم المستخدِم أو رقم الهاتف، يُعدّ أمرًا ضروريًّا.

أخطاء يجب تجنُّبها في كلمات المرور

هناك أخطاء شائعة تجعل كلمات المرور سهلة الاختراق، ويجب تجنُّبها لتفادي التعرُّض للخطر؛ من أهمّها ما يلي:

- استخدام كلمات مرور شائعة جدًّا، مثل: 123456 أو password، يجعل الحساب سهل التعرُّض للاختراق.
- تكرار كلمة المرور نفسها في أكثر من حسابٍ يزيد من احتمالية الوصول الكامل لجميع حساباتك إذا تمَّ تسريب واحدة منها.
- إرسال كلمة المرور إلى نفسك عبر البريد أو الرسائل هو تصرُّف غير آمِن إطلاقًا، ويجب تجنُّبه.
- مشاركة كلمة المرور مع أشخاص آخرين حتى لو كنت تثق بهم، أمر غير مُوصى به.

أدوات إدارة كلمات المرور

هذه الأدوات تساعدك في إنشاء وحفظ كلمات مرور قويَّة دون الحاجة لتذكُّر كل واحدة منها.

- تحفظ جميع كلمات المرور في مكان واحد مُشفَّر وآمِن، ولا يمكن الوصول إليه إلا بكلمة رئيسية قوية.
- تُوفر ميزة توليد كلمات مرور عشوائية وصعبة يمكن استخدامها فورًا لأي موقع.
- تجعل تجربة الاستخدام أسهل، خاصةً للمستخدِمين الذين يعانون ضعف البصر أو مشكلات في الحفظ.
- يمكن تحميلها كتطبيقات على الهاتف المحمول أو الحاسوب الشخصي.
- بعض البرامج مصمَّمة لتكون متوافقة مع قارئات الشاشة؛ مما يجعلها مثاليةً للمكفوفين.

المصادقة الثنائية (2FA)

المصادقة الثنائية هي وسيلة أمان تضيف خطوةً ثانيةً لحماية حسابك بعد كتابة كلمة المرور.

- تطلب منك إدخال رمز تحقُّق يتم إرساله إلى هاتفك أو بريدك الإلكتروني بعد كتابة كلمة المرور.
- تمنع المخترِق من الدخول حتى لو كان يعرف كلمة مرورك؛ لأنه لا يملك رمز التحقُّق الثاني.
- متاحة في معظم التطبيقات الشهيرة، مثل: Gmail و Facebook وTwitter.
- تساعد بشكلٍ خاصّ في حماية الحسابات البنكية والبريدية من الهجمات السيبرانية.
- من المهم تفعيلها في جميع حساباتك الشخصية والمهنيَّة.

تسجيل الخروج الآمِن

تسجيل الخروج من حساباتك هو خطوة أساسية في حفظ الأمان، خاصةً عند استخدام أجهزة ليست ملكك؛ وذلك باتّباع ما يلي:

- تأكَّد دائمًا من تسجيل الخروج بعد الانتهاء من استخدام أي حساب.
- لا تستخدم خاصية "تذكَّرني" على أجهزة مشتركة أو عامة.
- امسح سجل التصفُّح وكلمات المرور المحفوظة على أي جهاز لا تملكه.
- لا تترك جلسة مفتوحة دون مراقبة، حتى في المنزل.
- عند الشك في أن جهازًا ما استخدم حسابك، قُمْ بتغيير الكلمة فورًا.

حماية كلمة المرور من السرقة

الوقاية من السرقة الرقمية تبدأ بالحفاظ على خصوصية كلمة المرور وعدم مشاركتها بأي شكل. ولحماية كلمة مرورك من السرقة، ينبغي اتّباع الخطوات الآتية:

- لا تُرسِل كلمتك عبر الرسائل أو البريد الإلكتروني لأيّ أحد، مهما كنت تثق به.
- لا تكتب كلمتك على ورقة مُلصَقة على الجهاز أو في مكان مكشوف.
- عند إدخال الكلمة في جهاز عام، تأكَّدْ من عدم وجود برامج تتبُّع أو تسجيل.
- إذا لاحظت أي محاولة دخول غير طبيعية، غيِّرْ كلمتك فورًا.
- استخدِم أدوات الحماية مثل التحقُّق بخطوتَين كلَّما أمكن ذلك.

نصائح خاصة لإدارة كلمات المرور

يحتاج المكفوفون إلى تقنيَّات وأساليب مناسبة تساعدهم على حماية كلماتهم وتذكُّرها بطريقة آمِنة، ومن أهم تلك الأساليب ما يلي:

- استخدِمْ تطبيقات إدارة كلمات مرور تدعم القارئ الصوتي أو طريقة برايل.
- لا تعتمد فقط على الحفظ العقلي، بل استخدِمْ أدوات تكنولوجية لحمايتها.
- استشر شخصًا تثق به عند إعداد النظام، ثمَّ حافِظْ على السرية بعد ذلك.
- جرِّب استخدام التعرف على البصمة أو الوجه لتقليل الاعتماد على الكتابة.

ماذا تفعل إذا نسيت كلمة المرور؟

نسيان كلمة المرور أمر طبيعي، وهناك خطوات آمِنة يمكن اتّباعها لاستعادتها؛ من أهمّها:

- استخدِمْ خيار "نسيت كلمة المرور" الموجود في معظم المواقع.
- تأكَّد من أن بريدك الإلكتروني أو رقم هاتفك محدَّث لاستلام رمز الاستعادة.
- بعد استعادة الوصول، أنشِئ كلمةً جديدةً أقوى من السابقة.
- لا تستخدِمْ كلمة المرور القديمة إذا تمَّ اختراق الحساب.
- فكِّر في استخدام برنامج لحفظ كلمات المرور لتفادي النسيان مستقبلًا.

السؤال التفاعلي الأول:

أيّ مما يلي يُعدّ كلمة مرور قوية وآمِنة؟

أ. 123456

ب. Qwerty

ج. Ahmed1990

د. Gt#9L@2m$P

السؤال التفاعلي الثاني:

ما هو أول تصرُّف يجب أن تقوم به عند الشَّكّ في اختراق حسابك؟

أ) تَجاهُل الرسالة والانتظار.

ب) مشاركة كلمة المرور مع صديق للمساعدة.

ج) إنشاء حساب جديد فورًا.

د) تغيير كلمة المرور على الفور.

التصيد الاحتيالي

ما هو التصيُّد الاحتيالي؟

التصيُّد الاحتيالي هو محاولة لخداعك من خلال رسائل أو مواقع تبدو وكأنَّها حقيقية، لكنَّها مصمَّمة لسرقة معلوماتك.

- غالبًا ما تأتي على شكل رسائل بريد إلكتروني أو رسائل نصيَّة مزيَّفة.
- تطلب منك إدخال بيانات حساسة، مثل: كلمات المرور أو أرقام البطاقات البنكية.
- تستخدم لغة مستعجلة مثل "حسابك موقوف، تصرَّف الآن!" لتحفيزك على التفاعل دون تفكير.
- تقلّد شعارات مؤسسات معروفة لتبدو وكأنها شرعية.
- الهدف الرئيسي هو سرقة معلوماتك لاستغلالها ماليًّا أو للابتزاز.

أشكال التصيُّد الاحتيالي

تختلف طرق التصيُّد، لكنَّها تشترك في محاولتها خداع المستخدِم للحصول على معلومات سرّيَّة. ومن أبرز أشكال التصيُّد الاحتيالي ما يأتي:

- رسائل البريد الإلكتروني المزيَّفة التي تحاكي شكل الرسائل الرسمية.
- روابط تقودك إلى صفحات وهمية تطلب تسجيل الدخول أو إدخال معلومات حسَّاسة.
- مكالمات هاتفية يدَّعي فيها المتَّصل أنه من جهة رسمية أو بنك.
- رسائل نصية قصيرة تطلب تأكيد بياناتك أو الضغط على رابط مشبوه.
- إعلانات وهمية تَعدك بجوائز مقابل ملء استبيانات أو إدخال رقم بطاقتك.

مؤشرات الرسائل الاحتيالية

يمكن التعرف على الرسائل المزيَّفة من خلال ملاحظة بعض العلامات؛ من أهمّها:

- وجود أخطاء لغويَّة أو إملائية غير معتادة في الرسالة.
- عنوان البريد الإلكتروني لا يتطابق مع العنوان الرسمي للمؤسسة.
- الروابط تبدو غريبة أو غير مألوفة، حتى لو احتوَتْ على اسم جهة معروفة.
- الرسالة تطلب معلومات شخصية حسَّاسة بشكل مباشر.
- وجود تهديد أو استعجال لاتخاذ إجراء فَوْريّ، مثل: "سيُغلَق حسابك خلال 24 ساعة".

الهندسة الاجتماعية

الهندسة الاجتماعية تعتمد على استغلال المشاعر البشرية لخداعك، بدلًا من استخدام أدوات تقنية مُعقَّدة.

