

مخاطر الأمن السيبراني

حَقِيبَة خَاصَّة بِالْمُدَرِّب

شَرَايِح الْقَرْص



المرحلة الابتدائية

حقوق الملكية الفكرية

المادة مملوكة للوكالة الوطنية للأمن السيبراني في دولة قطر، وكافة حقوق الملكية الفكرية التي تشمل حق المؤلف وحقوق التأليف والنشر والطباعة، كلها مكفولة للوكالة الوطنية للأمن السيبراني في دولة قطر. وعليه، فجميع الحقوق محفوظة للوكالة، ولا يجوز إعادة نشر أي أجزاء من هذه المادة، أو الاقتباس منها، أو نسخ أي جزء منها، أو نقلها كلياً أو جزئياً في أي شكل وبأي وسيلة، سواءً بطرق إلكترونية أو آلية، بما في ذلك التصوير الفوتوغرافي، أو التسجيل، أو استخدام أي نظام من نظم تخزين المعلومات واسترجاعها سواءً من الأنظمة الحالية أو المبتكرة في المستقبل؛ إلا بعد الرجوع إلى الوكالة، والحصول على إذن خطي منها.

ومن يخالف ذلك يُعرض نفسه للمساءلة القانونية.

ديسمبر 2023م

الدوحة، قطر

هذا المحتوى إنتاج فريق

إدارة التميز السيبراني الوطني، الوكالة الوطنية للأمن السيبراني.

للاستفسار عن المبادرة أو البرنامج؛ يمكن التواصل عن طريق المواقع الإلكترونية أو الأرقام الهاتفية التالية:



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

🌐 <https://www.ncsa.gov.qa/>

✉ cyberexcellence@ncsa.gov.qa

☎ 00974 404 663 78

☎ 00974 404 663 62

التوزيع الزمني للورشة

المحتوى	الوقت المخصص
تمهيد	5 دقائق
الجزء النظري من المادة	25 دقيقة
عرض الفيديوهات التعليمية	25 دقيقة
استراحة قصيرة	20 دقيقة
تنفيذ الألعاب التدريبية	25 دقيقة
حوار ونقاش مع الطلبة	15 دقيقة
مشروع التخرج	5 دقائق
المدة الزمنية للورشة	ساعتان

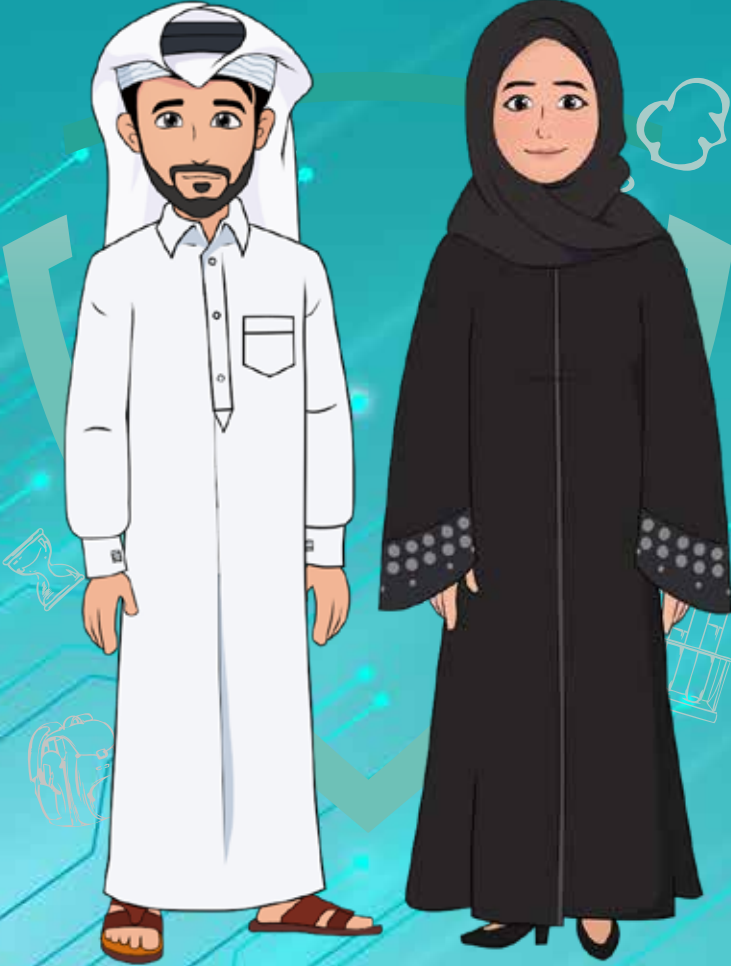
ما هو الأمان السيبرانيّ؟

هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التّشغيليّة، ومكوّناتها من أجهزة وبرامج، وما تُقدّمه من خِدَمات، وما تحويه من بيانات، من أيّ خرق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع.



أهمية الأمن السيبراني

يُعدّ الأمن السيبرانيّ من أهمّ الفروع الخاصة بالتكنولوجيا التي تهدف إلى حماية كافة المعلومات المهمة الخاصة بالأفراد والمؤسسات العامة والخاصة من الهجمات الإلكترونية التي تُؤدّي في النهاية إلى انتهاك خصوصية المؤسسات أو حتى الأفراد.



الجريمة الإلكترونية



هي شَكلٌ مُتطوِّر من أشكال الجريمة العابرة للحدود، التي تَحْدُث في مجال الفضاء الإلكتروني الذي لا حدود له، ويمكن لمُرتكبي الجرائم الإلكترونية وضحاياهم أن يكونوا في مناطق مختلفة، ويمكن أن تمتد آثار الجريمة عَبر المجتمعات في جميع أنحاء العالم.



أنواع الجرائم الإلكترونية



الاحتيال عبر البريد الإلكتروني والإنترنت.

تزوير الهوية

(حيث تتم سرقة المعلومات الشخصية واستخدامها).

سرقة البيانات المالية أو بيانات الدفع بالبطاقة.

سرقة بيانات الشركة وبيعها.

الابتزاز الإلكتروني

(طلب المال لمنع هُجُوم ضدَّ الأفراد أو المؤسسات).



< هجمات برمجيات الفدية (نوع من الابتزاز الإلكتروني).

< السرقة المشفرة (حيث يقوم المتسللون بتعدين العملات المشفرة باستخدام موارد لا يملكونها).

< التجسس الإلكتروني (حيث يتمكن المتسللون من الوصول إلى بيانات الأفراد والحكومات أو الشركات).

< التدخل في الأنظمة بطريقة تعرض الشبكة للخطر.

< انتهاك حقوق النشر.

< المقامرة غير المشروعة.

< بيع السلع غير المشروعة عبر الإنترنت.

الأخطاء الشائعة التي يقع فيها مُستخدِمُو الإنترنت

1

عدم مُتَابَعة أحدث التَّغْيِيرَات التي تُجْرِيهَا المواقع المختلفة لحماية المُسْتَحْدِمِينَ.

2

قَبُول طَلَبَات الصَّدَاقَةِ مِنْ أَشْخَاصٍ مَجْهُولِينَ أَمْرٌ خَطِرٌ؛ لِأَنَّهُ يُنْتِجُ لَهُمْ خَرَقَ خُصُوصِيَّتِكَ وَمَعْرِفَةَ مَعْلُومَاتِكَ الشَّخْصِيَّةِ.

3

تَجَاهُلُ تَحْدِيث أَنْظِمَةِ الْأَجْهَزةِ الذَّكِيَّةِ سِوَاءِ الْأَجْهَزةِ اللُّوْحِيَّةِ أَوْ الْهَوَاتِفِ مِمَّا يُعَرِّضُهَا لِعَشْرَاتِ الثُّغَرَاتِ الَّتِي قَدْ يَسْتَفْلُهَا مَخْتَرِقُو الْبَيَانَاتِ لِسَرْقَةِ الْبَيَانَاتِ وَخَرَقِ الْأَجْهَزةِ.

4

وَضْعُ كَلِمَاتٍ سِرٍّ مُتَشَابِهَةٍ لِجَمِيعِ الْحَسَابَاتِ الشَّخْصِيَّةِ.

5

الضَّغْطُ عَلَى أَيِّ رَابِطٍ غَيْرٍ مَعْرُوفٍ يَتَسَبَّبُ فِي خَرَقِ الْحَسَابَاتِ الشَّخْصِيَّةِ.

6

مُشَارَكَةُ الْمَعْلُومَاتِ الشَّخْصِيَّةِ.

كيفية التعامل مع خرق الحساب الشخصي على مواقع التواصل الاجتماعي



إذا كنت تشك في أن كلمة مرور حسابك على أحد مواقع التواصل الاجتماعي قد سُربت أو أن حسابك مُخترق؛ فعليك التصرف بسرعة؛ حيث يمكن للمتسللين من الدخول إلى حسابك وإزعاج أصدقائك وعائلتك، لذا يجب تأمين حسابك بسرعة، أو استعادته قبل فوات الأوان.

استخدام كلمة المرور لحماية البيانات

تؤدي كلمة المرور القويّة عدة وظائف هي:

03

منع أيّ شخص آخر من الدخول إلى حساباتك على الإنترنت مثل صفحات وسائل التواصل الاجتماعي.

02

حماية رسائلك الإلكترونية وملفاتك وبياناتك الأخرى.

01

الحفاظ على أمان بياناتك الشخصية.

كيف تُنشئ كلمة سرّ قويّة؟

ينبغي أن تتألّف كلمة المرور من أيّ مجموعة من الأحرف والأرقام والرّموز (أحرف ASCII العادية فقط)، ولا يمكن استخدام علامات تشكيل أو أحرف مُشكلة.



لا بُدَّ أن تتجنَّب الأمور التَّالية عند اختيار كلمة المرور:

- ❏ ضعيفة جدًا، مثل "password123".
- ❏ سبق واستخدمتها في حسابك.
- ❏ تبدأ أو تنتهي بمسافة فارغة.
- ❏ سهِّل تخمينها.
- ❏ استخدام كلمة مرور واحدة لجميع حساباتك المُهمَّة على الإنترنت.
- ❏ إعادة استخدام كلمات المرور في حساباتك المُهمَّة.
- ❏ تقلَّ عن 12 حرفًا.

عند إنشاء كلمة مرور يمكنك استخدام ما يلي:

< كلمات من أغنية أو قصيدة.

< مقولة مُميزة من فيلم أو خطاب.

< فقرة من كتاب.

< سلسلة كلمات ذات مَعْنَى بالنسبة إليك.

< اختصار: تكوين كلمة مرور من الحرف الأول من كُلِّ كلمة في جملة.



مع تجنب اختيار كلمات مرور يمكن توقعها أو تخمينها، من قبل أشخاص يعرفونك، أو استخدام معلومات قد يكون الآخرون على علم بها، أو يمكنهم الوصول إليها بسهولة، مثل:

اسم حيوانك الأليف.	لقبك أو الأحرف الأولى من اسمك.
اسم الشارع الذي تسكن فيه.	أعياد الميلاد أو السنوات المهمة لك.
رقم هاتفك.	أرقام من عنوانك.

الكلمات والعبارات والأنماط البسيطة مثل: <

أنماط لوحة المفاتيح، مثل
"qwerty" أو "qazwsx".

الأحرف أو الأرقام المتتالية
مثل "abcd" أو "1234".

الكلمات والعبارات الواضحة،
مثل "password".

حماية البريد الإلكتروني

من أهم الخطوات التي يجب عليك اتباعها:

- اختيار كلمة مرور قوية. <
- تفعيل ميزة "التحقق بخطوتين". <
- تغيير كلمات المرور بشكلٍ دوري. <
- استخدام كلمة مرور مختلفة لكل حساب. <
- تحديث البرامج الموجودة على الجهاز. <
- حظر مصدر البريد العشوائي ذي المحتوى المجهول. <
- تتبع رسائل البريد الإلكتروني المجهول. <



قواعد الاستخدام الآمن لشبكة الإنترنت

كُتابة كلمة مرور قويّة وتغييرها من حينٍ إلى آخر. <

تحميل الملفات والبرامج من المواقع الموثوقة. <

عدم نشر المعلومات الشخصية على الإنترنت. <

عدم فتح الإعلانات المُنبَثة على المواقع الإلكترونية. <

عدم استخدام الإنترنت لساعات طويلة. <

عدم فتح مُرَفَّقات البريد الإلكترونيّ الوارد من مجهولين. <

الحذر عند استخدام شبكة Wi-Fi عامّة. <



الاستخدام الطويل للإنترنت ومخاطر العزلة الاجتماعية

يؤدي الاستخدام الطويل لشبكة الإنترنت إلى المخاطر التالية:

تراجع العلاقات الأسرية والعلاقات الاجتماعية.

مشكلات صحية، مثل البدانة أو قلة الشهية وآلم المفاصل.

مشكلات نفسية، مثل الاكتئاب والقلق واضطراب النوم.

تراجع التحصيل الدراسي.

السلوك العدواني.



مخاطر قرصنة البيانات الشخصية

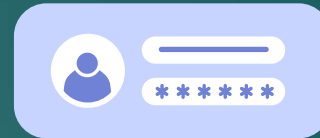
البيانات الشخصية هي رقم الهاتف وعنوان السكن واسم المدرسة وصور وأسماء أفراد العائلة، وغيره.

يعمل القراصنة الرقميون على سرقة البيانات الشخصية.

يتم استغلال البيانات الشخصية المسروقة لابتزاز الضحايا.

مشاركة المعلومات الشخصية على الإنترنت تسهل عملية قرصنتها.

لا تشارك أيًا من بياناتك الشخصية مع أي أحد كان.



مصادر المعلومات الموثوقة على الإنترنت

ليست كل المعلومات الموجودة على الإنترنت صحيحة ودقيقة.

تحتوي كثير من المواقع على معلومات مُضلّة أو غير دقيقة.

يجب الحصول على المعلومات من مصادر موثوقة.

المواقع الحكومية والمواقع الرسمية للشركات المعروفة تعدّ مصدرًا للمعلومات الموثوقة.



مخاطر وتحديات منصات التواصل الاجتماعي

- لِمنصات التواصل الاجتماعي إيجابيات شريطة أن نتعامل معها بوعي وحذر.
- يوجد العديد من المخاطر التي قد تواجهنا عند استخدام منصات التواصل الاجتماعي.
- من مخاطر منصات التواصل الاجتماعي:
 - سرقة البيانات الشخصية.
 - العزلة الاجتماعية.
 - الآثار النفسية، كالقلق والاكتئاب.
 - الأمراض الجسدية، مثل ضعف النظر.



المخاطر التي تُواجه الأجهزة الإلكترونية

التعرض للهجمات الإلكترونية.

سرقة البيانات المُخزنة على الأجهزة الإلكترونية.

الإصابة بالفيروسات.

يمكن حماية الأجهزة الإلكترونية من خلال ما يلي:

تثبيت برامج مُكافحة الفيروسات والبرمجيات الضارة.

تفعيل جدار الحماية.

عدم تحميل البرامج والملفات إلا من مواقع موثوقة.

استخدام كلمات مرور قوية وتغييرها بين الحين والآخر.





تمرين

صل بين العبارات في العمود الأول،
مع ما ينسجم معها في العمود الثاني.

توجيه

اقرأ الجمل الواردة بالجدول بدقة، ابدأ بالجُملة الأولى في العمود الأول، وابحث في العمود الثاني عن الجملة التي تستكمل معناها، أذناه مثال عن الوصل بين جُمْلَتَيْن.

- محاولات القرصنة وسرقة البيانات على المواقع الإلكترونية.
- حين تجلس لفترات طويلة على الإنترنت دون تعامل مع الآخرين.
- يؤدي إلى مشكلات أخلاقية ونفسية وعضوية.
- لأن الانفتاح على الثقافات الأخرى بدون ضوابط قد يؤدي إلى اكتساب ما هو غير مناسب لثقافتنا، ويتناقى مع معتقداتنا الدينية والثقافية.
- يؤدي إلى العزلة الاجتماعية.
- من الجرائم التي يعاقب عليها القانون.
- بالاكئاب ونوبات القلق والتوتر.

- ☐ الجلوس لأوقات طويلة على الإنترنت
- ☐ استخدام الإنترنت لأوقات طويلة يمكن أن يصيبك
- ☐ قد تتعرض لخرق الخصوصية من خلال
- ☐ خرق الخصوصية
- ☐ التعرض للمحتوى العنيف وغير المناسب للأطفال
- ☐ يمكنك أن تُصاب بإدمان الإنترنت
- ☐ يهدد الإنترنت الثقافة الوطنية

سؤال تفاعلي للمناقشة

◀ الإنترنت أداة تكنولوجيا نافعة في حال أحسنّا استخدامه، وقد يكون سبباً للمخاطر في حال عدم استخدامه بوعي.

ناقش مع زملائك ومُدربك أبرز المخاطر المرتبطة بالإنترنت،
لا سيّما في حال الإفراط في استخدامه.



CyberEco



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency