الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مبادئ عامة في السلامة الرقمية

الشريحة المُستهدَفة
ذوو الإعاقة البصرية

لغة برايل

النور Al Noor
تمكين وإدماج
Empowerment & Integration
الاجتماعي Social

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبـــادئ عامـــة فـي السلامـــة الرقميـة

الشريحة المستهدفة

ذوو الإعاقة البصرية

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الفهرس

الفهرس

الفهرس

حقوق الملكية الفكرية

المادة مملوكة للوكالة الوطنية للأمــن السيبراني في دولة قطر، وكافَّة حقــوق الملكية الفكرية التي تشــمل حــقّ المُؤلّف وحقوق التأليــف والنشــر والطباعة، كُلّهــا مكفولة للوكالــة الوطنية للأمن السيبراني فــي دولة قطر.

وعليه فجميــع الحقوق محفوظــة للوكالة، ولا يجوز إعادة نشــر أيّ أجزاء من هذا الكُتَيّب، أو الاقتباس منه، أو نَسْــخ أي جزء منه، أو نقله كلياً أو جزئيّاً في أي شــكلٍ وبأي وسيلة، ســواء بطُرق إلكترونية أو آليــة، بما في ذلك التصوير الفوتوغرافي، أو التســجيل، أو اســتخدام أي نظام من نُظُم تخزين المعلومات واســترجاعها، سواء من الأنظمة الحاليــة أو المُبتكَــرة في المســتقبَل؛ إلا بعد الرجوع إلــى الوكالة، والحصول علــى إذنٍ خَطّي منها.

ومَنْ يُخالِف ذلك يُعرّض نفسه للمُساءَلة القانونية.

للتواصل مع إدارة التميز السيبراني الوطني

0097 440 466 379

00974 404 663 62

cyberexcellence@ncsa.gov.qa

https://www.ncsa.gov.qa/

تمهيد

السَّلامــة الرقميَّــة ركيزة أساســيَّة لضمــان أمــن المعلومات، وحماية الأفراد والمجتمعات من التهديدات السيبرانية المتزايدة باستمرار.

تــمَّ تصميم هذا الكُتَيِّــب بهدف توعيــة ذوي الإعاقة البصرية بمبادئ السلامة الرقمية، وأفضل الممارســات التي تساعدهم على تفادي المخاطر السيبرانية؛ حيــث يهدف هذا الكُتَيّب إلى تعزيــز وعيهم بأبرز هــذه التهديــدات؛ مثل: التصيــد الاحتيالي، وسرقة الهوية الرقمية، والبرمجيَّات الضَّارَّة؛ ممَّا يجعل السلامة الرقمية أولويــةً حيويةً لهم.

وتُعــدّ هــذه الجهــود جزءاً مــن المبــادرة الوطنيــة للسلامة الرقميــة التي تُنظّمها الوكالة الوطنية للأمــن السيبراني، لبناء بيئــة رقمية آمِنَــة لجميع فئــات المجتمع.

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

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 سيبرانيّاً ومُتمكّن تكنولوجيّاً.

الشرائح المُستهدَفة

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

أدوات التوعية

تعتمد المبادرة على أدوات توعية متنوّعة ومتكاملة، تشمل ما يلي:

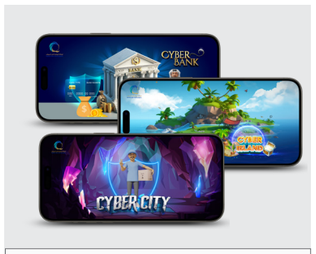
دليل السلامة الرقمية

كُتيّبات توعية مطبوعة

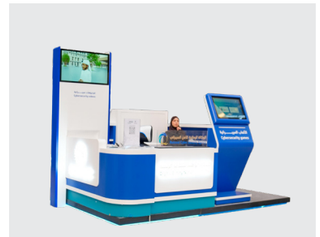
شرائح العرض (للمُدرّبين)

فيديوهات التوعية (أنيميشن)

فيديوهات التوعية (تمثيلية)



الألعاب السيبرانية



بوابة التوعية السيبرانية

الروبوت التفاعلي

وِرَش التوعية

مفهوم السلامة الرقمية

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

01 تساعد السلامة الرقمية على حماية معلوماتنا الشخصية من السرقة أو الاستخدام غَير المُصرَّح به.

02 تُمكِّننا من التفاعل على الإنترنت دون الوقوع في شِباك الاحتيال الإلكتروني أو التصيُّد.

03 تشمل استخدام أدوات الأمان، مثل: كلمات المرور والمصادقة الثنائية.

04 تُعزّز ثقة المستخدِم في استخدام البريد الإلكتروني والخدمات الإلكترونية المختلفة.

05 تضمن بيئةً رقميةً أكثر أماناً لذوي الإعاقة البصرية، خصوصاً عند الاعتماد على قارئات الشاشة.

ما هو الأمن السيبراني؟

الأمــن السيبراني هو مجموعة من السياســات والتقنيــات والإجراءات التي تهدف إلى حمايــة المعلومات الرقمية والأجهزة والشــبكات من الهجمــات السيبرانية.

يعمــل الأمــن السيبرانــي علــى منْــع المُتَســلّلين من الوصــول إلــى بياناتك الخاصــة أو تعديلها أو ســرقتها

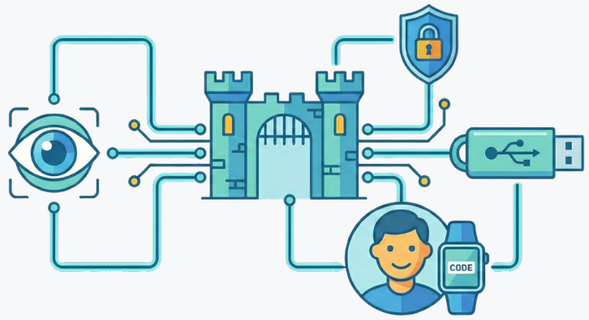
يتضمَّن مراقبــة الأنظمة وتحديثها بشــكلٍ دَوريّ لسَــدّ الثــغرات الأمنية

يشــمل الدفاع ضد أنواع متعددة مــن التهديدات، مثل: الفيروســات والتصيُّد والابتزاز الإلكتروني

كل مســتخدِم، حتى إن لم يكــن خبيراً، يجِــب أن يكون على دِراية بأساســيات هــذا المجال لحماية نفســه

التهديدات السيبرانية الشائعة

التهديــدات السيبرانية هي محاولات لإلحاق الضَّرر بالمُســتخدِم أو الجهــاز أو البيانات، وتُشــكِّل خطراً حقيقيّــاً على كل مَن يســتخدِم الإنترنت، ومــن أبرزها ما يلي:



التصيّــد الاحتيالي هو أســلوب مخادع لخــداع الضحية، ودفعه للكشــف عن معلومــات حسَّاســة، مثــل: كلمــات الــمرور أو بيانات بطاقــات الائتمان

الفيروســات والبرمجيــات الخبيثة قد تتســبَّب في تَلَف الجهاز، أو ســرقة الملفات المهمَّــة، أو تعطيل النظام بشكلٍ كامل

الهندســة الاجتماعيــة تعتمِــد على اســتغلال مشــاعر النــاس كالثّقة أو الخوف للحصول علــى بياناتهم دون اســتخدام أدوات تقنية

هجمات الشــبكات، مثــل: اختراق شــبكة Wi-Fi، تُتيــح للمهاجميــن التجسُّــس على كل ما تفعله على الإنترنت

البرامج المزيَّفة قد تُقنع المســتخدِم بتحميلها، لتبدأ بعدها بســرقة بياناته
أو السَيطرة على جهازه

أهمية كلمة المرور

كلمــة المرور هــي المفتاح الرئيســي للدخــول إلــى حســاباتك، ويجِــب أن تكــون قويّة؛ لأنهــا الحاجــز الأول ضد أي محــاولات اختراق.

01 من دون كلمة مرور جيّدة، يمكن لأي شــخص الدخــول إلى بريدك أو ملفاتك أو حتى حســابك البنكي.

02 كلمة الــمرور القوية تمنع الوصول غَير المُــصرَّح به إلى معلوماتك الحسَّاسة.

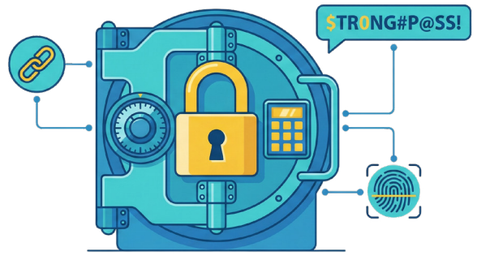
03 كثير مــن المخترِقين ينجحون فقط لأنّ المســتخدِمين يســتخدمون كلمات مرور ضعيفــة أو مكرَّرة.

04 اســتخدام كلمة مرور مميَّزة لكل حســاب يُقلّل من الخطر في حال اختراق أحد الحسابات.

05 حماية كلمة المرور تعني حماية الهوية الرقمية بشكلٍ كامل.

خصائص كلمة المرور القوية

كلمــة الــمرور القويــة ليســت مجــرد كلمة طويلــة، بل يجِــب أن تكــون صعبــة التوقُّع، ويصعــب كســرها بالبرمجيــات الخبيثــة أو التخميــن اليدوي.



01 يجِــب أن تحتــوي علــى 12 حَرفاً علــى الأقل؛ لتجعــل عملية كســرها صعبــة تقنيّاً.

02 مــن الأفضــل أن تتضمَّــن مزيجــاً مــن الحروف الكبيرة والصغيــرة لتزيد من تنــوُّع الاحتمالات.

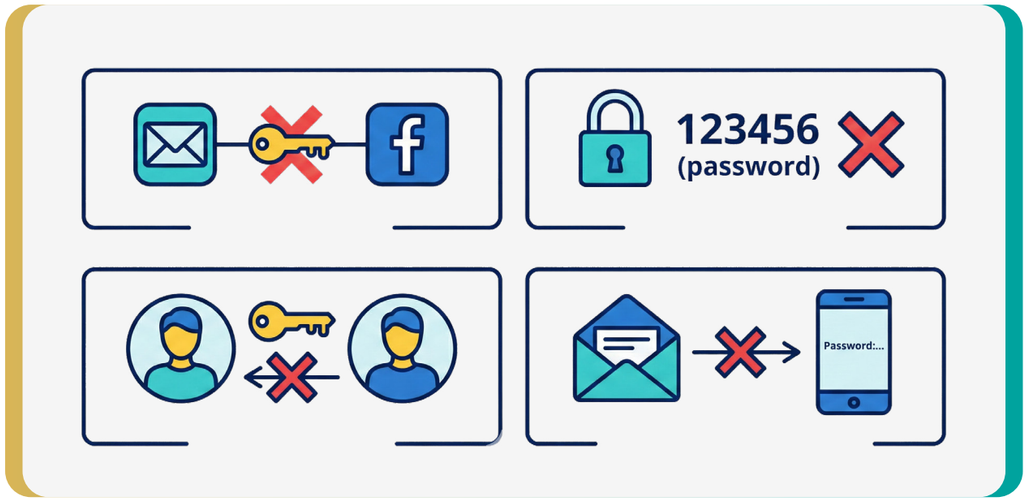
03 وجــود أرقــام ضمــن الكلمــة يُــعزّز تعقيدها، ويُصعّــب علــى المخترِقيــن تخمينهــا.

04 إضافة رموز مثــل: (! و@ و#) يجعل الكلمة أكثر أماناً، ويضيــف طبقة حماية إضافية.

05 تجنُّب الكلمات أو الأسماء المعروفة، مثل: اسم المستخدِم أو رقم الهاتف، يُعدّ أمراً ضروريّاً.

أخطاء يجِب تجنُّبها في كلمات المرور

هناك أخطاء شـائعة تجعل كلمات المرور سـهلة الاختراق، ويجِب تجنُّبها لتفادي التعرُّض للخطر مـن أهمّها ما يلي:



استخدام كلمات مرور شائعة جدّاً، مثل: 123456 أو (password)، يجعل الحساب سهل التعرُّض للاختراق

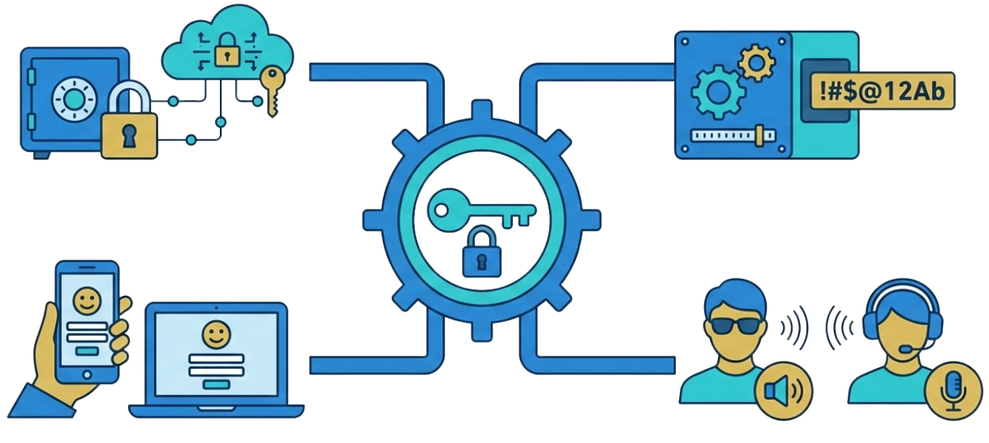
تـكرار كلمة الـمرور نفسـها في أكثر مـن حسـاب يزيد مـن احتمالية الوصـول الكامـل لجميع حسـاباتك إذا تـمَّ تسريب واحـدة منها

إرسـال كلمة الـمرور إلى نفسـك عبْر البريد أو الرسـائل هو تصـرُّف غَير آمِن إطلاقـاً، ويجِب تجنُّبه

مشـاركة كلمة المرور مع أشـخاص آخرين، حتى لو كنـتَ تثِق بهم، أمر غَير مُوصّى به

أدوات إدارة كلمات المرور

تُحفظ جميع كلمات المرور في مكان واحد مُشفَّر وآمِن، ولا يمكن الوصول إليه إلا بكلمة رئيسية قوية.



01 تُوفر ميزة توليد كلمات مرور عشوائية وصعبة يمكن استخدامها فَوراً لأي موقع.

02 كلمة المرور القوية تمنع الوصول غَير المُصرَّح به إلى معلوماتك الحسَّاسة.

03 تجعل تجربة الاستخدام أسهل، خاصةً للمستخدِمين الذين يعانون ضعف البصر أو مشكلات في الحفظ.

04 يمكن تحميلها كتطبيقات على الهاتف المحمول أو الحاسوب الشخصي.

05 بعض البرامج مصمَّمة لتكون متوافقة مع قارئات الشاشة؛ مما يجعلها مثاليةً للمكفوفين.

المصادقة الثنائية (2FA)

المصادقــة الثنائية هي وســيلة أمان تضيف خطــوةً ثانيةً لحماية حســابك بعد كتابة كلمــة المرور.

تطلــب منك
إدخال رمــز تحقُّق يتم إرســاله إلى هاتفــك أو بريــدك الإلكتروني بعد كتابة كلمــة المرور.

تمنــع المخترِق
من الدخــول، حتــى لــو كان يعرف كلمــة مرورك؛ لأنــه لا يملــك رمــز التحقُّــق الثاني.

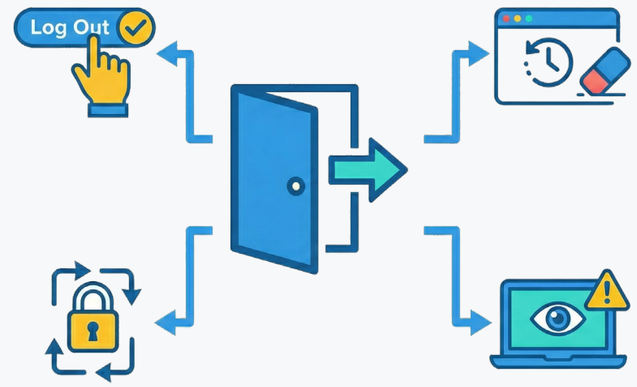
متاحــة فــي
معظــم التطبيقــات الشــهيرة، مثل: Gmail Facebookg Xg.

تســاعد بشــكلٍ
خاصّ في حماية الحســابات البنكية والبريدية مــن الهجمــات السيبرانية.

مــن المهــم تفعيلهــا فــي جميــع
حســاباتك الشــخصية والمهنيَّــة.

تسجيل الخروج الآمِن

تســجيل الخروج من حســاباتك هو خطوة أساســية في حِفظ الأمــان، خاصةً عند اســتخدام أجهزة ليســت ملكك؛ وذلك باتّباع ما يلي:



01	تأكَّد دائماً من تسجيل الخروج بعد الانتهاء من استخدام أي حساب.
02	لا تَستخدِم خاصية (تذكَّرني) على أجهزة مشترَكة أو عامة.
03	امسح سجِل التصفُّح وكلمات المرور المحفوظة على أي جهاز لا تملكه.
04	لا تترك جلسة مفتوحة دون مراقبة، حتى في المنزل.
05	عند الشك في أن جهازاً ما استخدَم حسابك، قُمْ بتغيير الكلمة فَوراً.

حماية كلمة المرور من السرقة

الوقايـة مـن السـرقة الرقميـة تبـدأ بالحفـاظ علـى خصوصيـة كلمـة الـمرور وعـدم مشاركتها بأي شكل، ولحماية كلمة مرورك من السرقة، ينبغي اتّباع الخطوات الآتية:

01 لا تُرسِل كلمتك عبْر الرسائل أو البريد الإلكتروني لأيّ أحد، مهما كنتَ تثِق به.

02 لا تكتب كلمتك على ورقة مُلصَقة على الجهاز أو في مكان مكشوف.

03 عند إدخال الكلمة في جهاز عام، تأكَّدْ من عدم وجود برامج تتبُّع أو تسجيل.

04 إذا لاحظتَ أي محاولة دخول غَير طبيعية، غيِّرْ كلمة المرور فَوراً.

05 استخدِم أدوات الحماية مثل: التحقُّق بخطوتَين كلّما أمكن ذلك.

نصائح خاصة لإدارة كلمات المرور

يحتاج ذوو الإعاقة البصرية إلى تقنيّات وأســاليب مناســبة تساعدهم على حماية كلماتهم وتذكُّرها بطريقــة آمِنة، ومن أهم تلك الأســاليب ما يلي:

- اســتخدِمْ تطبيقات إدارة كلمات مرور تدعم القارئ الصَوتي أو طريقة برايل
- لا تعتمِد فقط على الحفظ العقلي، بل اســتخدِمْ أدوات تكنولوجية لحمايتها
- استشِــر شــخصاً تثِق به عند إعداد النظام، ثــمَّ حافِظْ علــى السرية بعد ذلك
- جرِّب اســتخدام التعرف على البصمة أو الوجه لتقليــل الاعتماد على الكتابة

ماذا تفعل إذا نسيتَ كلمة المرور؟

نسـيان كلمة المرور أمـر طبيعي، وهناك خطـوات آمِنة يمكـن اتّباعها لاسـتعادتها من أهمّها:

اسـتخدِمْ خيار (نسـيت كلمة المرور) الموجود في معظـم المواقع.

تأكَّد من أن بريـدك الإلكتروني أو رقم هاتفك محدَّث لاستلام رمز الاستعادة.

بعد اسـتعادة الوصول، أنشِـئ كلمـة مرور جديدة أقـوى من السـابقة

لا تسـتخدِمْ كلمـة الـمرور القديمـة إذا تمَّ اختراق الحسـاب

فكِّر فـي اسـتخدام برنامـج لحِفـظ كلمات الـمرور لتفادي النسـيان مسـتقبَلاً

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 هــو أول تصــرُّف يجِب أن تقــوم به عند الشَّــكّ في اختراق حســابك؟

أ. تَجاهُل الرسالة والانتظار

ب. مشاركة كلمة المرور مع صديق للمساعدة

ج. إنشاء حساب جديد فَوراً

د. تغيير كلمة المرور على الفَور

التصيُّد الاحتيالي

ما هو التصيُّد الاحتيالي؟

التصيُّـد الاحتيالـي هو محاولـة لخداعك من خلال رسـائل أو مواقع تبدو وكأنَّها حقيقية، لكنَّها مصمَّمة لسـرقة معلوماتك.

غالباً ما تأتي على شكل رسائل بريد إلكتروني أو رسائل نصيَّة مزيَّفة

تطلب منك إدخال بيانات حساسة، مثل: كلمات المرور أو أرقام البطاقات البنكية

تستخدِم 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 ماليّاً أو للابتزاز

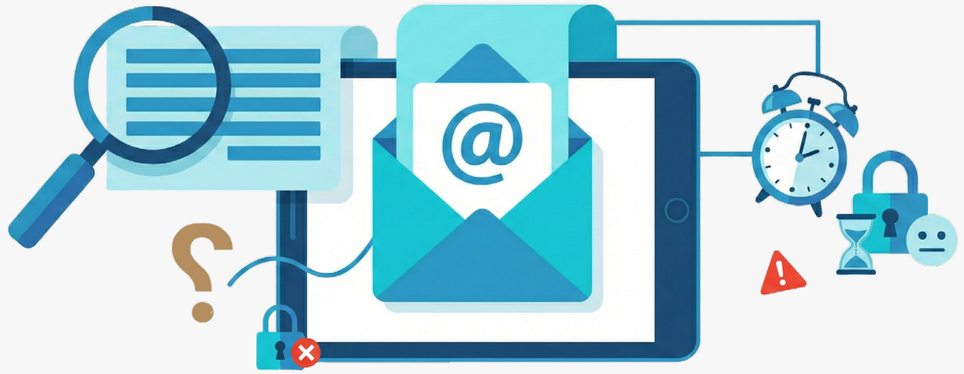
« ما أشكال التصيُّد الاحتيالي؟

تختلف طُرق التصيُّد، لكنَّها تشترك في محاولتها خداع المستخدِم للحصول على معلومات سرِّيَّة، 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 بَنْك.
- رسائل نصية قصيرة تطلب تأكيد بياناتك أو الضغط على رابط مشبوه.
- إعلانات وهمية تَعِدك بجوائز مقابل مِلء استبيانات أو إدخال رقم بطاقتك.

مؤشرات الرسائل الاحتيالية

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



01 وجــود أخطــاء لغويّــة أو إملائيــة غَير معتــادة في الرسالة.

02 عنــوان البريــد الإلكترونــي لا يتطابق مــع العنوان الرســمي للمؤسسة.

03 الروابط تبدو غريبــة أو غَير مألوفة، حتــى لو احتوَتْ على اســم جهة معروفة.

04 الرســالة تطلب معلومات شــخصية حسَّاســة بشكل مباشِر.

05 وجود تهديد أو اســتعجال لاتخاذ إجراء فَــوْريّ، مثل: (سيُغلَق حســابك خلال 24 ساعة).

الهندسة الاجتماعية

الهندسة الاجتماعية تعتمِد على استغلال المشاعر البَشرية لخداعك، بدلاً من استخدام أدوات تقنية مُعقَّدة.

01 يســتخدِم المهاجِم أســلوب الإقناع والتلاعب النَّفسي للحصول علــى معلوماتك.

02 قــد يتظاهر بأنــه موظَّــف دعم فنــي، أو صديــق، أو مسؤول.

03 يعتمِد على جمــع معلومات عنك مــن مواقع التواصل لجعلك تثِق به.

04 يســتغِل مشــاعر مثل: الخوف، أو التعاطــف، أو الحرج لدفعــك للتجاوب.

05 تُعد مــن أخطر الوســائل لأنَّهــا لا تحتاج إلــى مهارات تقنيــة، بل تعتمِــد على ســلوك الضحيَّة.

مخاطر شبكات Wi-Fi العامة

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

يمكن لأيّ شـخص متّصل بنفس الشـبكة التنصُّت علـى البيانات المرسَلة.

بعض المهاجمين يُنشـئون شـبكات باسم يشبه أسـماء الفنادق أو المقاهي لجَـذْب الضحايا.

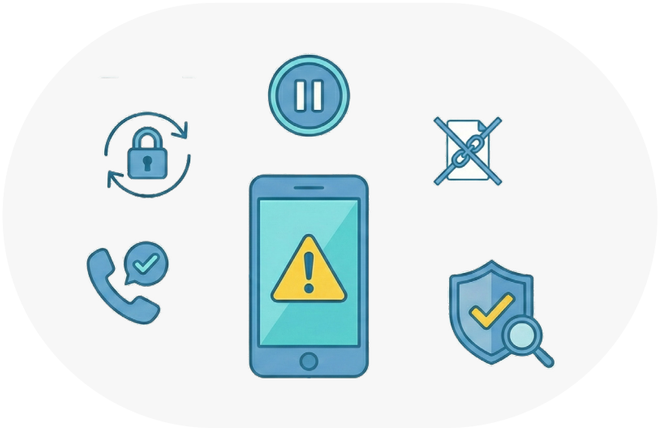
لا يُنصَح بإجراء معـاملات مالية أو إدخال كلمـات مرور في أثناء الاتصال بها.

غالباً ما تكون هذه الشـبكات غَير مُشـفَّرة؛ مما يسمح برؤية كل ما تُرسله.

يجِب اسـتخدام (VPN) عنـد الاضطرار لاسـتخدام شـبكة عامَّة؛ لحمايـة الاتصال.

التصرُّف الصحيح عند الشَّك بالاحتيال

إذا شعرتَ أن هناك شيئاً مريباً في رسالة أو موقع، يجِب أن تتوقَّف وتتأكد قبل التفاعل، وذلك باتباع الإرشادات الآتية:



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

تطبيقات وهمية للاحتيال

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

قد تطلــب أذونات غَير منطقيــة، مثل: الوصول إلى الرسائل أو الكاميرا

يمكنها التجسُّــس علــى المكالمات أو نَسْــخ البيانات الشــخصية

في بعض الحالات، تُستخدَم لتفعيل اشتراكات مدفوعة بدون عِلْمك

يجِــب تحميــل التطبيقــات فقط مــن المتاجر الرســمية، مثــل: Google Play أو App Store

اقرأ تقييمات المســتخدِمين، وراجِعْ عدد مرات التحميل قبــل التثبيت

الهجمات عبْر الإعلانات

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

قد تبــدأ بإعلان جذَّاب، مثــل: (اربح هاتفًــا جديدًا)، أو (احصل على وظيفــة أحلامك).

بمجــرد النقــر عليهــا، يتم تثبيــت برمجيات ضــارّة أو توجيهــك لموقــع مزيَّف.

بعض هــذه الإعلانات تظهــر في مواقــع معروفة، لكنهــا تأتي من شــركات غَيــر موثوقة.

لا تنقــر علــى الإعلانــات التــي تطلــب معلوماتك الشــخصية فوراً.

اســتخدِمْ إضافــات المتصفّــح التــي تمنــع الإعلانات المنبثقــة أو التتبُّع.

كيف تحمي نفسك من الاحتيال؟

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

01

لا تفتح أيّ رسالة إلكترونية أو رابط قبل التأكد من مصدره الحقيقي.

02

لا تُدخِلْ بياناتك الشخصية في مواقع لا تثق بها أو لا تبدأ بـ HTTPS.

03

فعِّل المصادقة الثنائية في جميع حساباتك، خاصَّةً البريد الإلكتروني والبنوك.

04

استخدِمْ برنامج حماية فعَّالًا، وحدِّثْه باستمرار.

05

إذا شعرت بالشكّ، استشِرْ خبيرًا أو تَواصَلْ مع الجهة المعنيَّة مباشرةً.

السؤال التفاعلي الثالث

عند تلقّي رسالة تُخبرك أنك ربحتَ جائزة وتطلب بياناتك، ماذا يجِب 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 لَونه أزرق

ب. أن يحتوي على صوَر جميلة

ج. أن يبدأ بـ (http)

د. أن يبدأ بـ (https) ويوجَد رمز القفل بجانبه

الهجمات السيبرانية والبرمجيات الخبيـــثة وطُـــرق الوقـــايـــة

ما هي الهجمات السيبرانية؟

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

01 قد يستهدف الأفراد أو الشركات أو المؤسسات الحكومية.

02 يهدف إلى سرقة البيانات، أو تخريب الأنظمة، أو طلب فدية مالية.

03 يتم غالبًا عبر الإنترنت، لكنّه قد يبدأ بوسائل بسيطة مثل رسالة بريد إلكتروني.

04 يمكن أن يؤدي إلى خسائر مالية كبيرة أو تسريب معلومات حسّاسة.

05 تشمل أنواع الهجمات: الفيروسات، التصيُّد، الفدية، والهندسة الاجتماعية.

الفيروسات

الفــيروس هو برنامــج ضــارّ يدخل إلى جهــازك ويُغيِّــر طريقة عملــه، أو يُتلف البيانــات الموجــودة عليه.

01 يُرفق غالبًا مع ملفات تبدو طبيعية مثل الصُّوَر أو المستندات.

02 يبدأ الفيروس بالانتشار عند فتح الملف أو تشغيله.

03 بعض الفيروسات تتسبَّب في حذف الملفات أو تعطيل النظام بشكلٍ كاملٍ.

04 ينتقل من جهازٍ إلى آخر عبر الإنترنت أو وسائط مثل USB

05 الحماية منه تكون عبر برامج مكافحة الفيروسات المُحدَّثة باستمرار.

ديدان الحاسوب

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

01 لا تحتاج الدودة إلى ملف لبدء نشاطها، بل تنتشر من خلال الشبكات أو البريد الإلكتروني.

02 تستهدف عادةً الأنظمة المتصلة ببعضها داخل المنزل أو الشركة.

03 يمكنها إبطاء سرعة الإنترنت أو الأجهزة بشدَّة.

04 بعض الديدان تُستخدَم كنقطة دخول لتثبيت برمجيات أخرى خطيرة.

05 الوقاية منها تتطلب تحديث الأنظمة وبرامج الحماية، خاصَّةً في الشبكات المفتوحة.

فيروس حصان طروادة

هـذا الفيروس يتنكَّر على شـكل برنامج مفيـد، لكنّـه فـي الحقيقـة يعمل على إيـذاء جهازك أو سـرقة معلوماتك.

01	يبدو وكأنه أداة مفيدة، مثل لعبة أو برنامج تنظيف الجهاز.
02	عند تشغيله، يفتح باباً خلَفيّاً يُتيح للمهاجم التحكُّم بجهازك.
03	لا يُظهِر نفسه بشكل واضح مما يُصعّب من اكتشافه.
04	يُستخدَم أحياناً لسرقة كلمات المرور أو مراقبة الشاشة.
05	الوقاية منه تكون بعدم تحميل البرامج من مواقع مجهولة أو روابط مشبوهة.

برمجيات الفــدية (Ransomware)

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

01 تُرسَل عادةً عبْر رسائل بريد إلكتروني تحتوي على مرفقات مزيَّفة.

02 بعد الإصابة، تُغلَق الملفات أو النظام بالكامل.

03 المهاجم يطلب فدية غالباً بعملة رقمية مثل البيتكوين.

04 حتى عند الدفع، لا يوجد ضمان لاسترجاع الملفات.

05 الحل الأفضل هو الوقاية، والنَّسْخ الاحتياطي المنتظِم، وعدم فتح المرفقات المشبوهة.

برمجيات التجسُّس (Spyware)

تعمـل هـذه البرمجيـات فـي الخفاء، وتُسـجِّل كل ما تفعله على الجهاز، بما في ذلك ضغطـات لوحـة المفاتيح.

01 تُرسِل معلوماتك للمهاجم، بما في ذلك كلمات المرور ورسائل البريد.

02 قد تراقِب الكاميرا أو الميكروفون دون إذنك.

03 يمكن أن تُبطئ الجهاز وتجعله يتصرّف بغرابة.

04 من الصعب ملاحظتها دون برنامج متخصّص.

05 استخدِمْ جدار حماية (Firewall)، ومضاد فيروسات قويّاً لاكتشافها.

الفرق بين الفيروسات وبرمجيات الفدية

كلاهما برمجيات ضارة، لكن يختلفان في طريقة التأثير والأسلوب.

1. الفيروس يهدف غالبًا إلى الإفساد أو التخريب العام للجهاز أو النظام.

2. برمجية الفدية تُركّز على حبس ملفاتك مقابل المال.

3. الفيروسات قد تعمل بصمتٍ، أما الفدية فتُظهر رسائل تهديد واضحة.

4. كلاهما ينتشر غالبًا من خلال روابط أو مرفقات مشبوهة.

5. كلاهما يمكن الوقاية منه من خلال التحديثات الدورية وبرامج الحماية.

كيف تَكتشف الإصابة ببرمجيات ضارة؟

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

01 بطء مُفاجِئ في الجهاز أو اســتهلاك أعلى للطاقة.

02 رســائل خطأ غريبــة أو اختفــاء بعض الملفات.

03 فتــح مواقــع تلقائيًّــا أو برامج تعمل دون إذنك.

04 تعــذُّر الوصــول إلــى ملفاتــك أو تغيير أســماء الملفــات بشــكل عشــوائي.

05 ظهــور رســالة تطلب فديــةً أو كلمة مرور لفتــح ملفَّاتك.

طرق الوقاية من البرمجيات الخبيثة

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

1 
لا تفتح مرفقات البريد الإلكتروني إلا إذا كنت تعرف المُرسِل.

2 
قُمْ بتحديث نظام التشغيل والتطبيقات بانتظامٍ.

3 
استخدِمْ برنامج مكافحة فيروسات مَوثُوق مع التحديث التلقائي.

4 
لا تقم بتوصيل أجهزة USB من مصادر غير معروفة.

5 
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.

01 يمكنك عمل نُسَخ احتياطية على قرص خارجي أو سحابة إلكترونية.

02 يجب أن تكون النُّسخة منفصلةً عن الجهاز الأساسي.

03 لا توصل القرص الاحتياطي بالإنترنت إلا عند النَّسخ فقط.

04 قم بالنَّسخ دوريًّا، أسبوعيًّا، أو شهريًّا بحسب أهمية الملفات.

05 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 تلقائيّاً

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 قُرص (USB) من صديق

د. تحديث البرامج وعدم فتح المرفقات المَشبُوهة

إجابات الأسئلة التفاعلية

01
إجابة السؤال التفاعلي الأول
د. Gt#9L@2m$P

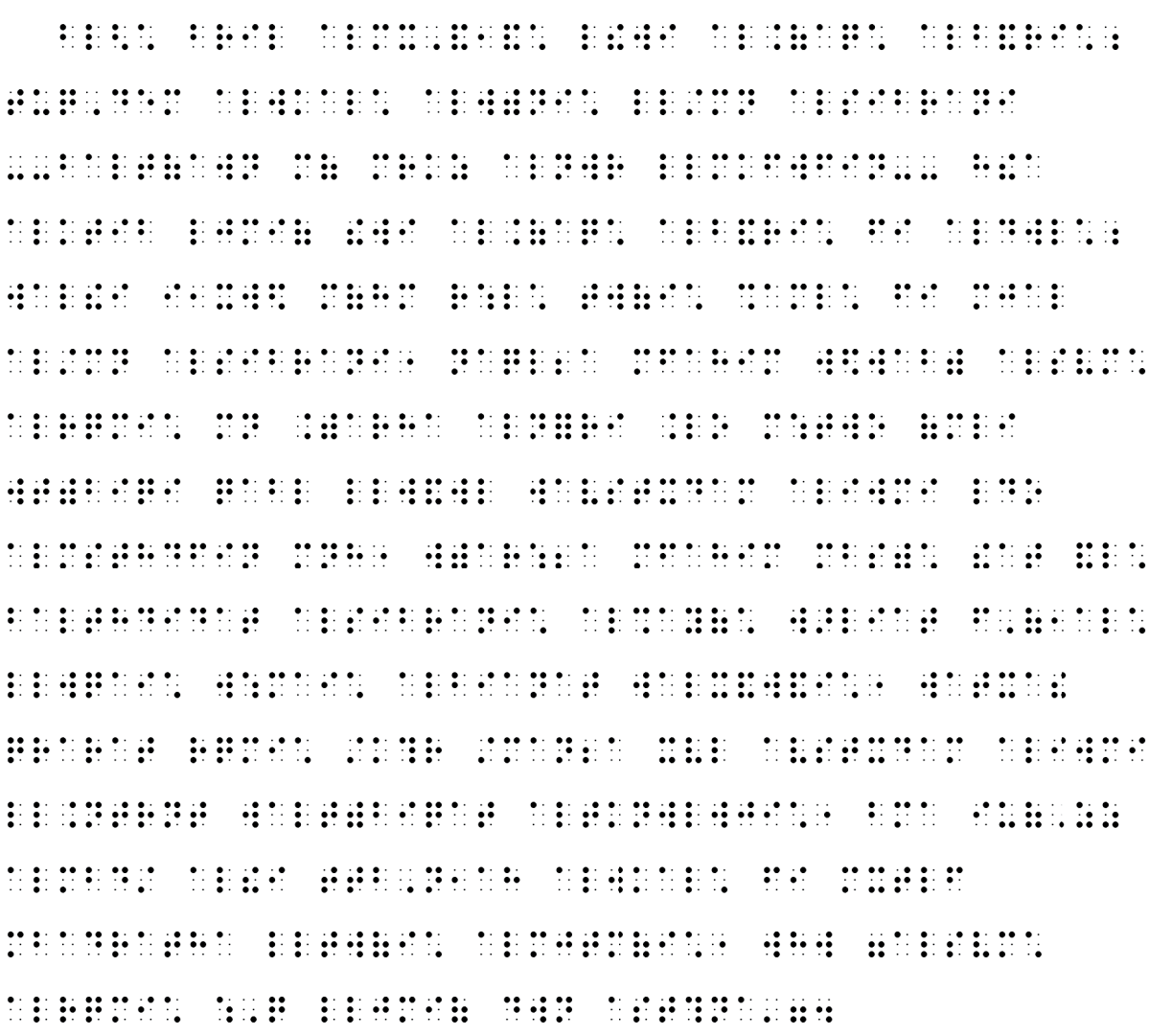
02
إجابة السؤال التفاعلي الثاني
د. تغيير كلمة المرور على الفَوْر

03
إجابة السؤال التفاعلي الثالث
ج. التحقُّق من مصدر الرسالة قبل أي تصرُّف

04
إجابة السؤال التفاعلي الرابع
د. أن يبدأ بـ https ويوجد رمز القفل بجانبه

05
إجابة السؤال التفاعلي الخامس
ج. تشفير الملفات، وطلب فدية مقابل استرجاعها

06
إجابة السؤال التفاعلي السادس
د. تحديث البرامج وعدم فتح المرفقات المشبوهة



بلغة بريل المخصَّصة لذوي الإعاقة البصرية؛ تُقدِّم الوكالة الوطنية للأمن السيبراني -بالتعاون مع مركز النور للمكفوفين- هذا الكتيب لجميع ذوي الإعاقة البصرية في الدولة؛ والذي يَخوض معهم رحلة توعية شاملة في مجال الأمن السيبراني، ناقلًا مفاهيم وضوابط السلامة الرقمية من إطارها النظري إلى محتوى عملي وتطبيقي قابل للوصول والاستخدام اليومي لدى المستهدفين منه، وطارحًا مفاهيم مبسطة ذات صلة بالتهديدات السيبرانية الشائعة وآليات فعَّالة للوقاية وحماية البيانات والخصوصية، واتخاذ قرارات رقمية أكثر أمانًا خلال الاستخدام اليومي للإنترنت والتطبيقات التكنولوجية، بما يُعزّز المبدأ الذي تتبنَّاه الوكالة في مختلف مبادراتها للتوعية المجتمعية، وهو "السلامة الرقمية حقّ للجميع دون استثناء".