CyberEco

مَعًا لِدَعْمِ السَّلامَة الرَّقميّة

Together to support digital safety

مَخاطِر الأَمْن السّيبرانيّ

شرائح العَرْض

حَقِيبَة خاصَّة بالمُدَرِّب

المرحلة الابتدائيَّة

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

حُقُوق المِلْكِيَّة الفِكْرِيَّة

ديسمبر 2023م

الدوحة، قطر

هذا المحتوى إنتاج فريق

إدَارة التَّميُّز السّيبرانيّ الوَطنيّ، الوكالة الوطنيَّة للأَمْن السّيبرانيّ.

للاستفسار عن المُبادَرة أو البرنامج؛ يمكن التَّواصُل عن طريق المواقع الإلكترونيَّة أو الأرقام الهاتفيَّة التَّالية:

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

التَّوزيع الزَّمنيّ للوَرشَة

المحتوى	الوقت المُخصَّص
تمهيد	5 دقائق
الجُزْء النَّظريّ من المادَّة	25 دقيقة
عَرْض الفيديوهات التَّعليميَّة	25 دقيقة
استراحة قصيرة	20 دقيقة
تنفيذ الأَلْعَاب التَّدريبيَّة	25 دقيقة
حِوَار ونِقَاش مع الطَّلَبة	15 دقيقة
مَشروع التَّخرُّج	5 دقائق
المُدَّة الزَّمنيَّة للورشَة	ساعتان

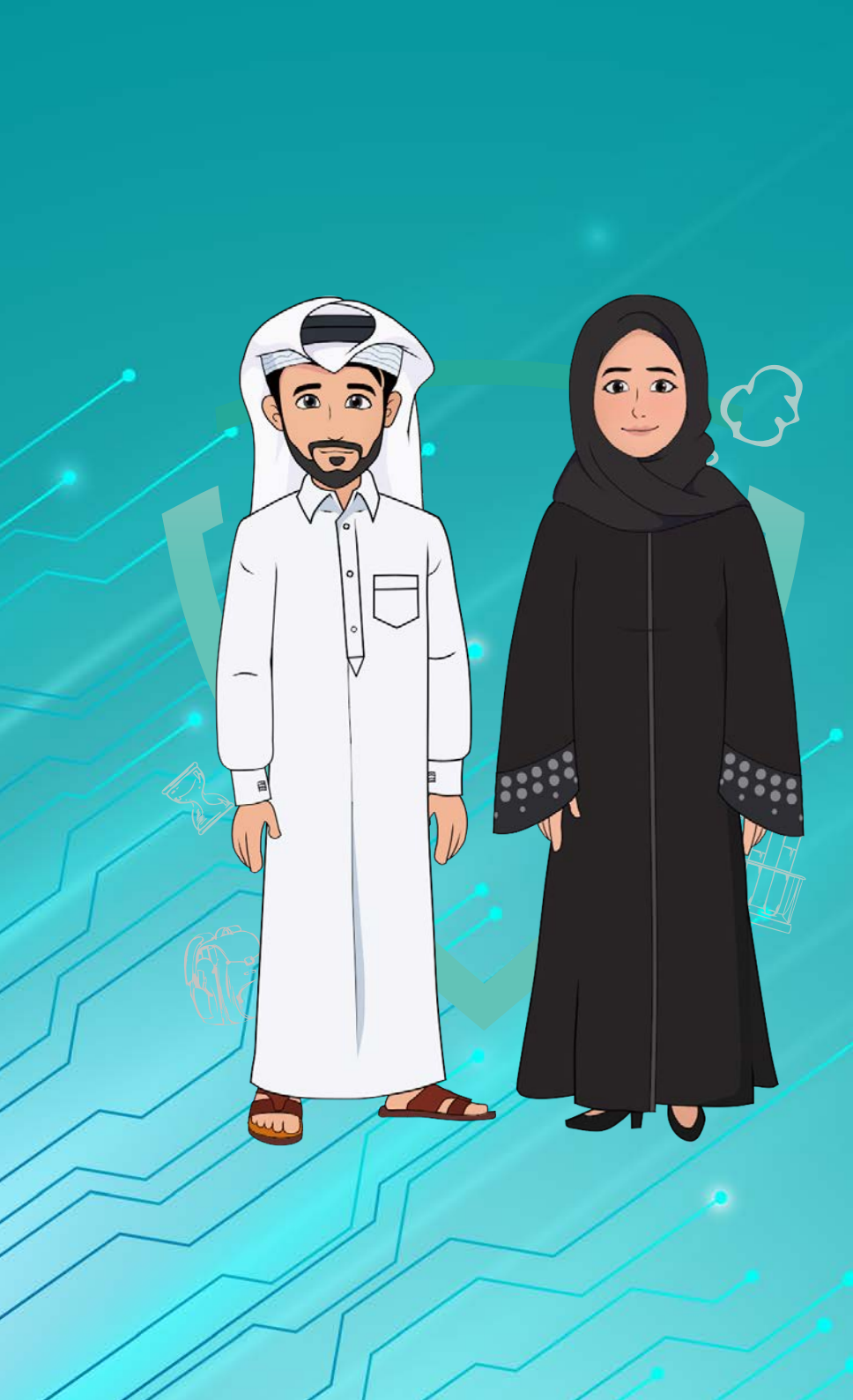
فهرس المحتوى العِلْمِيّ

الفَصْل الأَوَّل
مفهوم الأَمْن السّيبرانيّ والسَّلامَة الرَّقميَّة

مفهوم الأَمْن السّيبرانيّ؟

ما هو الأَمْن السّيبرانيّ؟

هو حماية الشَّبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التَّشْغيليَّة، ومكوّناتها من أجهزة وبرامج، وما تُقدّمه من خِدْمَات، وما تحتويه من بيانات، من أيّ خرق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع.



أهميَّة الأَمْن السّيبرانيّ

يُعدّ الأَمْن السّيبرانيّ من أهمّ الفروع الخاصَّة بالتكنولوجيا التي تهدف إلى حماية كافَّة المعلومات المُهمَّة الخاصَّة بالأفراد والمُؤسَّسَات العامَّة والخاصَّة من الهجمات الإلكترونيَّة التي تُؤدِّي في النهاية إلى انتهاك خصوصيَّة المُؤسَّسَات أو حتى الأفراد.

أنْوَاع الأَمْن السّيبرانيّ

هناك عدّة أنواع مختلفة من الأَمْن السّيبرانيّ، وهي فيما يلي

01

النَّوع الأوَّل

أمْن الشَّبكات
Network Security

02

النَّوع الثَّاني

الأمْن السّحابيّ
Cloud Security

03

النَّوع الثَّالث

أمْن التَّطبيقات
Application Security

04

النَّوع الرَّابع

الأمْن التَّشْغيليّ
Operational Security

خصائص ومُمَيِّزات الأَمْن السّيبرانيّ

01 حماية البيانات

تُسبِّب الهجمات الإلكترونيَّة قَلقًا كبيرًا للعديد من الأفراد والشَّركات؛ لذا يَتمّ الاستعانة بأدوات الأَمْن السّيبرانيّ للحفاظ على سِرِّيَّة كافَّة البيانات.

02 حماية المِلْكِيَّة الفكريَّة

هناك أنواع خاصَّة بحماية المِلْكِيَّة مثل: العلامة التجاريَّة, البيانات والأسرار الخاصَّة بالتجارة, حقوق النَّشْر, وغيرها.

خصائص ومُمَيِّزات الأَمْن السّيبرانيّ

03 الحماية من سرقة الأموال

يبحث مخترقو البيانات عن الثّغرَات التي يمكن من خلالها سرقة الأموال الخاصَّة بالمشروعات التّجاريَّة الصَّغيرة والكبيرة، وهنا تأتي الحاجة لتحديث البرامج واستخدام كلمات مرور قويَّة، وتشفير البيانات المُهمَّة.

04 الحماية من التَّجَسُّس

تزيد عمليات التَّجَسُّس من فُرَص سرقة البيانات الشَّخصيَّة وأرقام البطاقات الائتمانيَّة؛ نتيجةً للتَّعامُلات الشِّرائيَّة عبر الإنترنت، والتي إن لم يكن عليها غطاء أمني كافٍ يمكن خرق الأجهزة وسرقتها.

خصائص ومُمَيِّزات الأَمْن السّيبرانيّ

05 زيادة ثقة العملاء

من الأمور التي يُحقِّقها الأَمْن السّيبرانيّ زيادة ثقة العملاء بالمؤسَّسَات والشَّركات التي يتعاملون معها، بفَضْل حماية أنظمة الكشف عن الاختراقات والأنظمة الخاصَّة بمَنْع التَّطفُّل وتشفير بيانات العملاء السِّرِّيَّة.

06 حماية الأعمال

يساعد الأَمْن السّيبرانيّ في تصفُّح الإنترنت ومُمارَسة العمل بشكلٍ آمِن دون الخوف من التَّهْديدات المُحتَمَلة التي يمكن أن تحدث عَبْر شبكات الإنترنت.

خصائص ومُمَيِّزات الأَمْن السّيبرانيّ

07 حماية البيانات الشَّخصيَّة

يساعد الأَمْن السّيبرانيّ على حماية كافَّة البيانات الخاصَّة من السَّرِقَة أو التَّلاعُب بها؛ حيث يمنع خرق أيّ فيروس للأجهزة الإلكترونيَّة.

08 توفير الأمان والحفاظ على الإنتاجيَّة

عند خرق الفيروسات للأجهزة العاملة بالشَّركات والمُؤسَّسَات يَعُوق ذلك المُوظَّفين عن أداء عملهم، وأحيانًا قد يتوقَّف العمل بالكامل.