- يستخدم المهاجِم أسلوب الإقناع والتلاعب النَّفسي للحصول على معلوماتك.
- قد يتظاهر بأنه موظَّف دعم فني، أو صديق، أو مسؤول.
- يعتمد على جمع معلومات عنك من مواقع التواصل لجعلك تثق به.
- يستغل مشاعر مثل: الخوف، أو التعاطف، أو الحرج لدفعك للتجاوب.
- تُعدّ من أخطر الوسائل لأنَّها لا تحتاج إلى مهارات تقنية، بل تعتمد على سلوك الضحيَّة.

مخاطر شبكات Wi-Fi العامة

استخدام الشبكات المفتوحة قد يُعرّض بياناتك للاختراق إذا لم تتَّخذ احتياطات كافية.

- يمكن لأيّ شخص متَّصل بنفس الشبكة التنصُّت على البيانات المرسَلة.
- بعض المهاجمين ينشئون شبكات باسم يشبه أسماء الفنادق أو المقاهي لجَذْب الضحايا.
- غالبًا ما تكون هذه الشبكات غير مُشفَّرة؛ مما يسمح برؤية كل ما تُرسله.
- لا يُنصَح بإجراء معاملات مالية أو إدخال كلمات مرور أثناء الاتصال بها.
- يجب استخدام VPN عند الاضطرار لاستخدام شبكة عامَّة؛ لحماية الاتصال.

التصرُّف الصحيح عند الشَّك بالاحتيال

إذا شعرت أن هناك شيئًا مريبًا في رسالة أو موقع، يجب أن تتوقَّف وتتأكد قبل التفاعل؛ وذلك باتباع الإرشادات الآتية:

- لا تفتح الروابط المشبوهة ولا تُدخِل بياناتك.
- تواصَلْ مع الجهة الرسمية عبر أرقامها المعروفة لتأكيد الرسالة.
- استخدِمْ برامج الحماية الموثوقة التي تكشف المواقع الاحتيالية.
- لا تُعد إرسال الرسالة إلى الآخرين دون التأكُّد من صحَّتها.
- في حال أدخلت معلوماتك بالفعل، بادِرْ بتغيير كلمات المرور فورًا.

تطبيقات وهمية للاحتيال

بعض التطبيقات المصمَّمة بطريقة احترافية تكون في الواقع أدوات لجمع البيانات أو تنفيذ الاحتيال.

- قد تطلب أذونات غير منطقية، مثل: الوصول إلى الرسائل أو الكاميرا.
- يمكنها التجسُّس على المكالمات أو نَسْخ البيانات الشخصية.
- في بعض الحالات، تُستخدَم لتفعيل اشتراكات مدفوعة بدون عِلْمك.
- يجب تحميل التطبيقات فقط من المتاجر الرسمية، مثل: Google Play أو App Store
- اقرأ تقييمات المستخدِمين، وراجِعْ عدد مرات التحميل قبل التثبيت.

الهجمات عبر الإعلانات

بعض الإعلانات الرقمية تحتوي على روابط خبيثة تؤدي إلى مواقع خطيرة.

- قد تبدأ بإعلان جذَّاب، مثل: "ربح هاتف جديد"، أو "احصل على وظيفة أحلامك".
- بمجرد النقر عليها، يتم تثبيت برمجيات ضارّة أو توجيهك لموقع مزيَّف.
- بعض هذه الإعلانات تظهر في مواقع معروفة، لكنها تأتي من شركات غير موثوقة.
- لا تنقر على الإعلانات التي تطلب معلوماتك الشخصية فورًا.
- استخدِمْ إضافات المتصفّح التي تمنع الإعلانات المنبثقة أو التتبُّع.

كيف تحمي نفسك من الاحتيال؟

الحماية تبدأ بالوعي، وتتطلب اتباع ممارسات آمِنة دائمًا عند استخدام الإنترنت، ومن أهم تلك الممارسات ما يلي:

- لا تفتح أيّ رسالة إلكترونية أو رابطًا قبل التأكد من مصدره الحقيقي.
- لا تُدخِلْ بياناتك الشخصية في مواقع لا تثق بها أو لا تبدأ بـHTTPS
- فعِّل المصادقة الثنائية في جميع حساباتك، خاصَّةً البريد الإلكتروني والبنوك.
- استخدِمْ برنامج حماية فعَّالًا، وحدِّثْه باستمرار.
- إذا شعرت بالشكّ، استشِرْ خبيرًا أو تَواصَلْ مع الجهة المعنيَّة مباشرةً.

السؤال التفاعلي الثالث:

عند تلقّي رسالة تخبرك أنك ربحت جائزة وتطلب بياناتك، ماذا يجب أن تفعل؟

أ) إدخال البيانات للحصول على الجائزة.

ب) مشاركة الإعلان مع الأصدقاء.

ج) التحقُّق من مصدر الرسالة قبل أي تصرُّف.

د) الضغط على الرابط لتجربة الحظ.

السؤال التفاعلي الرابع:

ما العلامة التي تُشير إلى أن الموقع آمِن عند إدخال معلوماتك؟

أ) أن يكون لونه أزرق.

ب) أن يحتوي على صور جميلة.

ج) أن يبدأ بـhttp.

د) أن يبدأ بـ https ويوجد رمز القفل بجانبه.

الهجمات السيبرانية والبرمجيات الخبيثة وطرق الوقاية

ما هي الهجمات السيبرانية؟

الهجوم السيبراني هو محاولة خبيثة للوصول إلى بياناتك، أو تعطيل أجهزتك الرقمية بطرق غير قانونية.

- قد يستهدف الأفراد أو الشركات أو المؤسسات الحكومية.
- الهدف هو سرقة البيانات، أو تخريب الأنظمة، أو طلب فدية مالية.
- يتم غالبًا عبر الإنترنت، لكنَّه قد يبدأ بوسائل بسيطة مثل رسالة بريد إلكتروني.
- يمكن أن يؤدي إلى خسائر مالية كبيرة أو تسريب معلومات حسَّاسة.
- تشمل أنواع الهجمات: الفيروسات، التصيُّد، الفدية، والهندسة الاجتماعية.

الفيروسات

الفيروس هو برنامج ضارّ يدخل إلى جهازك ويُغيّر طريقة عمله، أو يتلف البيانات الموجودة عليه.

- يُرفق غالبًا مع ملفات تبدو طبيعية مثل الصُّوَر أو المستندات.
- يبدأ الفيروس بالانتشار عند فتح الملف أو تشغيله.
- بعض الفيروسات تتسبَّب في حذف الملفات أو تعطيل النظام بشكلٍ كاملٍ.
- ينتقل من جهازٍ إلى آخر عبر الإنترنت أو وسائط مثل USB
- الحماية منه تكون عبر برامج مكافحة الفيروسات المُحدَّثة باستمرار.

ديدان الحاسوب

ديدان الحاسوب هي برامج خبيثة تُشبه الفيروسات، لكنَّها أكثر خطورةً بسبب قدرتها على الانتشار التلقائي.

- لا تحتاج الدودة إلى ملف لبدء نشاطها، بل تنتشر من خلال الشبكات أو البريد الإلكتروني.
- تستهدف عادةً الأنظمة المتصلة ببعضها داخل المنزل أو الشركة.
- يمكنها إبطاء سرعة الإنترنت أو الأجهزة بشدَّة.
- بعض الديدان تُستخدَم كنقطة دخول لتثبيت برمجيات أخرى خطيرة.
- الوقاية منها تتطلب تحديث الأنظمة وبرامج الحماية، خاصَّةً في الشبكات المفتوحة.

فيروس حصان طروادة

هذا الفيروس يتنكَّر على شكل برنامج مفيد، لكنَّه في الحقيقة يعمل على إيذاء جهازك أو سرقة معلوماتك.

- يبدو وكأنه أداة مفيدة، مثل لعبة أو برنامج تنظيف الجهاز.
- عند تشغيله، يفتح بابًا خلفيًّا يُتيح للمهاجم التحكُّم بجهازك.
- لا يُظهِر نفسه بشكل واضح مما يُصعّب من اكتشافه.
- يُستخدم أحيانًا لسرقة كلمات المرور أو مراقبة الشاشة.
- الوقاية منه تكون بعدم تحميل البرامج من مواقع مجهولة أو روابط مشبوهة.

برمجيات الفدية (Ransomware)

برمجيات الفدية هي أحد أخطر أنواع الهجمات؛ حيث يتم تشفير ملفاتك ثم يُطلَب منك دفع مبلغ مالي لفَكّ التشفير.

- تُرسل عادةً عبر رسائل بريد إلكتروني تحتوي على مرفقات مزيَّفة.
- بعد الإصابة، تُغلق الملفات أو النظام بالكامل.
- المهاجم يطلب فدية غالبًا بعملة رقمية مثل البيتكوين.
- حتى عند الدفع، لا يوجد ضمان لاسترجاع الملفات.
- الحل الأفضل هو الوقاية: النَّسخ الاحتياطي المنتظِم، وعدم فتح المرفقات المشبوهة.

برمجيات التجسُّس (Spyware)

تعمل هذه البرمجيات في الخفاء، وتُسجِّل كل ما تفعله على الجهاز، بما في ذلك ضغطات لوحة المفاتيح.

- تُرسِل معلوماتك للمهاجم، بما في ذلك كلمات المرور ورسائل البريد.
- قد تراقب الكاميرا أو الميكروفون دون إذنك.
- يمكن أن تُبطئ الجهاز وتجعله يتصرّف بغرابة.
- من الصعب ملاحظتها دون برنامج متخصّص.
- استخدِمْ جدار حماية (Firewall) ومضاد فيروسات قويًّا لاكتشافها.

الفرق بين الفيروسات وبرمجيات الفدية

كلاهما برمجيات ضارة، لكن يختلفان في طريقة التأثير والأسلوب.

- الفيروس يهدف غالبًا إلى الإفساد أو التخريب العام للجهاز أو النظام.
- برمجية الفدية تُركّز على حبس ملفاتك مقابل المال.
- الفيروسات قد تعمل بصمتٍ، أما الفدية تظهر رسائل تهديد واضحة.
- كلاهما ينتشر غالبًا من خلال روابط أو مرفقات مشبوهة.
- كلاهما يمكن الوقاية منه من خلال التحديثات الدورية وبرامج الحماية.

كيف تكتشف الإصابة ببرمجيات ضارة؟

هناك علامات تدل على وجود مشكلة في جهازك؛ من أهمها ما يأتي:

- بطء مُفاجِئ في الجهاز أو استهلاك أعلى للطاقة.
- رسائل خطأ غريبة أو اختفاء بعض الملفات.
- فتح مواقع تلقائيًّا أو برامج تعمل دون إذنك.
- تعذُّر الوصول إلى ملفاتك أو تغيير أسماء الملفات بشكل عشوائي.
- ظهور رسالة تطلب فديةً أو كلمة مرور لفتح ملفَّاتك.

طرق الوقاية من البرمجيات الخبيثة

الوقاية دائمًا أفضل من العلاج، ويمكنك حماية نفسك بعدَّة خطوات بسيطة؛ أبرزها ما يأتي:

- لا تفتح مرفقات البريد الإلكتروني إلا إذا كنت تعرف المُرسِل.
- قُمْ بتحديث نظام التشغيل والتطبيقات بانتظامٍ.
- استخدِمْ برنامج مكافحة فيروسات مَوثُوق مع التحديث التلقائي.
- لا تقم بتوصيل أجهزة USB من مصادر غير معروفة.
- فعِّل جدار الحماية لمنع الاتصالات غير المُصرَّح بها.

أهمية النَّسخ الاحتياطي

النَّسخ الاحتياطي هو حفظ نسخة من بياناتك في مكان آمِن، لاستخدامها في حال ضياع الملفات أو تشفيرها.

- يمكنك عمل نُسَخ احتياطية على قرص خارجي أو سحابة إلكترونية.
- يجب أن تكون النُّسخة منفصلةً عن الجهاز الأساسي.
- لا توصل القرص الاحتياطي بالإنترنت إلا عند النَّسخ فقط.
- قم بالنَّسخ دوريًّا، أسبوعيًّا، أو شهريًّا حسب أهمية الملفات.
- هذا الإجراء بسيط، لكنَّه يحميك من خسائر كبيرة لاحقًا.

السؤال التفاعلي الخامس:

ما هي نتيجة الإصابة ببرمجيات الفدية؟

أ) حذف الصُّوَر فقط.

ب) سرقة الإنترنت.

ج) تشفير الملفات وطلب فدية مقابل استرجاعها.

د) إعادة تشغيل الجهاز تلقائيًّا.

السؤال التفاعلي السادس:

أيّ من الآتي يُعدّ من أهم خطوات الوقاية من البرمجيات الخبيثة؟

أ) تَجاهُل التحديثات.

ب) تحميل البرامج من أيّ موقع.

ج) استخدام قرص USB من صديق.

د) تحديث البرامج وعدم فتح المرفقات المَشبُوهة.

إجابات الأسئلة التفاعلية

إجابة السؤال التفاعلي الأول

د) Gt#9L@2m$P

إجابة السؤال التفاعلي الثاني

د) تغيير كلمة المرور على الفَوْر.

إجابة السؤال التفاعلي الثالث

ج) التحقُّق من مصدر الرسالة قبل أي تصرُّف.

إجابة السؤال التفاعلي الرابع

د) أن يبدأ بـ https ويوجد رمز القفل بجانبه.

إجابة السؤال التفاعلي الخامس

ج) تشفير الملفات، وطلب فديَّة مقابل استرجاعها.

إجابة السؤال التفاعلي السادس

د) تحديث البرامج وعدم فتح المرفقات المشبوهة.