خصائص ومُمَيِّزات الأَمْن السّيبرانيّ

09 حماية المواقع الإلكترونيَّة

يعتمد عددٌ كبيرٌ من الشَّركات والمُؤسَّسَات على المواقع الإلكترونيَّة لجَذْب العملاء، وللحفاظ على سُمْعتهم الطَّيِّبَة يعتمدون على برامج حماية تَمْنَع الاختراقات أو تعطيل العمل بالموقع في حال دخول أيّ فيروس.

10 استعادة البيانات المُسرَّبة

لا تقتصر مَهمَّة الأَمْن السّيبرانيّ فقط على الحفاظ على البيانات، بل من ضمن فوائده أنه يساعد في استرجاع البيانات التي تمّت سرقتها وتسريبها في أسرع وَقْتٍ.

الفَـــــرْق بيـــــن
أَمْـن المَعْلُومَـــات
والأَمْـــن السّيبرانـيّ

أَمْن المَعْلُومَات

يهتمّ بالحفاظ على سرِّيَّة المعلومات والبيانات التي يقوم مُستخدِم الإنترنت برَبْطها ببعض مواقع التَّواصُل الاجتماعيّ والمِنَصَّات الإلكترونيَّة من أيّ محاولة خرق أو تجسُّس إلكترونيّ.

ما هي أنواع أَمْن المَعْلُومَات الأساسيَّة؟

01 أنظمة حماية البرامج والتَّطبيقات.

02 أنظمة حماية نظام التَّشْغيل.

03 أنظمة حماية الدُّخُول والخروج للتَّطبيقات.

04 أنظمة حماية البرمجيَّات والإلكترونيَّات.

المَخَاطِر التي يتعامل معها أَمْن المَعْلُومَات

01

استخدام تقنيات وأجهزة ذات مُعامِل أمانٍ مُنْخَفِضٍ.

02

مشكلات في التَّشْفِير.

03

وجود تَلف في البيانات؛ سواءٌ الرَّقميَّة أم غير الرَّقميَّة.

04

الاعتماد على برنامج أمانٍ ضعيفٍ أو غير مُطوَّر خاصَّةً عند التَّعامُل مع البيانات الضَّخْمَة.

ما هي المبادئ الأساسيَّة لأَمْن المَعْلُومَات؟

01 السِّرِّيَّة

02 عدم التَّنصُّل والإنكار

03 الأصالة

04 المُساءَلة

05 السَّلامة أو النَّزاهَة

06 إتاحة المعلومات

أهم الإجراءات التي يَستخدمها مُتخَصِّصو أَمْن المَعْلُومَات

01 تقوية كلمة المرور

02 مُصادَقة ثنائيَّة أو مُتَعَدِّدَة العوامل؛ مثل رَبْط الموقع الإلكترونيّ بالهاتف

03 إمكانيَّة التَّحكُّم في صلاحيَّة الوصول إلى البيانات

04 التَّشْفِير

05 المسؤوليَّة القانونيَّة

06 الوَعْي الثَّقافيّ

أوجه التَّشابُه بين الأَمْن السّيبرانيّ وأَمْن المَعْلُومَات

يتشابه مجالا أَمْن المَعْلُومَات والأَمْن السّيبرانيّ من حيث الاهتمام بأَمْن المَعْلُومَات الإلكترونيَّة أو السّيبرانيَّة.

يهتمّ الأَمْن السّيبرانيّ بأَمْن كُلّ ما هو موجود في الفضاء السّيبرانيّ بما في ذلك أَمْن المَعْلُومَات، بينما يهتمّ مجال أَمْن المَعْلُومَات بالحفاظ على المعلومات، حتى لو كانت على الإنترنت.

ما الفَـــــرْق بيـــــن
أَمْـن المَعْلُومَـــات
والأَمْـــن السّيبرانـيّ؟

أَمْن المَعْلُومَات

- يحفظ أَمْن المَعْلُومَات جميع بياناتك عند المُوافَقة على شروط استخدام التَّطبيق الإلكترونيّ.
- يكون أَمْن المَعْلُومَات عُرْضَة للخرق عند استخدام أنظمة التَّجَسُّس والقَرْصَنَة والفيروسات.
- يمكن لأَمْن المَعْلُومَات إبلاغك بمحاولة خرق إلكترونيّ لإحدى مِنَصَّاتك أو البيانات التي تمتلكها.
- ينتهي دور أَمْن المَعْلُومَات إذا توقَّف المُسْتَخْدِم عن السَّماح باستخدام معلوماته التي يُوفِّرها في بداية استخدام التَّطبيق.
- يمكن لأَمْن المَعْلُومَات حماية صُوَر وبيانات الأشخاص المُصنّفين علنًا على مواقع الشَّبكات الاجتماعيَّة للمُستخدِم.

الأَمْن السّيبرانيّ

- يمنع التَّطبيق نفسه من التَّجَسُّس عليك وابتزازك وتتبُّعك.
- هو نظام إلكترونيّ يحمي الأجهزة نفسها ومُوجِّهات التَّجَسُّس على الإنترنت من تلقّي أيّ نَوْع من الفيروسات.
- يمكنه تتبُّع المُتَسَلِّل الإلكترونيّ، ومعرفة هُويّته الشَّخصيَّة وجَمْع معلومات عنه.
- يمكن للأمن السّيبرانيّ تحديد موقع المُسْتَخْدِم ونشاطه وتَفاعُله مع البيئة الخارجيَّة؛ من خلال الاتِّصال بأكثر من مِنَصَّة رقميَّة واحدة.
- يُساعِدُك في الوصول إلى جميع البيانات وجميع الهويات التي تَصل إلى بياناتك بشكلٍ قانونيّ أو غير قانونيّ.

الفَصْل الثَّاني
المَخَاطِر المُرْتَبِطَة بالأَمْن السّيبرانيّ

الجرائم الإلكترونيَّة (مَخَاطِر الإنترنت)

الجريمة الإلكترونيَّة

هي شَكْل مُتطوِّر من أشكال الجريمة العابرة للحدود، التي تَحْدث في مجال الفضاء الإلكترونيّ الذي لا حدود له، ويمكن لمُرتكبي الجرائم الإلكترونيَّة وضحاياهم أن يكونوا في مناطق مختلفة، ويمكن أن تمتدّ آثار الجريمة عَبْر المجتمعات في جميع أنحاء العالَم.

أنواع الجرائم الإلكترونيَّة

- الاحتيال عبر البريد الإلكترونيّ والإنترنت.
- تزوير الهُوِيَّة
  (حيث تتمّ سرقة المعلومات الشَّخصيَّة واستخدامها).
- سرقة البيانات الماليَّة أو بيانات الدَّفْع بالبطاقة.
- سرقة بيانات الشَّركة وبَيْعها.
- الابتزاز الإلكترونيّ
  (طلب المال لمَنْع هُجُوم ضدّ الأفراد أو المؤَسَّسَات).

- هجمات برمجيَّات الفِدْيَة (نَوْع من الابتزاز الإلكترونيّ).
- السَّرِقَة المُشَفَّرَة (حيث يقوم المُتَسَلِّلون بتَعْدين العُملَات المُشَفَّرَة باستخدام موارد لا يملكونها).
- التَّجَسُّس الإلكترونيّ (حيث يَتمكَّن المُتَسَلِّلون من الوصول إلى بيانات الأفراد والحكومات أو الشَّركات).
- التَّدخُّل في الأنظمة بطريقة تُعرِّض الشَّبكة للخطر.
- انتهاك حُقُوق النَّشْر.
- المُقامَرَة غير المشروعة.
- بيع السِّلع غير المشروعة عبر الإنترنت.

الجرائم الإلكترونيَّة تشمل أمرين؛ هما:

- نشاط إجراميّ يستهدف أجهزة الحاسوب باستخدام الفيروسات وأنواع أخرى من البرمجيات الخبيثة.
- نشاط إجراميّ يستخدم أجهزة الحاسوب لارتكاب جرائم كالابتزاز.

طريقة عمل مخترقي البيانات

يُصيب مُرْتَكِبُو الجرائم الإلكترونيَّة "السّيبرانيَّة" أجهزة الحاسوب المُستهدَفة ببرمجيَّة خبيثة لإتلاف الأجهزة أو إيقافها عن العمل، وقد يستخدمون تلك البرمجيَّة الخبيثة في حَذْف البيانات أو سرقتها.

وغالبًا ما يفعل مُرْتَكِبُو الجرائم الإلكترونيَّة الأمرين في الوقت نفسه، فَهُم يَستهدفون أجهزة الحاسوب التي تحتوي على فيروسات أولًا، ثمَّ يستخدمونها لنَشْر البرمجيَّات الخبيثة على أجهزة أخرى أو عَبْر الشَّبكة.

الأخطاء الشَّائعة التي يقع فيها مُسْتَخْدِمُو الإنترنت

1. وَضْع كلمات سِرّ مُتشابهة لجميع الحسابات الشَّخصيَّة.
2. عدم مُتابَعة أحدث التَّغييرات التي تُجريها المواقع المختلفة لحماية المُسْتَخْدِمين.
3. تَجاهُل تحديث أنظمة الأجهزة الذَّكيَّة سواءٌ الأجهزة اللوحية أو الهواتف ممَّا يُعرِّضها لعشرات الثّغرات التي قد يَستغلّها مخترقو البيانات لسرقة البيانات وخرق الأجهزة.
4. الضَّغْط على أيّ رابط غير معروف يتسبَّب في خرق الحسابات الشَّخصيَّة.
5. قَبُول طَلَبات الصَّداقة من أشخاص مجهولين أمرٌ خَطِر؛ لأنَّه يُتيح لهم خرق خصوصيَّتك ومعرفة معلوماتك الشَّخصيَّة.
6. مُشارَكة المعلومات الشَّخصيَّة.

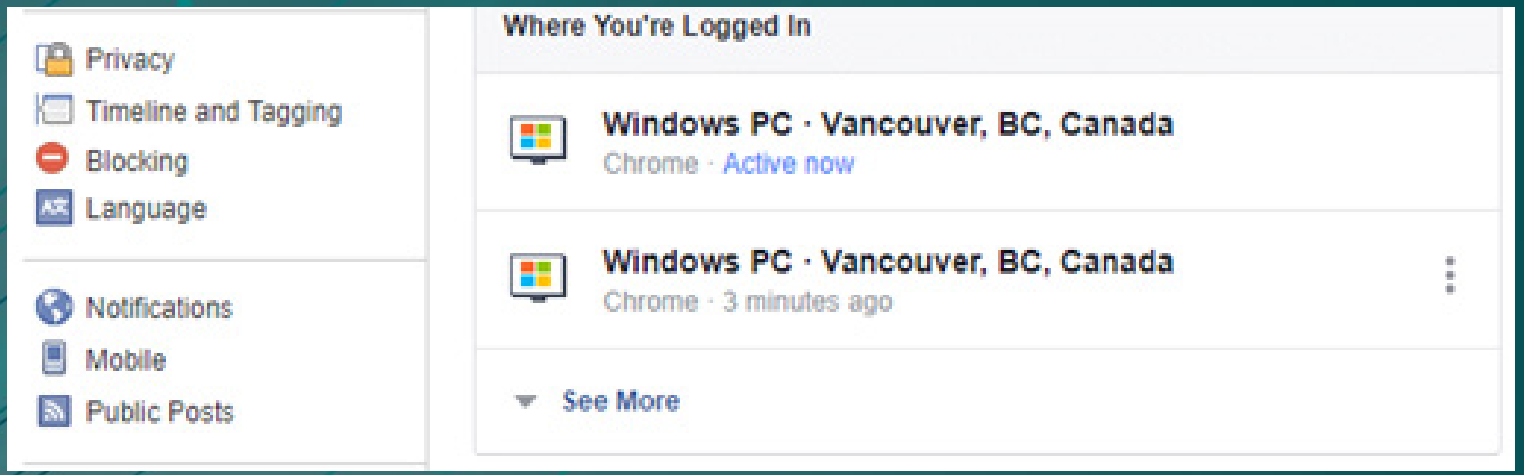
كيفيَّة التَّعامُل مع خرق الحساب الشَّخصيّ على مواقع التَّواصُل الاجتماعيّ

إذا كنتَ تشكّ في أنَّ كلمة مرور حسابك على أحد مواقع التَّواصُل الاجتماعيّ قد سُرِّبت أو أن حسابك مُخْتَرَق؛ فعليك التَّصرُّف بسرعةٍ؛ حيث يُمكن للمُتَسَلِّلين مَنْعُك من الدُّخُول إلى حسابك وإزعاج أصدقائك وعائلتك، لذا يجب تأمين حسابك بسرعةٍ، أو استعادته قبل فَوات الأوان.

كيف تعرف أنَّ حسابك مُخْتَرَق؟

إذا تمكَّن أحد المُتَسَلِّلين من الدُّخُول إلى حسابك على أحد مَواقع التَّواصُل الاجتماعيّ؛ فسوف يترك أثرًا، ويمكن معرفة ذلك من خلال:

- انْقُر على السَّهم في الجزء العُلْوِيّ الأيمن.
- من القائمة، اخْتَرْ (الإعدادات) Settings.
- انْتَقِلْ إلى (الأمان وتسجيل الدُّخُول) Security and Login.
- في الجزء العُلْوِيّ، سترى قائمة بالأجهزة التي قُمتَ من خلالها بتسجيل الدُّخول إلى حسابك خلال الفترة الأخيرة؛ ومتى كانت نَشِطة.
- انْقُر على (عَرْض المزيد) See More، لفتح تلك القائمة ومُراجعة الجلسات القديمة.



إذا لاحظتَ أيّ نشاطٍ مُرِيب في تسجيلات الدُّخُول الخاصَّة بك، فعليكَ القيام بالآتي:

- تغيير كلمة المرور
- الإبلاغ عن الاختراق
- إزالة التَّطبيقات المشكوك فيها
- التَّحكُّم في الضَّرر

أخْبِر أصْدِقاءَك وعائلتك بما حدَث، وإذا لم تتمكَّن حاليًّا من الوصول إلى حسابك، فاتَّصِل بأصدقائك في Facebook من خلال مواقع التَّواصُل الاجتماعيّ الأخرى، أو عَبْر البريد الإلكترونيّ، أو اطْلُب من صديق مُشتَرك إبلاغهم عبر Facebook.

كيف أحمي نفسي من الجرائم الإلكترونيَّة؟

1. إبقاء البرنامج ونظام التَّشْغيل مُحدَّثَيْن
2. استخدام برنامج مُكَافَحَة الفيروسات وتحديثه باستمرار
3. استخدام كلمات مرور قويَّة
4. تَجاهُل المُرفَقات في رسائل البريد الإلكترونيّ العشوائيَّة
5. الاتِّصال بالشَّركات مُباشَرةً بشأن الطَّلبات المريبة
6. الامتناع عن تقديم المعلومات الشَّخصيَّة إلا إذا كنت آمنًا
7. عدم فَتْح الرَّوَابِط
8. التَّنَبُّه لعناوين مواقع URL التي تزورها

كيف نَتَعامل مع الإساءة عبر مواقع التَّواصُل الاجتماعيّ؟

(التَّنَمُّر عبر الإنترنت)

ما هو التَّنَمُّر عبر الإنترنت؟

- التَّنَمُّر عَبْر الإنترنت هو التَّنَمُّر باستخدام التّقنيات الرَّقميَّة.
- سلوك مُتكرّر يهدف إلى تخويف الأشخاص المُستهدَفين أو إغضابهم أو التَّشهير بهم.

أمثلة على التَّنَمُّر عبر الإنترنت

- نَشْر الأكاذيب أو نَشْر صُور مُحْرِجَة لشَخْص ما على وسائل التَّواصُل الاجتماعيّ.
- إرسال رسائل أو صُوَر أو مقاطع فيديو مُؤذية أو مُسيئة أو تهديدات عبر مِنَصَّات التَّراسُل.
- سرقة هُوِيَّة أحدٍ ما وتوجيه رسائل مسيئة للآخرين باسمه أو من خلال حسابات وَهْميَّة.

كيف نُمَيِّز بين المِزَاح والتَّنَمُّر عبر الإنترنت؟

من عادة الأصدقاء أن يَمْزَحُوا مع بعضهم، ولكن في حال أحْزَنَتْكَ الكلمات أو كنتَ تَعتقد أن الشَّخص الآخر يَضْحك عليك بدلًا من أن يَضْحك معك؛ فحينها تكون المزحة قد تجاوزتَ حُدودها، وتصبح تَنمُّرًا.

كيف نَتعامَل مع التَّنَمُّر عَبْر الإنترنت؟

1. التَّحدُّث إلى شخصٍ تثق به من قبيل صديقٍ أو فردٍ من الأسرة أو مُرشِد اجتماعيّ في المدرسة، أو شخصٍ بَالِغ آخر تَثِق به.

2. إذا كان التَّنَمُّر يحدث عبر وسائل التَّواصُل الاجتماعيّ، قمْ بحَجْب الشَّخص الذي يمارس التَّنَمُّر والإبلاغ عن سلوكه إلى موقع التَّواصُل الاجتماعيّ المعنيّ.

3. جَمْع أدِلَّة مثل رسائل نَصِّيَّة أو صورة تتضمَّن المَوادّ المسيئة المنشورة عبر مواقع التَّواصُل الاجتماعيّ ضدّك والإبلاغ عنها.

4. فَكِّر مَرتين قبل أن تنشر أو تشارك أيّ شيء على شبكة الإنترنت؛ فقد يظل موجودًا على الإنترنت إلى الأبد، ويمكن أن يُستخدَم لإيذائك لاحقًا.

5. لا تُعطِ أيّ تفاصيل شخصيَّة من قبيل عنوانك أو رقم هاتفك أو اسم مَدرستك.

6. تعرَّف على إعدادات الخصوصيَّة على تطبيقات التَّواصُل الاجتماعيّ المُفضَّلة لديك.

الفَصْل الثَّالث

كيف أحمي نفسي من التَّهْديدات الرَّقميَّة؟

استخدام كلمة المرور لحماية البيانات

تؤدي كلمة المرور القويَّة عدة وظائف هي:

01

الحفاظ على أمان بياناتك الشَّخصيَّة.

02

حماية رسائلك الإلكترونيَّة وملفَّاتك وبياناتك الأخرى.

03

منع أيّ شخص آخر من الدُّخُول إلى حساباتك على الإنترنت مثل صفحات وسائل التَّواصُل الاجتماعيّ.

كيف تُنْشِئ كلمة سِرّ قويَّة؟

ينبغي أن تتألَّف كلمة المرور من أيّ مجموعة من الأحرف والأرقام والرُّمُوز (أحرف ASCII العاديَّة فقط)، ولا يمكن استخدام علامات تشكيل أو أحرف مُشكلة.

لا بُدّ أن تتجنَّب الأمور التَّالية عند اختيار كلمة المرور:

- ضعيفة جدًّا، مثل "password123".
- سبق واستخدمتها في حسابك.
- تبدأ أو تنتهي بمسافة فارغة.
- سَهْل تَخْمينها.
- استخدام كلمة مرور واحدة لجميع حساباتك المُهمَّة على الإنترنت.
- إعادة استخدام كلمات المرور في حساباتك المُهمَّة.
- تقلّ عن 12 حرفًا.

عند إنشاء كلمة مرور يمكنك استخدام ما يلي:

- كلمات من أغنيَّة أو قصيدة.
- مَقُولة مُميَّزة من فيلم أو خِطَاب.
- فقرة من كِتَاب.
- سلسلة كلمات ذات مَغْزى بالنِّسبة إليك.
- اختصار: تكوين كلمة مرور من الحرف الأول من كُلّ كلمة في جملة.

مع تجنُّب اختيار كلمات مرور يمكن تَوقُّعها أو تَخْمينها، من قِبَل أشخاص يعرفونك، أو استخدام معلومات قد يكون الآخرون على عِلْم بها، أو يمكنهم الوصول إليها بسهولةٍ، مثل:

- لَقَبك أو الأَحْرُف الأُولَى من اسمك.
- اسم حيوانك الأليف.
- أعياد الميلاد أو السَّنوات المُهمَّة لك.
- اسم الشَّارع الذي تسكن فيه.
- أرقام من عنوانك.
- رقم هاتفك.

الكلمات والعبارات والأنماط البسيطة مثل:

- الكلمات والعبارات الواضحة، مثل "password".
- الأحرف أو الأرقام المُتتابِعَة مثل "abcd" أو "1234".
- أنماط لوحة المفاتيح، مثل "qwerty" أو "qazwsx".

حماية البريد الإلكترونيّ

من أهمّ الخطوات التي يجب عليك اتّباعها:

- اختيار كلمة مرور قويَّة.
- تفعيل ميزة "التَّحقُّق بخُطْوَتَيْنِ".
- تغيير كلمات المرور بشكلٍ دَوْريّ.
- استخدام كلمة مرور مختلفة لكل حساب.
- تحديث البرامج الموجودة على الجهاز.
- حَظْر مَصْدر البريد العشوائيّ ذي المحتوى المجهول.
- تَتبُّع رسائل البريد الإلكترونيّ المجهول.

وللقيام بذلك في Gmail اتَّبع الخطوات التَّالية

1

افْتَح حساب Gmail الخاصّ بك باستخدام أيّ مُتصفِّح.

2

افْتَح رسالة البريد الإلكترونيّ التي تريد تَتبُّعها.

3

انْقُر فوق رمز المزيد (⋮) بجوار كلمة "ردّ"، الموجود في الزَّاوية العُلويَّة من الرِّسَالة.

4

حدِّد على "عَرْض النُّسخة الأصليَّة" من القائمة.

5

سيتمّ فَتْح نافذة جديدة تحتوي على معلومات الرِّسَالة الأصليَّة؛ بما في ذلك: نتائج المُصادَقَة، وعنوان "أي بي" (IP) الخاصّ بالمُرسِل، وتاريخ الإنشاء ورَقْم تعريف الرِّسَالة.

ولتَتبُّع رسائل البريد الإلكترونيّ في خِدْمَات البريد الأخرى من خلال التَّالي:

01

في Outlook:
انْقُر على "ملفّ"، ثمَّ على "الخصائص".

02

في Hotmail:
انْقُر بزِر الماوس الأيمن على الرِّسَالة الإلكترونيَّة، ثم حدِّد "عرض مصدر الرِّسَالة".

03

في Apple Mail:
انْقُر على "عرض"، ثم "الرِّسَالة"، وحدِّد على "جميع العناوين".

04

في Yahoo:
انْقُر على "المزيد"، ثمّ حَدِّد على "عرض الرِّسَالة الأصليَّة".

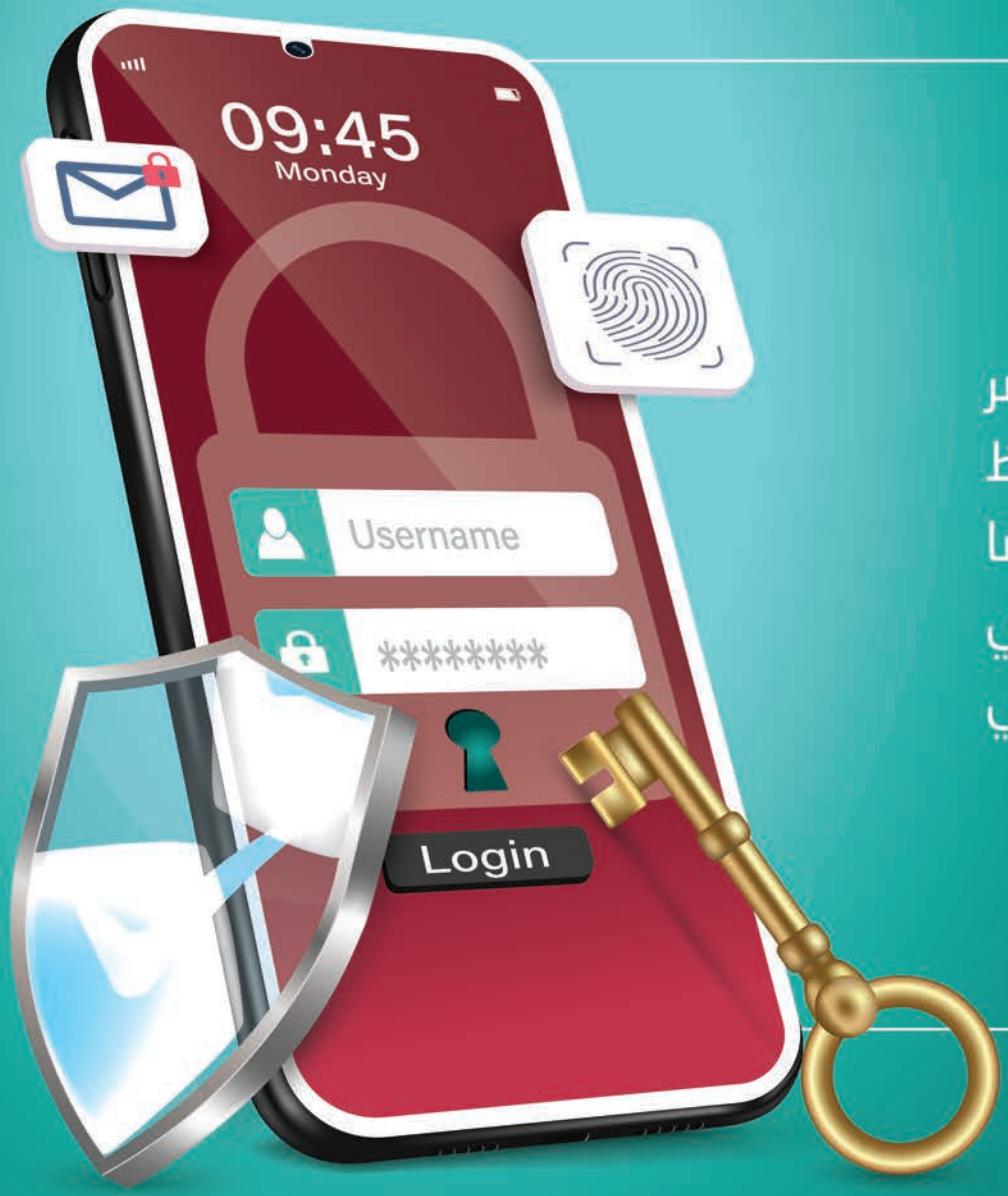
ماذا أفعل عند تَعرُّضي للتَّهديدات الرَّقميَّة؟

في حال تَعرُّضك للابتزاز الإلكترونيّ... عليك بالآتي:

- لا تُحاوِل الرَّدّ على الشَّخص المُبتَزّ أو إقناعه بعدم نَشْر معلوماتك وصُوَرك الشَّخصيَّة؛ فهذا يُعْطِي انطباعًا بأنَّك ضَعْيف أو مُستجِيب لمَطَالبهم، ما يَدْفعهم إلى زيادتها أو التَّحقُّق من صِحّتها
- قُمْ بتخزين المحتوى الذي تمَّ ابتزازك به، مع عدم حَذْف رسائل التَّهْديد؛ فهي دليلٌ يمكن استخدامه لإدانة المُجْرِمين
- وَقْف متابَعَة المُبتزّ لحساباتك على مواقع التَّواصُل الاجتماعيّ، وتغيير كلمات المرور الخاصَّة بك على الفَوْر، فيُفضَّل استخدام كلمات مرور مختلفة تتضمَّن أرقامًا وحروفًا ورموزًا لحساباتك المُتنوّعة
- أخْبِر شخصًا موثوقًا بما حدَث لك مثل الأب أو الأم أو مُشْرفك في المدرسة؛ لتزويدك بالدَّعْم النَّفسيّ، كما يُفضَّل طَلَب الدَّعْم النَّفسيّ من مُتخصِّصين؛ كي لا يُؤثِّر الابتزاز في صِحّتك العقليَّة والنَّفْسيَّة
- تواصل مع إدارة مكافحة الجرائم الإلكترونيَّة بوزارة الدَّاخليَّة.

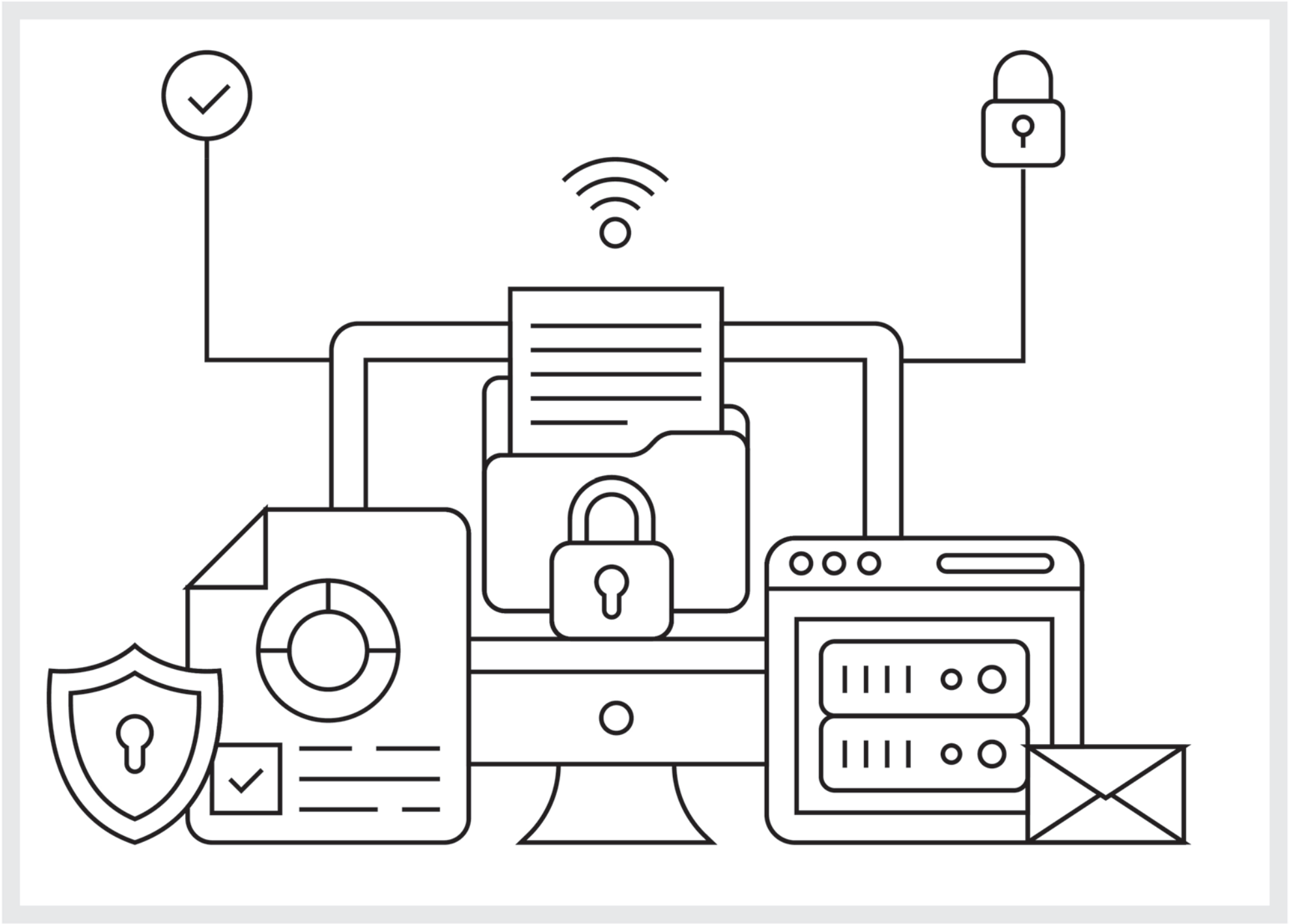
تمارين وتَدْريبَات

أولًا: التَّمَارين الصَّفيَّة



هل تعلم؟

الأَمْن السّيبرانيّ لا تَقتصر مَهمّته فقط على الحِفَاظ على البيانات، بل يساعد أيضًا في استرجاع البيانات التي تمَّت سَرقتها وتَسريبها في أسرع وقتٍ.



التَّمرين الأَوَّل

ضَعْ علامة (✓) أمام العبارة الصحيحة، أو علامة (✗) أمام العبارة الخاطئة:

1. الأَمْن السّـيبرانيّ هو حمـــاية الأجهـزة والشَّبكات والتَّطبيقات من المَخَاطِر الرَّقميَّة.
2. لا تتحمَّـــل المُؤسَّسَـات مسـؤوليَّة تـأمين البيانات الخاصَّة بها أو بالعملاء المُتعامِلين معها.
3. حماية البيانات تَخْلق ثقةً بين المُؤسَّسَة والعملاء المُتعامِلين معها.
4. لا بُدَّ من اتِّخاذ تدابير وأدوات مُتخَصِّصة من أجل حماية البيانات خاصَّة غير المُصَرَّح بالوصول إليها.
5. يحتاج الأفراد إلى معرفة أُسُس الأمـان الرَّقميّ لحمـــاية أنفسهم وبياناتهم الخاصَّة من المَخَاطِر السّيبرانيَّة.

توجيه

اقـرأ الجُمَـل الـوَارِدَة في الجَـدْول بِتَمَعُّنٍ، وفكِّر فيما إذا كانت كانت المعلومات صحيحة أم خاطئة، فإذا كانت صحيحةً ضَعْ علامة (✓)، وإذا كانت خاطئةً ضَعْ علامة (✗)، واطلب مساعدة المُدَرِّب في حال احتجت إلى ذلك.

6 ازداد الاهتمـام بالأَمْن السّـيبرانيّ بعد اعتـماد أغلب المُؤسَّـسَات والحكومات على الخِدْمَات الرَّقميَّة والإلكترونيَّة.

7 خَرْق الخصوصيَّة وسـرقة البيانات مشـكلة سَـهْلة لا عَواقِب كبيرة لها.

8 الهجمات الإلكترونية لها الكثير من الفوائد.

9 يمكن للهجمات الإلكترونية أن تكشف البيانات السِّرِّيَّة أو تَتَسبَّب في سرقتها أو حَذْفها بشكلٍ مُتعمَّد.

10 لا تَحْدُث الهجمات الإلكترونية بشـكلٍ مُتَعَمَّد، ويمكن لأيّ شخصٍ القيام بها.


PASSWORD PROTECTED
انْتَبِه!
وضع كلمة سرّ واحدة لجميع الحسابات الشّخصيّة والبريد الإلكترونيّ، يزيد من فُرَص خرق أجهــزتك الإلكترونيّة.
* * * * *


01001110
01110100
0111011101
111100010110

هل تعلم؟

مخترقو الأجهزة والبيانات (الهاكرز) يبحثون عن الثّغرات التي يمكن من خلالها سرقة الأموال والمعلومات الخاصّة، ولتفادي ذلك ينبغي تحديث البرامج واستخدام كلمات مرور قويّة وتغييرها بين الحين والآخر، وتشفير البيانات المُهمَّة.

التَّمْرين الثَّاني

صِلْ بين العِبَارات في العمـود الأوَّل، مع ما يَنْسَجم معها في العَمُود الثَّاني.

توجيه

اقرأ الجمل الواردة بالجدول بدقة، ابدأ بالجُمْلَة الأُولَى في العَمُود الأَوَّل، وابحث في العمود الثَّاني عن الجملة التي تستكمل معناها، أَدْنَاهُ مثال عن الوَصْل بين جُمْلَتَيْن.

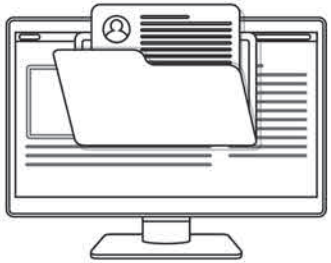
الجلوس لأوقات طويلة على الإنترنت	محـاولات القَرْصَنــة وسرقة البيانات على المواقع الإلكترونيَّة.
استخدام الإنترنت لأوقاتٍ طويلةٍ يمكن أن يصيبك	حين تجلس لفترات طويلة على الإنترنت دون تعامُل مع الآخرين.
قد تتعرَّض لخرق الخصوصية من خلال	يُـــؤدِّي إلـــى مشـكلات أخـــلاقيَّة ونفســـيَّة وعضـــويَّة.
خرق الخصوصية	لأنَّ الانفتاح على الثَّقافات الأخرى بدون ضوابط قد يُؤدِّي إلى اكتســـاب مـــا هو غير مُناسِب لثقافتنا، ويتنافَى مع مُعتقداتنا الدِّينيَّة والثَّقافيَّة.
التَّعرُّض للمحتوى العَنِيف وغير المُناسِب للأطفال	لأنَّ بعض الجماعات الإرهابيَّة تلجأ إليه لتجـنيد الشَّباب والإضرار بالمجتمع.
يمكنك أن تُصَاب بإدمان الإنترنت	يُـؤدِّي إلـى العُـزْلة الاجتـــماعيَّـــة.
يُهدِّد الإنترنت أمان المجتمع	من الجرائم التي يُعاقِب عليها القانون.
يُهدِّد الإنترنت الثَّقافة الوطنيَّة	بالاكتـــئاب ونَوْبـــات القـــلق والتَّـــوتُّر.

انْتَبِه!

تجاهُل إعدادات الخصوصيَّة،
وعدم مُتابَعَة أحدث التَّغييرات
بنُظُم التَّشْغيل يعرِّض بياناتك
لخَطَر الاختراق.

التَّمْرين الثَّالث

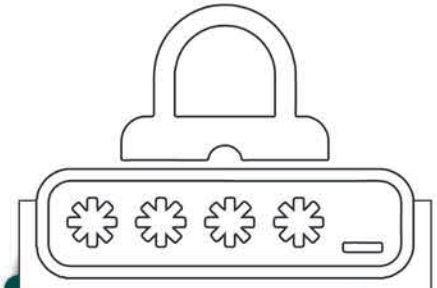
اقرأ الكلمات التَّالية بِتَمَعُّنٍ، وفَكِّر فيما إذا كانت هذه الكلمات تُعَبِّر عن شيءٍ يمكن **سَرقته عن طريق الإنترنت**، فعلى سبيل المثال: الصُّوَر والمَقَاطِع المُصَوَّرَة الخاصَّة تُعَدّ من الأشياء التي يُمْكِن سَرقتها من خلال شبكة الإنترنت.. **فأيّ شيءٍ مما يلي يمكن سرقته عن طريق الإنترنت لَوِّنه بأحد الألوان.**



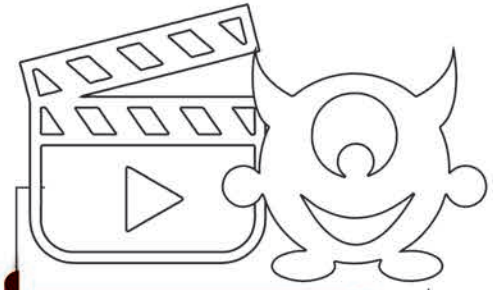
المعلـومـات والمسـتنـدات الموجـودة على الحـاسـوب

أرقام الحسابات المصرفيّة

أرقام بطاقات الائتمان

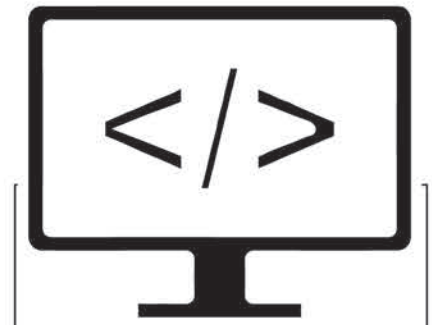


كلمات المرور

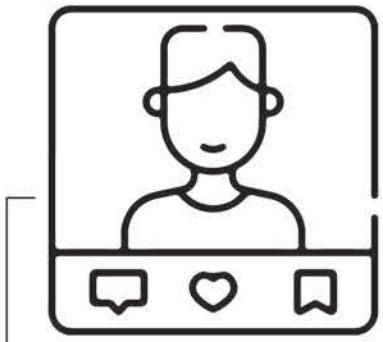


ملفّات أفلام الكارتون

بيانات الأوراق الرَّسميَّة مثل الرُّخْصَة وجواز السَّفَر

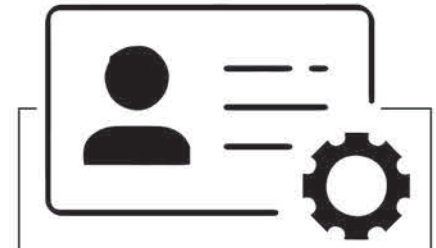


الأكواد المصدريّة والخوارزميّات

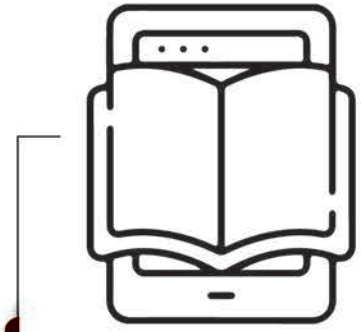


المنشورات على منصّات التّواصل الاجتماعيّ

مواعيد العمل



بيانات الحسابات على منصّات التّواصل الاجتماعيّ



الكُتُب الرّقميّة

ملفّات الأغاني

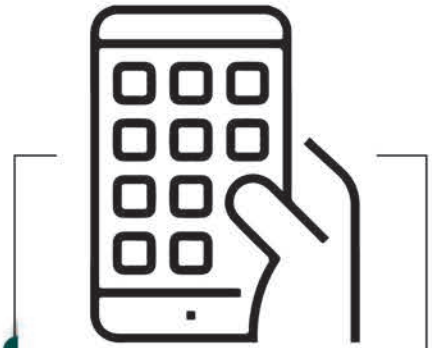
الهُويّات الإلكترونيّة

أسماء وقوائم العُمَلاء

الصُّوَر والمَقاطِع
المُصوَّرة الخاصَّة

سجلات الموارد البشريّة
وبيانات المُوظَّفين

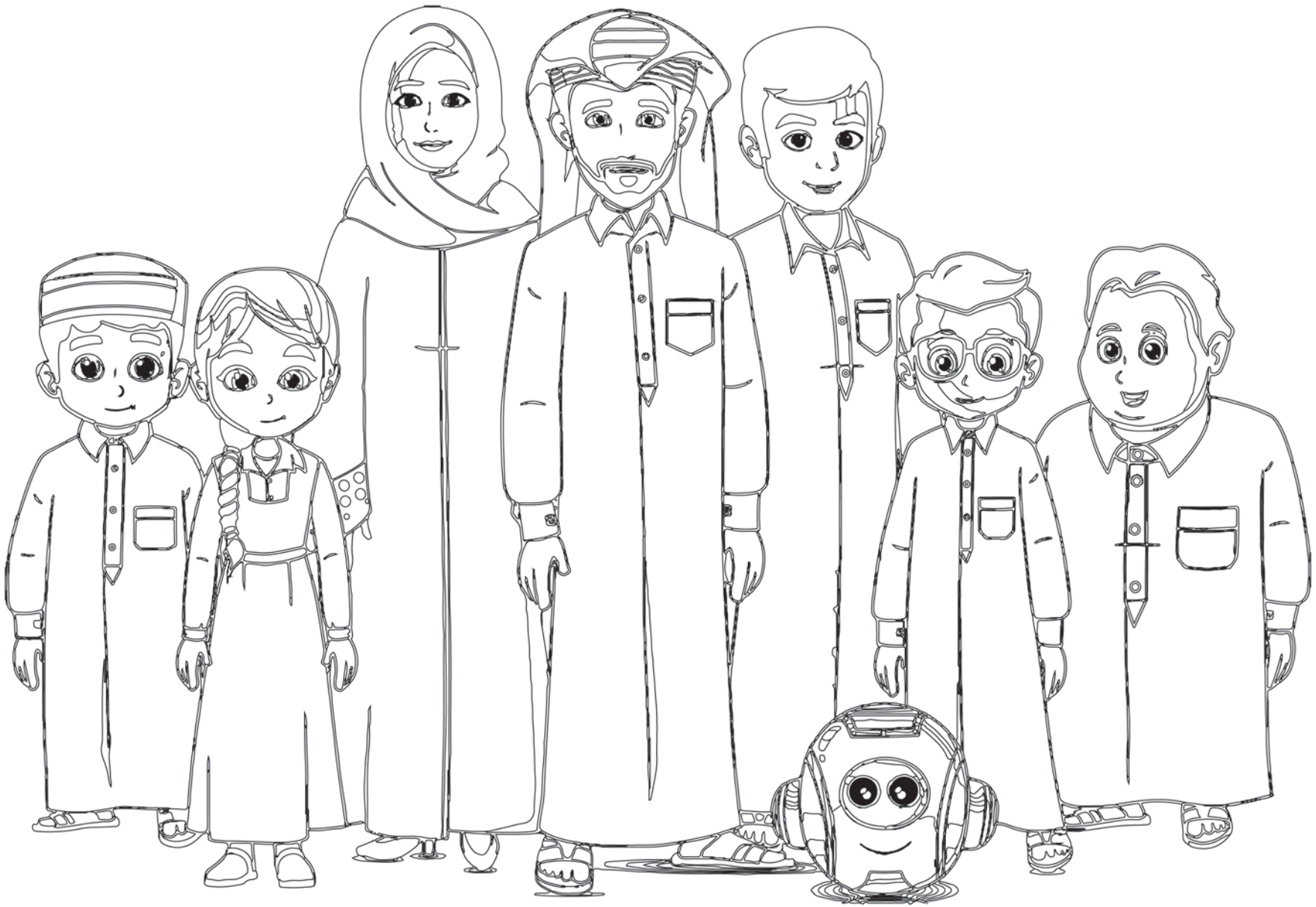
السِّجلات الطِّبيَّة



التَّطبيقات

انْتَبِه!

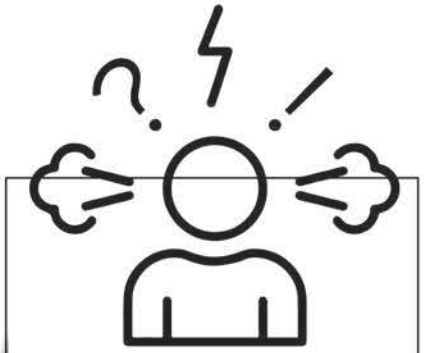
عدم تحديث أنظمة الأجهزة الذَّكيَّة؛ سواءٌ أجهزة الحاسوب الشخصي أو الهواتف، يُعرِّضها لعَشَرات الثّغرَات التي يَسْتَغِلُّها مخترقو الأجهزة لسَرقة البيانات وخرق الأجهزة.



التَّمْرين الرابع

اقرأ الكلمات الوَارِدَة بِتَمَعُّنٍ، وفَكِّر فيما إذا كانت هـذه الـكلـمـات تُـعَـبِّـر عـن **الآثار والمخاطر الرقمية** ثمّ قُمْ بتلوين المُرَبَّع الذي به الكلمة أو العبارة.

القَلَق



التَّوتُّر

الفَخْر

السَّعادَة

تَشتُّت الانتباه

الرَّغْبَة في تَرْك المدرسة

تَجنُّب الأصدِقَاء

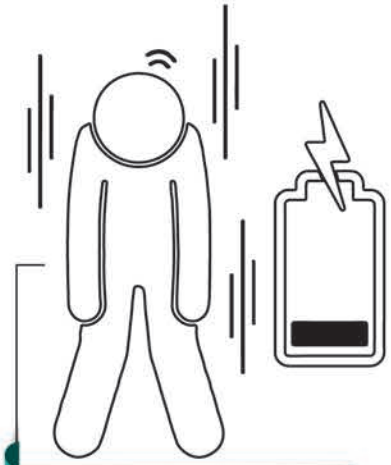
القُدْرَة على المُواجَهة

تناقُص العَلامَات الدِّراسيَّة

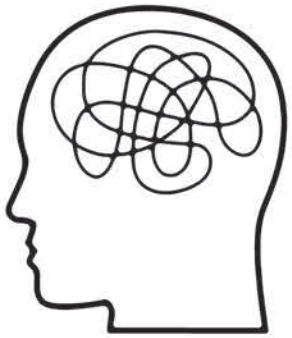
فَقْد احترام الذَّات

مشكلات النَّوْم

زيادة الصَّدَاقَات



فُقْدَان الطَّاقة



المَشْكِلَات النَّفسيَّة

الخوف من المُواجَهَة

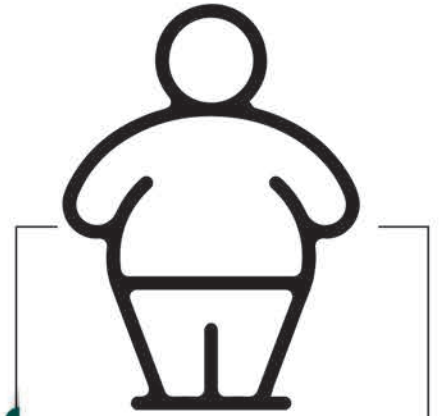
فُقْدان الثِّقة بالنَّفس

التَّعاسَة

الرَّغْبَة في القيام بالأنْشِطَة

تجنُّب الخروج

التَّركيز



زيادة الوَزْن

هل تعلم؟

كثرة الإعلانات تُعدّ مؤشّرًا على وجود الفيروسات على مواقع الويب، والتي تنتقل إلى الأجهزة الإلكترونيَّة بمجرد الضَّغْط عليها.

التَّمْرين الخامس

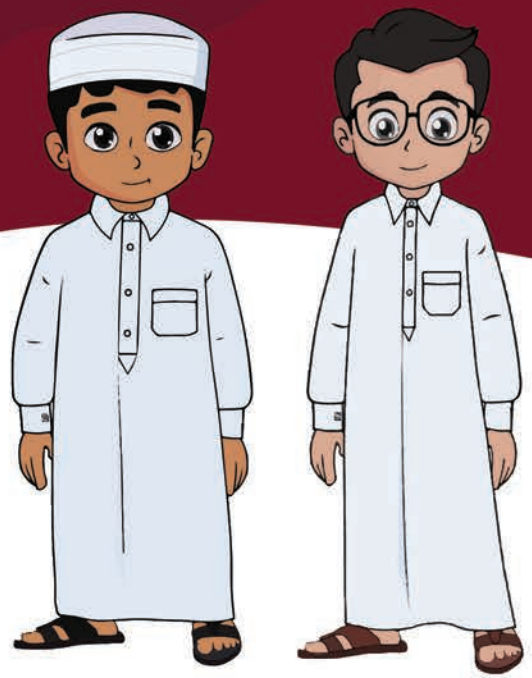
اقرأ كلمات المرور الوَارِدَة أَدْنَاهُ بِتَمَعُّنٍ، وفَكِّر فيما إذا كانت هذه الكلمات تُعَدّ **كلمات مرور قويّة أم لا**.
تَذَكَّر ما شَرَحَهُ لك المُدَرِّب عن مَعَايير اختيار كلمات المرور القَوِيّة، فمثلًا كلمة المرور **123456 ليست قويّة**؛ لأنّه يَسْهُل تَخْمِينُها، ولأنّها مُؤَلَّفَة من أرقامٍ مُتَتالِيةٍ.

- [ ] **123456**
- [ ] **Password**
- [ ] **Medo123**
- [ ] **Me@12do**
- [ ] **Penten**
- [ ] **654321**
- [ ] **Pass123**
- [ ] **123medo**
- [ ] **2020MMeeDDoo$%**
- [ ] **Klmetser**

انْتَبِه! الضَّغْط على أيّ رابط غير معروفٍ أو مشكوكٍ فيه، يتسبَّب في خرق الحسابات الشخصية.

التَّمْرين السَّادس

اختر الإجابة الصحيحة فيما يلي:



1. **حين أتَعَرَّض لجريمةٍ إلكترونيَّة عليَّ أن:**

- [ ] أسكت تمامًا ولا أُخْبِر أيّ أحدٍ.
- [ ] أتَواصَل مع الشُّرطة دون عِلْم والدي ووالدتي.
- [ ] أتَوجَّه فَوْرًا إلى أحد والديَّ أو إلى مُعلِّمي في المدرسة.

2. **حين أتعرَّض لجريمة الابتزاز الإلكترونيّ،**

أوَّل شيءٍ يجب عليَّ، أن:

- [ ] أُهدِّد مَن يقوم بابتزازي وأستفزّه.
- [ ] أحظُره تمامًا، وأُبَلِّغ عنه مُقدِّمي الخدمة.
- [ ] أُحاول إعطاءَه ما يُريد؛ كي لا يَضُرّني بما يَعْرفه عنّي.

3. **لحماية نفسي على شبكة الإنترنت عليَّ:**

- [ ] أنْ أُخْبِر الجميع كلّ شيءٍ عنّي.
- [ ] ألَّا أُكَوِّن أيّ صَداقَات علَى الإنترنت مطلقًا.
- [ ] أنْ أُشَارك المعلومات العاديَّة وغير الخاصَّة، والتي لا يمكن أن يَستغلّها أحدٌ ضدِّي.


ثانيًا: التَّمارين اللَّاصَفِّيَّة

انْتَبِه!

مُشارَكة الكثير من التَّفاصيل عن الحياة الشَّخصيَّة، وطبيعة عملنا ومنزلنا على الإنترنت تُعرِّضنا للخرق والسَّـرِقَة.

التَّمْرين الأوَّل

اقرأ الكلمات الوَارِدَة أَدْنَاهُ بِتَمَعُّنٍ، وابحثْ في الخانات عن حُرُوف مُتتالية تُشَكِّل هذه الكلمات، أَدْنَاهُ مثال لكلمة **"لُصُوص"**، وكيف تمَّ إيجاد أحْرُف الكلمة في الجدول:

ا	ل	أ	م	ن	ا	ل	س	ي	ب	ر	ا	ن	ي
ل	ص	غ	ش	ب	ذ	خ	د	م	ا	ت	س	س	ي
ج	و	و	ك	ا	ر	ث	ة	ا	ل	س	ر	ي	ة
ر	ص	ك	ل		ا	ل	ه	ج	م	ا	ت	ر	ذ
ي	غ	ش	ة	ا	ل	م	خ	ا	ط	ر	ل	ا	ف
م	ا	ل	ا	ح	ت	ي	ا	ل		س	ر	ق	ة
ة	ح	م	ا	ي	ة	ا	ل	ب	ي	ا	ن	ا	ت
ا	ل	أ	م	ا	ن	ا	ل	ر	ق	م	ي	ع	ة

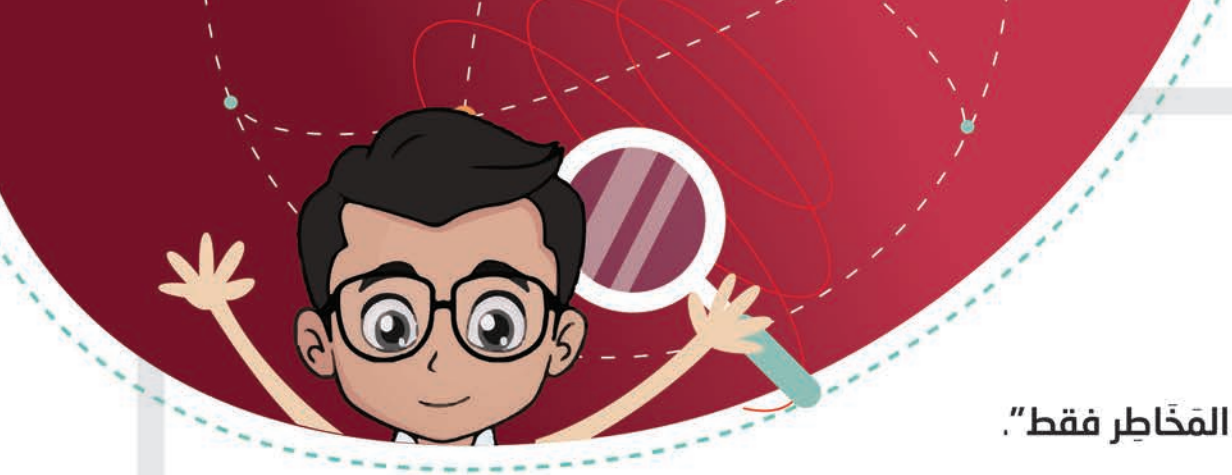
الأَمْن السّيبرانيّ - الأمان الرَّقميّ - الهجمات - الجريمة - البيانات - السِّرِّيَّة - المَخَاطِر

الاحتيال - خِدْمات - سرقة - مشكلة - حماية - ~~لصوص~~ - كارثة

التَّمْرين الثَّاني

اقرأ العبارات الوَارِدَة أَدْنَاهُ بِتَمَعُّنٍ، واقرأ الكلمات أو العبارات الوَارِدَة بين إشارَتَي التَّنصيص "..."، وحَدِّد الكلمة المُناسِبَة

- الإنترنت شبكة " ☑ **دوليَّة** ☐ **محليَّة**".
- الإنترنت وسيلة " ☐ **للتَّعلُّم والتَّرفيه** ☐ **للتَّرفيه والتَّسلية**".
- الإنترنت مُهِمّ لنَقْل ومُشارَكة " ☐ **البيانات** ☐ **الأفلام والمسلسلات**".
- هناك ارتباط بين الإصابة بـ " ☐ **النّحافة** ☐ **السِّمنة**" وبين استخدام الإنترنت لوقتٍ طويلٍ.
- استخدام الإنترنت لوقتٍ طويلٍ قد يتسبَّب في جعلك " ☐ **منعزلًا اجتماعيًّا** ☐ **اجتماعيًّا ومُحِبًّا للتَّجمُّعات**".
- هناك أبحاث تُؤكِّد أنَّ استخدام الإنترنت لوقتٍ طويلٍ قد يُصيبك بالكثير من" ☐ **الترقيات** ☐ **الأمراض**" الجسديَّة والنفسيَّة.



- الإنترنت مليء بـ "◯ **الفوائد والمَخَاطِر** ◯ **المَخَاطِر فقط**".
- تَسْتَغِلّ الجماعات الإرهابيَّة الإنترنت لـ "◯ **تعليم** ◯ **تجنيد**" **الشَّباب.**
- سرقة البيانات وخرق الحسابات الشَّخصيَّة "◯ **جريمة** ◯ **جائزة**" في القانون.
- من أبرز مشكلات الإنترنت أنَّ كلّ البيانات مُعرَّضة "◯ **للحفظ** ◯ **للسَّرقة والخَرْق**".
- إدمان الإنترنت قد يُؤثِّر على قُدْرتك على "◯ **التَّفَاعُل والتَّعامُل** ◯ **الحُضُور**" مع الآخرين.
- التَّعرُّض لثقافات جديدة قد يُؤدِّي إلى "◯ **رفض** ◯ **اكتساب**" عادات تُخالِف معتقداتنا وقِيَمنا.
- يُهدِّد الإنترنت الثَّقافة المجتمعيَّة بسبب "◯ **انغلاقه** ◯ **انفتاحه**" على العالَم وثقافاته المختلفة.
- الأطفال هم الأكثر عُرْضَة للمشكلات على شبكة الإنترنت بسبب المحتوى "◯ **العنيف** ◯ **الموسيقي**".
- إدمان الإنترنت من المُشكلات الشَّائعة والتي تَحْدُث بسبب

" ◯ **استخدام الإنترنت لـــــوقتٍ طويـــلٍ** ◯ **استـــخدام الإنترنت لمدة ســاعتين كلّ يوم**".

التَّمْرين الثَّالث

اقرأ الجُمَل الوَارِدَة في الجدول بِتَمَعُّنٍ، وفَكِّر إذا كانت المعلومات **صحيحة أم خاطئة**، وإذا وَجَدْتَها صحيحةً اكْتُب بجانبها (صحيح)، وإذا وَجَدْتَها خاطئة اكْتُب بجانبها (خطأ)، اطلب مُساعَدَة المُدَرِّب في حال احتجت لذلك.

يمكن للمُخْتَرِقِينَ سَرِقَة البيانات الخاصَّة بالمُستخْدِمِين من خلال الاحتيال والتَّظَاهُر بأنَّهم جهة موثوقة، مثل البنوك أو شركات الاتِّصالات.		
كلمات المرور الضَّعيفة قد تكون أسْهل طَريقة لسَرقة البيانات.		
أحيانًا يُرْسِل المُخْتَرِق ملفًّا أو رابطًا عبر البريد الإلكترونيّ وبمُجرَّد الضَّغْط عليه يَتِمّ خرق الجهاز بكلِّ سهولةٍ وسرقة البيانات.		
لا مُشكلة من سَرِقة البيانات.		
لا يمكن للمُخْتَرِق الاستفادة من البيانات التي قام بسَرِقتها.		
عليك اختيار كلمات سِرّ بسيطة، ويمكن تخمينها بسهولة.		

لا بُدَّ أن تتأكَّد أنَّه لا تُوجد ثَغرَات أمنيَّة في نظام حاسوبك أو تطبيقات مُختَرَقَة على هاتفك لتَجَنُّب خَطَر سرقة البيانات.

لا يَحْدُث أيّ خطأ بشريّ يمكن أن يُؤدِّي إلى سرقة البيانات.

التَّنزيلات دائمًا آمِنَة، ولا يمكن خرق الأجهزة أو سرقة البيانات من خلالها.

يمكن أن تتسبَّب المشكلات في قواعد البيانات أو الخوادم في سرقة البيانات وسهولة دُخُول المُخْتَرِقِين إلى الشَّبكات أو الأجهزة.

قد يتسبَّب الشَّخْص نفسه في سرقة بياناته دون أن يَشْعُر، فقط بالإفصاح عن كثير من المعلومات من خلال مِنَصَّات التَّواصُل الاجتماعيّ.

أحيانًا تتسبَّب سرقة الهواتف أو أجهزة الحاسوب في تسريب البيانات.

استخدام شبكات Wi-Fi (الإنترنت) العامَّة، أو أجهزة الحاسوب في الأماكن العامَّة مثل المكتبات قد يُعرِّض البيانات لخطر السَّرقة.

لا تحتاج الشركات أو المُؤسَّسَات إلى تأمين قواعد البيانات أو الخوادم من أجل حماية بيانات العملاء.

التَّمْرين الرَّابع

لَوِّن الصُّورَة التَّالية

التَّمْرين الخامس

ضع علامة (✓) أمام العِبارات التي يمكـــن أن تُســـاعِدَك فـــي كتـــابة **كلمة مرور قويَّة**

اقرأ العبارات الوَارِدَة بِتَمَعُّنٍ، وفَكِّر فيما إذا كانت هذه العبارة تُعَبِّر عن شروط كتابة كلمة مرور قويَّة، تَذَكَّرْ ما شَرَحَه لك المُدَرِّب عن مَعايير اختيار كلمات المرور القَويَّة.

أسْتَخْدم نفس حُرُوف اسم المُستَخْدِم.	
أسْتَخْدم مجموعةً مُتَنَوِّعَة من الحروف والأرقام.	
أستَخْدم تاريخ يوم ميلادي.	
أسْتَخْدم مجموعةً من الحروف الكبيرة والصَّغيرة وبعض الرُّموز.	
أسْتَخْدم كلمةً لا يُمْكِنُني تَذكُّرها.	
أسْتَخْدم كلمةً قريبةً من كلمات المرور القديمة.	
أسْتَخْدِم كلمة password.	
أسْتَخْدِم اسم قطَّتي/كلبي.	
أسْتَخْدم تاريخًا مُمَيَّزًا بالنِّسبة لي.	
أسْتَخْدم كلمة يَسْهُل عليَّ تَذَكُّرها، ويصعب على الآخرين تَخْمينها.	

انْتَبِه!

قبول طلبات الصَّداقة من أشخاص مجهولين أمرٌ خطيرٌ؛ لأنَّه يُتيح لهم خرق خصوصيتك ومعرفة معلوماتك الشَّخصيَّة.


الألعاب التّدْريبيّة

نَاقِشْ مع زُمَلائك الأسئلة التَّالية

01 الأَمْن السّيبرانيّ cyber security يُطلق عليه أيضًا

(.....) (عدد الحروف 10)

02 طول كلمة المرور القويَّة

(.....) (عدد الحروف 6)

03 أشخاص يُسبِّبون ضررًا بالغًا في أجهزتنا الإلكترونيَّة

(.....) (عدد الحروف 7)

04 أحد أنواع الأَمْن السّيبرانيّ

(.....) (عدد الحروف 12)

05 أحد أمثلة الحقوق الفكريَّة

(.....) (عدد الحروف 15)

ضَع المُسمَّى المُناسِـــب

تحتوي على روابط أو ملفَّات بها فيروسات أو برمجيَّات خبيثة، وبمُجَرَّد فَتْحها أو النَّقْر عليها تَسْرق بياناتك... ما هي؟ .....

بمُجرَّد قَبُولك لها فإنَّ خصوصيّتك ومعلوماتك الشَّخصيَّة تُصبح مُهدَّدة... ما هي؟ .....

مَهمّته هي حماية نُظُم التَّشْغيل المعلوماتيَّة ومُكوّناتها من أجهزة وخِدْمَات وبيانات... ما هو هذا الشَّيء؟ .....

شَكْل مُتطوّر من أشكال الجريمة العَابِرة للحدود، التي تحدث في مجال الفضاء الإلكترونيّ. .....

نَشْر أكاذيب أو صُوَر مُحْرِجَة لشخصٍ ما، أو إرسال رسائل مُؤذية، أو تهديد لشخصٍ ما على وسائل التَّواصُل الاجتماعيّ، كلّها صُوَر من .....

تتألَّف كلمة المرور القويَّة من .....

مشروع التَّخرُّج

مشروع التَّخرُّج هو واجبٌ تقوم به بمُفْرَدك أو بالاشتراك مع زميل أو زميلين من زُمَلائك، تقوم من خلاله وتحت إشراف المُدرِّب بأحد الواجبات التَّالية:

كتابة قِصَّة قصيرة عن شَخْصٍ ما تعرَّض لأحد المَخاطِر الرَّقميَّة، (تختار أنتَ هذه المَخاطِر)، وتُبَيِّن كيف تَصرَّف بحكمةٍ، وتَمكَّن من مُواجَهَة هذه المَخاطِر، وما هي الإجراءات التي قام بها.

تَخيَّل نَفسَك أنَّكَ مُدَرِّب، وستقوم بكتابة بعض التَّوجيهات للطَّلَبَة تُبَيِّن لهم فيها كيف يَقُومون بحماية أنفسهم من المَخاطِر الرَّقميَّة.

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency