مَنَاهِج الأَمْن السِّيبْرَانِيّ التَّعْلِيمِيَّة

Cyber Security Curricula Education

الاستخدام الآمِن لشَبَكة الإنترنت

من مخاطر استخدام الإنترنت:
التَّعَرُّض لسرقة البيانات.

اخمِ معلوماتكَ الشَّخصيَّة
مثل كلمات المرور والصُّوَر.

لَا تُشارِكْ بياناتك مع الغُرَباء
ولا تُرسلها لأيّ شَخْصٍ لا تَعْرفه.

قواعد التَّصفُّح الآمِن للإنترنت

احْمِ نَفْسَك أثناءَ زيارة مواقع الويب؛ كي لا تتعرَّض لسرقة بياناتك.

تجنَّب الضَّغْط على الإعلانات التي تُصادفك أثناءَ تصفُّح الإنترنت.

برامج الحماية تَمْنع الفيروسات من تَخْريب الأجهزة الإلكترونيَّة.

الاستخدام الآمِن للبريد الإلكترونيّ

علينا أن نُنْشِئ كلمةَ مرورٍ قويَّة للبريد الإلكترونيّ.

يجب أن تكون كلمة المرور مُكوَّنة من أحْرُف وأرقامٍ ورموزٍ.

يجب أنْ نَحْمِي البريد الإلكترونيّ، ولا نُشَارِك معلوماته مع أيّ شَخْص.

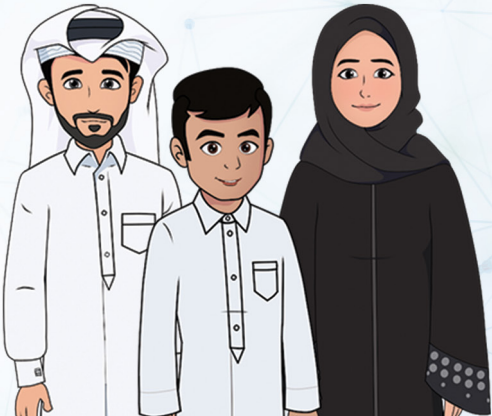
المعلومات المَوْثُوقَة على الإنترنت

حقوق النَّشْر والطِّباعة

علينا أن نَذْكُر مَصَادِر معلوماتنا.

لا يَجُوز أنْ نَقُوم بنَسْخ نصٍّ مَا ثُمَّ نَنْسبه لأنفسنا.

حقوق النَّشْر والطِّباعة تُمْنَح لمُؤَلِّف المحتوى الأصْلِيّ.



صِحّتُك والحاسوب

قَضاء وقتٍ طويلٍ مع الأجهزة الإلكترونيَّة قد يُسبِّب مشكلات صِحِّيَّة.

منها: ضَعْف النَّظَر، وإجهاد العينَيْن، وتَقوُّس العمود الفقريّ.

علينا أن نَخْرجَ من البيت، ونلعب مع أصدقائنا؛ لكي نُحَافِظ على صِحَّتِنا.

العُزْلَة الاجتماعيَّة

قضاء وقتٍ طويلٍ مع الأجهزة الإلكترونيَّة يُسَبِّب عُزْلَة اجتماعيَّة.

ازدادت العُزْلَة بَعْد قضاء النَّاس أوقاتًا طويلةً مع أجهزتهم الإلكترونيَّة.

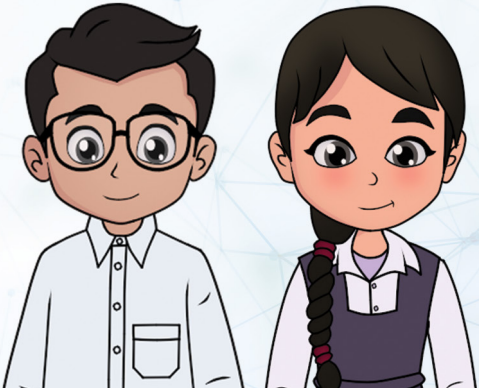
علينا أنْ نُوَزِّع وَقْتنا بين الدِّراسَة، والمَرَح مع الأصدقاء، والأجهزة الإلكترونيَّة.

المِلْكِيَّة الفِكْرِيَّة

المِلْكِيَّة الفِكْرِيَّة هي فكرةٌ أو ابتكارٌ أو عملٌ قام به شخصٌ ما.

علينا الاستئذان قبل استخدام أيّ مَادَّة عليها حقوق مِلْكِيَّة فِكْرِيَّة.

انتهاك حقوق المِلْكِيَّة الفِكْرِيَّة يُعَرِّضْنَا للمُسَاءَلة القانونيَّة.

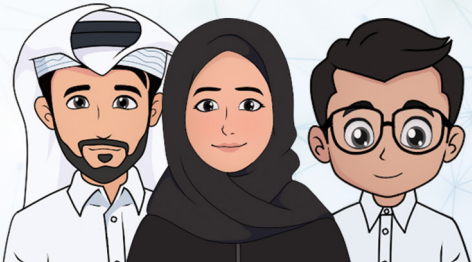


حماية الحاسوب

علينا اختيارُ كَلِمَة مُرُور قويَّة للبريد الإلكترونيّ.

كلمة المرور القويَّة تكون مُؤَلَّفَة من أحرفٍ وأرقامٍ ورموزٍ.

يجب أنْ لَا نَسْتَخدم أسماءَنا أو الكلمات والتَّواريخ الشَّائعة ككلمات مرورٍ.

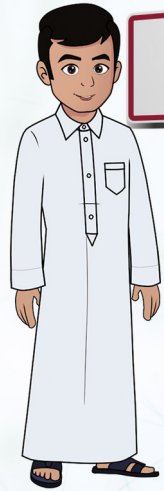


تراخيص البرامج

هناك الكثيرُ من المخاطر التي قد تَتعَرَّض لها أثناء استخدام الإنترنت.

علينا تَجَنُّب الوقوع في مشكلات قانونيَّة بسبب سوء استخدام الإنترنت والمعلومات.

علينا أن نَسْتَعِين بأحد الوالدَيْنِ أو بالمُعَلِّم للحصول على البرامج من مَصَادِرها الصَّحيحة.



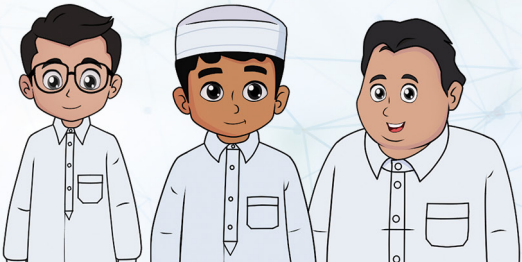
النَّشْر الرَّقميّ
ووسائل التَّواصُل الاجتماعيّ

شبكات التَّواصُل تُتِيح لنا التَّوَاصُل مع الآخرين.

تُتِيح شَبَكات التَّواصُل نَشْر الصُّوَر والنُّصوص ومقاطع الفيديو والمقالات المُتَنَوِّعَة.

إساءة استخدام شَبَكات التَّواصُل تَجْعلنا عُرْضَة لأذَى الغُرَباء.

لا تَنْشُر خصوصيّاتك كعنوان المنزل أو المدرسة أو رَقْم الهاتف على الإنترنت.

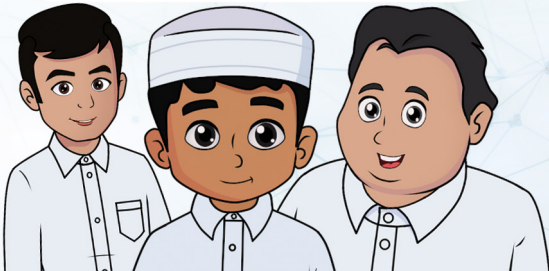


القَرْصَنة الرَّقمِيَّة

حقوق النَّشْر هي حقوق تُمْنَح لأصحاب المِلْكِيَّة الفِكْرِيَّة.

القَرْصَنة هي انتهاكُ حقوقِ النَّشْر.

يجب احترام حقوق الآخرين وعدم التَّعدِّي عليها.

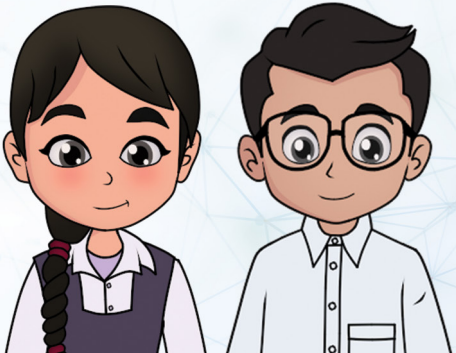


التَّنَمُّر الإلكترونيّ

التَّنَمُّر الإلكترونيّ هو الإساءَة للآخرين بالكلام أو بنَشْر الصُّوَر، أو غيرها.

علينا ألَّا نُشَارِك صُوَر وبيانات الآخرين بدونِ إِذْنهم.

علينا ألَّا نُشَارِك أيّ مَنْشُورات غير لائقة، أو قد تُسَبِّب الأذَى للآخرين.

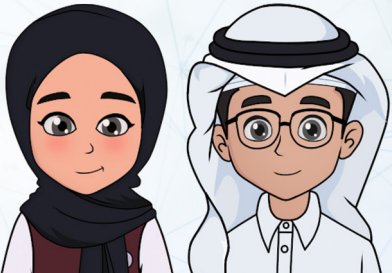


البرامـج الخبيثـة

علينا حماية أجهزتنا الإلكترونيَّة من مخاطر البرامج الخَبِيثة.

يتمّ تَصْميم البرامج الخبيثة بغَرَض إتلاف البيانات أو الإضرار بالأجهزة.

من البرامج الخبيثة: أحصنة طروادة (Trojans)، والدِّيدان (Worms)، وبرمجيَّات التَّجسُّس (Spyware).

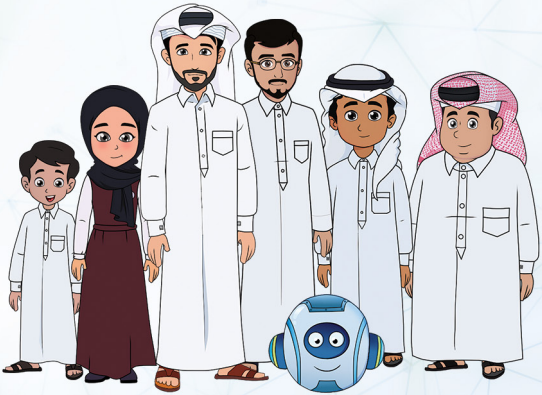


حماية الشَّبكات من
البرامج الخبيثة

علينا أنْ لا نكشف عن اسم المستخدِم أو كلمة المرور الخاصَّيْن بنا.

علينا أنْ لا نفتح رسائل البريد الإلكترونيّ من مصدرٍ غير معروفٍ.

علينا التَّأكُّد من تحديث برنامج مُكافَحَة الفيروسات.



من فوائد شبكات التَّواصُل الاجتماعيّ

تُساعدنا شبكات التَّواصُل الاجتماعيّ على التَّواصُل مع الأشخاص حول العالَم.

تُتيح تبادُل الأفكار والآراء مع الآخرين، وتُسهِّل الحصول على الأخبار

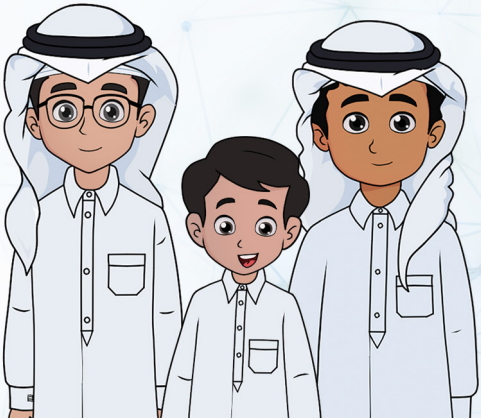
تُساعد في عمليّات التَّسويق الإلكترونيّ والأعمال التّجاريّة.

من تَحدِّيات شبكات التَّواصُل الاجتماعيّ

شبكات التَّواصُل الاجتماعيّ تُؤثِّر على العلاقات الحقيقيَّة بين الأشخاص.

تُسهِّل نَشْر الشَّائعات والأكاذيب، وقد تُعرِّضنا لعمليَّات الابتزاز.

علينا تجنُّب نَشْر المعلومات الشَّخصيَّة عبر شَبَكات التَّواصُل الاجتماعيّ.

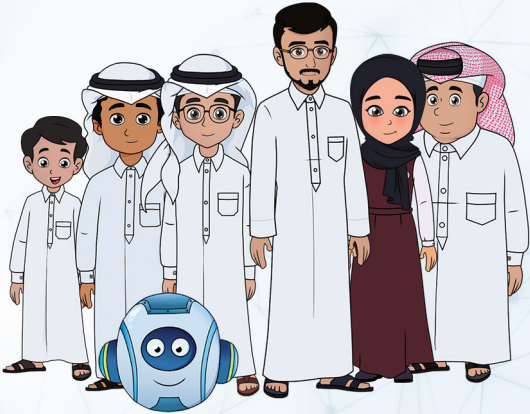


إجراءات لحماية الحاسوب

برامج مُكافَحَة الفيروسات تَحْمي الحواسيب من الفيروسات.

يجب تثبيت برنامج مُكافَحة الفيروسات على جهاز الحاسوب.

عليك التَّأكُّد من تحديث برنامج مُكافَحَة الفيروسات باستمرار.

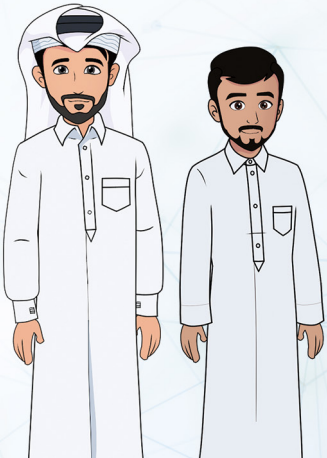


بروتوكولات الاتِّصال في الشَّبكات

بروتوكول الاتِّصال: هو نظامٌ رقميّ يَتضمَّن قواعدَ لتبادل الرَّسائل.

يتمّ تقسيم المعلومات إلى حُزَم؛ يُحَدَّد فيها الجهاز المُرْسِل والمُستقْبِل.

كلُّ حُزْمَة تتكوَّن من ثلاثة أجزاء: الرأس (Header)، والجِسْم (Payload)، والذَّيْل (Trailer).

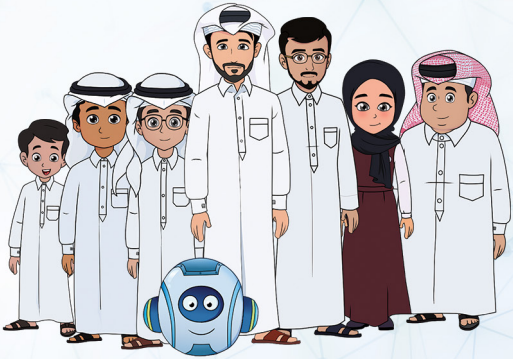


خصوصيَّة البيانات

قد تطلب منا مواقع الويب بياناتنا الشَّخصيَّة.

إعطاء البيانات الشَّخصيَّة لأيّ جهةٍ عبر الإنترنت يُعدّ خَطرًا.

احِرْص على عدم مُشارَكة المعلومات الشَّخصيَّة.

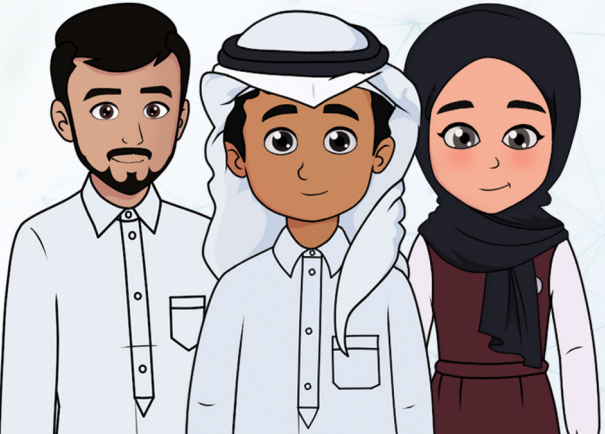


معلومات الأطفال الشَّخصيَّة

من الخَطَر مُشَارَكَة البيانات الخاصَّة بالأطفال عبر الإنترنت.

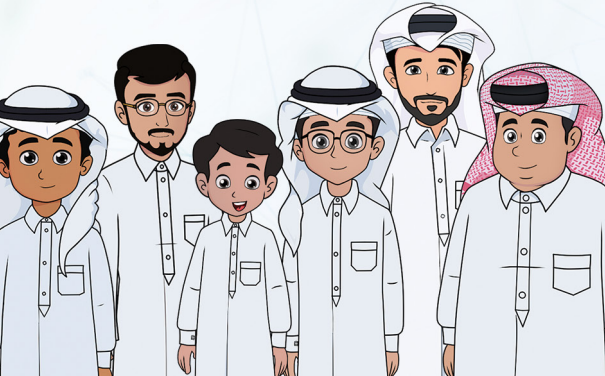
اقرأ دائمًا بيان الخصوصيَّة الذي يُوضِّح نَوْع وسبب طَلَب المعلومات.

لا يمكننا الوُثُوق بالأشخاص الغُرَباء الذين نَتعَرَّف عليهم عَبْر الإنترنت.



النَّسْخ الاحتياطيّ وحماية قواعد البيانات

- نستطيع حماية البيانات بعمل نُسَخ احتياطيَّة.
- يمكن تخزين النُّسَخ الاحتياطيَّة على حساب التَّخزين السَّحابيّ Cloud Storage، أو على وسائط التَّخزين الخارجيَّة.



النَّسخ الاحتياطيّ وحماية قواعد البيانات بكلمة مرور

يمكننا استخدام كلمات المرور في Microsoft Access لحماية بياناتنا.

لحماية عَمَلنا ومِلَفَّاتنا علينا حمايةُ قواعدِ البيانات بكلمةِ مرورٍ.

لكي نقوم بتعيين كلمة المرور لقاعدة البيانات يَجب فَتْحها في وَضْع Exclusive Mode

الاجتماعات عبر الإنترنت

1. تُتِيح شبكة الإنترنت إمكانيَّة عَقْد الاجتماعات عن بُعْد.

2. يمكننا مُشارَكة المِلفَّات والبيانات والعُرُوض التَّقديميَّة عبر الإنترنت.

3. هناك تطبيقات حديثة وُظِّفَتْ لإجراء الاجتماعات عن بُعْد؛ مثل تطبيق zoom.

أفْضَل المُمَارَسَات للعمل عبر شبكة الإنترنت

الاجتماعات عبر الإنترنت آمِنَة إذا التزَمْنا بالإجراءات السَّليمَة.

علينا مُشارَكة المعلومات بحَذَر، والانتباه إلى المَصاعب المُحتَمَلَة.

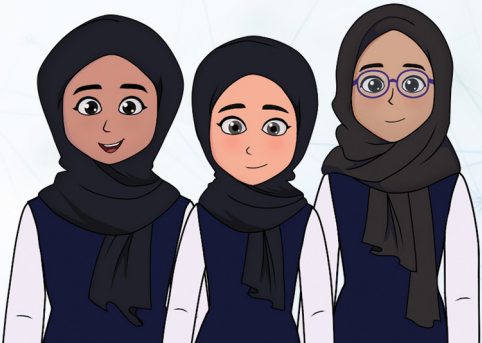
علينا أنْ لَا نُشارك معلوماتنا الشَّخصيَّة مع الغُرَباء.

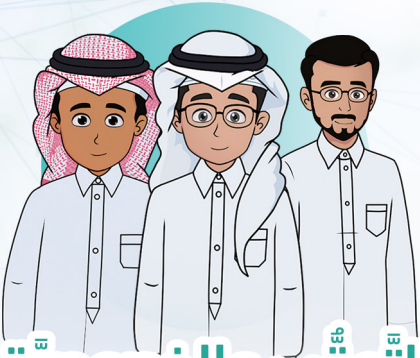
تقييم مصادر المعلومات على الإنترنت

تُوجد 6 معايير أساسيَّة لتقييم المصادر الإلكترونيَّة.

من معايير التَّقييم: الجهة المسؤولة، الغَرض والتَّغطية.

من معايير التَّقييم: الدِّقَّة والصَّلاحيَّة، الموضوعيَّة والمصداقيَّة.





التَّعقُّب والخصوصيَّة

كلّما استخدمنا الإنترنت نترك كمًّا هائلًا من المعلومات.

يقوم موقع Google بتتبُّع كلّ حركة نقوم بها على الإنترنت.

القانون يُجرِّم اختراق خُصوصيَّات الآخرين.

قطر أوَّل دولة خليجيَّة تَفْرض قانونًا لحماية البيانات الشَّخصيَّة.

بروتوكولات أمن الشبكة

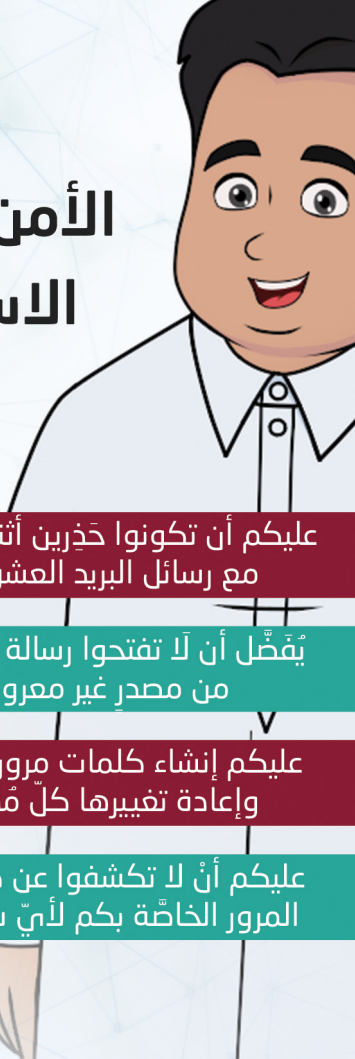
يتمّ بثّ الإشارة اللّاسلكيَّة في الهواء.

بروتوكولات أمن الشَّبكة تضمن أمن وسلامة البيانات أثناء نَقْلها.

تَمرُّ البيانات من جدار الحماية إذا تطابقت مع المعايير المُحدَّدة.

يُستخدَم بروتوكول (WPA3) لتشفير البيانات.

الأمن وقابليَّة الاستخدام



عليكم أن تكونوا حَذِرين أثناء التَّعامل مع رسائل البريد العشوائيّ.

يُفَضَّل أن لَا تفتحوا رسالة إلكترونيَّة من مصدرٍ غير معروفٍ.

عليكم إنشاء كلمات مرور قويَّة، وإعادة تغييرها كلّ مُدَّة.

عليكم أنْ لا تكشفوا عن كلمات المرور الخاصَّة بكم لأيّ شخصٍ.

أنظمة المُرَاقَبَة

أنظمة المُرَاقَبَة تُراقب الأحداث، وتُقدّم البيانات إلى خوادم أخرى على الشَّبكة.

من أكثر أنظمة المُرَاقَبَة شيوعًا واستخدامًا: أنظمة الإنذار ضِدَّ السَّرقة.

من تطبيقات أنظمة التَّحكُّم: الغسَّالات ومُكيِّفات الهواء، وأنظمة الإنذار الأمنيّ.

أمْن المعلومات في المُؤسَّسَات التّجاريَّة

تقوم الشَّركات باستخدام كلمات مرور قويَّة للوصول إلى مِلفَّاتها.

تُوفِّر الشَّركات أجهزةً مناسبة لحماية شَبكتها وبريدها الإلكترونيّ.

تقوم الشَّركات بتوعية مُوظّفيها رقميًّا.

تعمل الشَّركات على تحديث أنظمة التَّشغيل وبرامج الحماية.

الحَوْسَبة السَّحابيَّة

الأمن المعلوماتيّ

بعض البنوك تحتفظ ببيانات العملاء على أجهزة الخوادم الدَّاخليَّة.

من مزايا الحَوْسَبة السَّحابيَّة: قابليَّة التوسُّع حسب نُمُوّ المُؤسَّسَة.

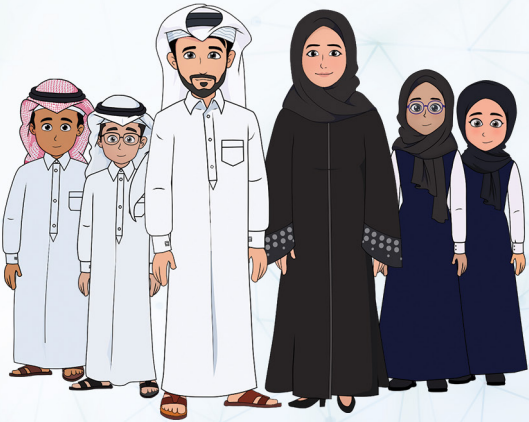
من مزايا الحَوْسَبة السَّحابيَّة: إمكانيَّة الوصول للأنظمة من أيّ مكان.

من مزايا الحَوْسَبة السَّحابيَّة: تقليل التَّكلفة.

المُسْتَشْعِرَات

المُسْتَشْعِر هو جهازٌ يَكشف عن وجود إشارة كالحركة والضّوء والضَّغْط.

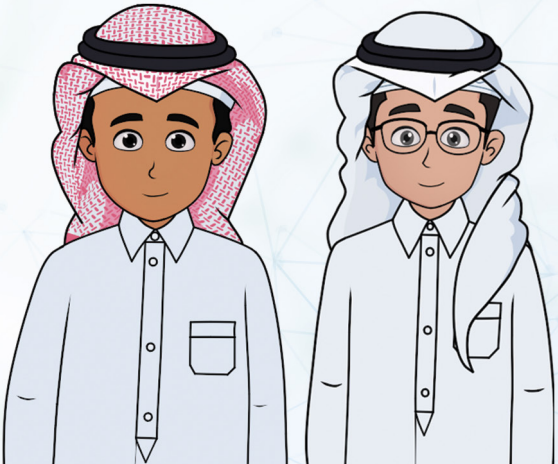
من أنواع المُسْتَشْعِرَات: مُسْتَشْعِرَات الحرارة، ومُسْتَشْعِرَات الدخان، ومُسْتَشْعِرَات اللَّمْس، والحركة، والضّوء، والضَّغط.



البَحْث والتَّحقُّق من جَوْدَة المعلومات

عندما نقوم بجمع أيّ معلومات علينا التَّحقُّق من معايير جَوْدَة المعلومات.

من أهمّ معايير جودة المعلومات: الدِّقَّة، المُلاءَمة، التَّوقيت، مستوى التَّفاصيل والكفاية.

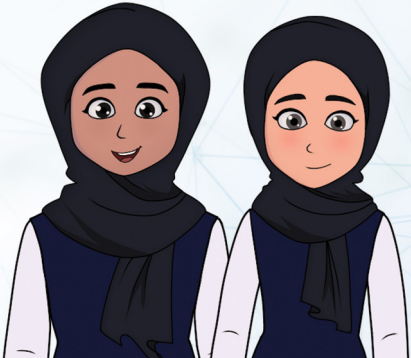


جَمْع البيانات والتَّحقُّق منها

جَمْع البيانات هو جَمْع وقياس المعلومات على المُتَغَيِّرَات المُستَهْدَفَة.

تُصنَّف مصادر البيانات إلى: مصادر رئيسة، ومصادر ثانويَّة.

يجب أن نعتمد على مصادر موثوقة أثناء جَمْع المعلومات.

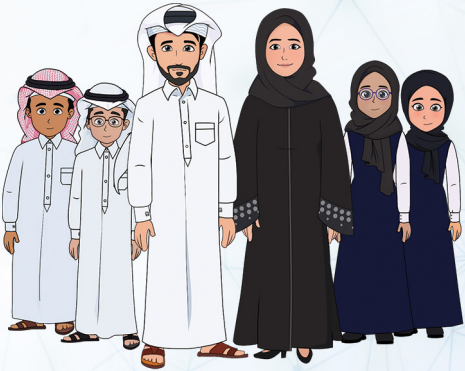


تشفير البيانات

التَّشْفير هو وسيلة لحماية البيانات بإخفائها عن الأشخاص الآخرين.

يَتِمّ فَكّ التَّشْفير مِن قِبَل الشَّخص الذي يملك مفتاحًا خاصًّا.

للتَّشفير نوعان رئيسان: التَّشْفير المُتماثِل والتَّشْفِير غير المُتماثِل.



تصميم النِّظَام

المسائل الأمنيَّة المُتعَلِّقة بالنِّظَام

دَوْرَة حياة النِّظَام تَمُرُّ بمراحل التَّحليل والتَّصميم والتَّنفيذ والاختبار والنَّشْر.

تصميم النِّظَام هو مرحلة تحديد عناصر النِّظَام ومُكوّناته.

يتمّ خلال مرحلة التَّصميم تحديد عناصر النِّظَام ومكوّناته وواجهات النِّظَام.

هل ملفَّاتي بأمانٍ على التَّخْزين السّحابيّ؟

يقدّم موفّرو خدمات التَّخْزين السّحابيّ خدمة أكثر أمانًا للشَّركات.

على الشركات توخّي الدِّقَّة عند اتِّخاذ قرار الانتقال إلى الحَوْسَبة السَّحابيَّة Cloud computing.

على الشَّركات الالتزام بسياسات الأمْن الرَّقميّ.

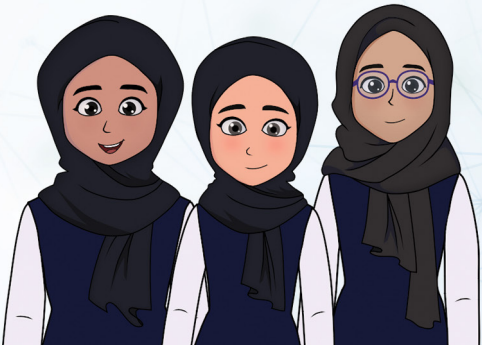
من الضَّروريّ إعداد المُوظَّفين للانتقال للحَوْسَبَة السَّحابيَّة.

المشاريع القائمة على Raspberry Pi
أنظمة المُرَاقَبَة الرَّقميَّة

المنزل الذَّكيّ مثالٌ لعمليَّة الأتمتة باستخدام (Raspberry Pi).

في المنزل الذَّكيّ يمكن إجراء المَرَاقَبَة والتَّحكُّم بالأجهزة عن بُعْد.

يمكن بناء نظام مُرَاقَبَة باستخدام (Raspberry Pi) بكاميرات عالية الدِّقَّة.

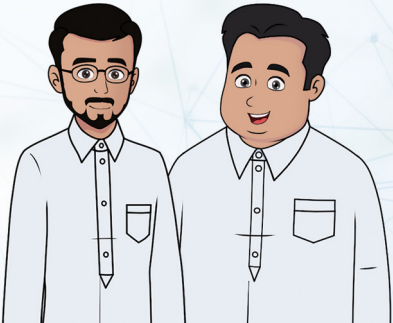


البَحْث والتَّحقُّق من جَوْدة المعلومات (دراسة السُّوق)

دراسة السُّوق هي جَمْع وتحليل البيانات والمعلومات حول سُوق مُعيَّن.

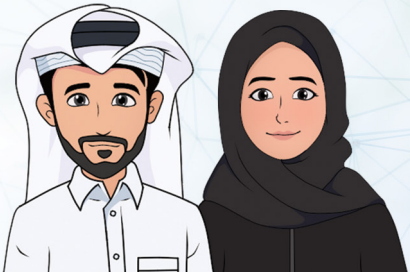
تهدف دراسة السُّوق إلى معرفة عادات الشُّراء وسلوك المُستهلِكِين واحتياجاتهم الحاليَّة.

لا بُدَّ من التَّأكُّد من جَوْدَة المعلومات عند دراسة السُّوق.



المعاملات الماليَّة الآمنة عبر الإنترنت

- عليك اتِّباع خطوات الأمان لإتمام المعاملات الماليَّة عبر الإنترنت.
- تأكَّدْ من تحديث البرامج في الحاسوب والأجهزة الإلكترونيَّة.
- كُنْ حَذِرًا عند تسوُّقك عبر الإنترنت.
- ابحثْ عن إشارات الثِّقَة والشَّهادات الرَّقميَّة.
- اقرأ اتِّفاقيَّة الخُصوصيَّة.
- احتفظْ بسجِلَّات معاملاتك عبر الإنترنت.



عمليَّات الاحتيال عبر الإنترنت

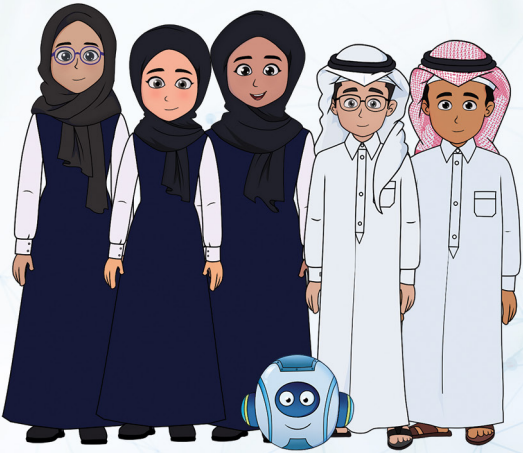
- يمكن أن نقع ضحيَّة للاحتيال الإلكترونيّ.
- يمكننا معرفة المواقع الزَّائفة إذا قدَّمت لنا تخفيضاتٍ كبيرةً.
- المواقع الزَّائفة تصميمها رديءٌ ولُغتها ضعيفة.
- عناوين URL في المواقع الزَّائفة تحتوي كلماتٍ أو أحرفًا غريبة.

إشارات الثِّقة والاتِّصال الآمِن

ينبغي وَضْع شعارات الأمان وإشارات الثِّقة على صفحات الويب.

مِن أهمّ إشارات الثِّقَة: شعار (Verified by Visa، Norton Seal)

الاتِّصال الآمِن هو اتِّصال يتمُّ تَشْفيره بواسطة بروتوكولات الأمان.

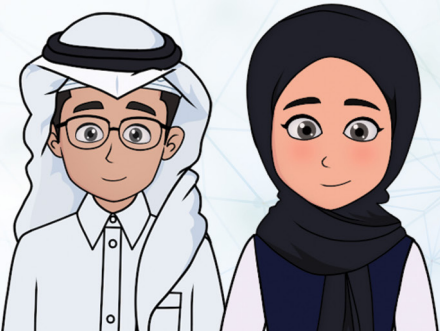


الأمن الرَّقميّ
وأمْن المعلومات

الأمن الرَّقميّ يختصُّ بحماية بيانات المُؤسَّسَة.

الأمن الرَّقميّ يختصُّ بضمان استمراريَّة العمل في المُؤسَّسَة.

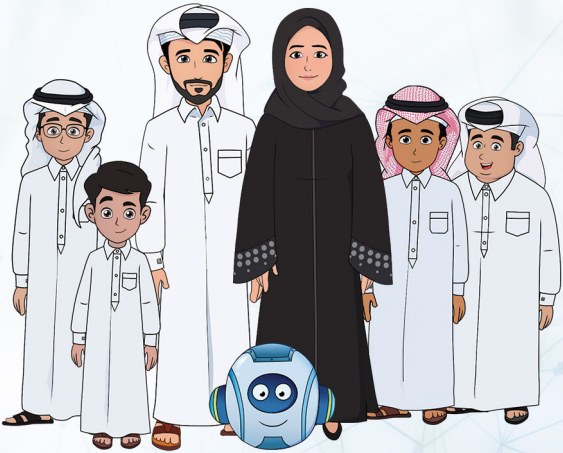
يُتيح الأمن الرَّقميّ التَّشغيل الآمِن لتطبيقات تكنولوجيا المعلومات.



أهميَّة أمن المعلومات ومُثلَّث الحماية

أهميَّة أمن المعلومات تزداد بزيادة أهميَّة البيانات والمعلومات.

يتكوّن مُثلَّث الحماية من ثلاثة عناصر: السريَّة، التَّكامل، التَّوافُر.

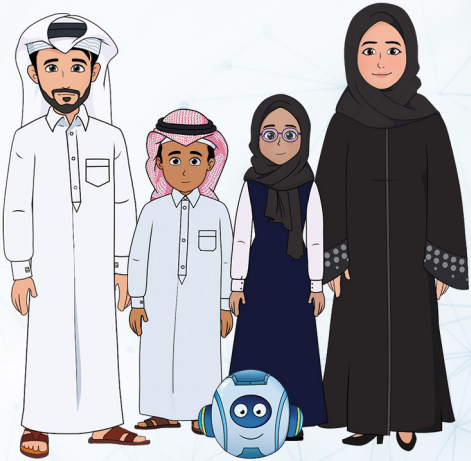


أشكال الجرائم الإلكترونيَّة

انتشرت الجرائم الإلكترونيَّة بعد اعتماد التّجارة والتَّرفيه على الأجهزة الإلكترونيَّة.

من أشكال الجرائم الإلكترونيَّة: الاحتيال الإلكترونيّ، والمُضايقات عبر الإنترنت.

من الجرائم الإلكترونيَّة أيضًا: التَّسلُّل الإلكترونيّ، سرقة الهُويَّة، وانتهاك الخُصوصيَّة.



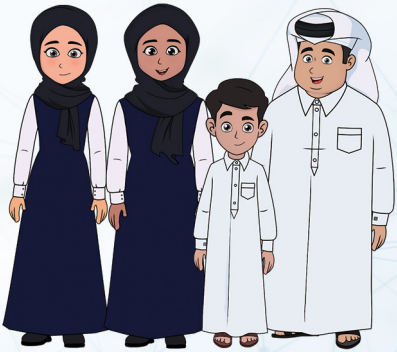
احتياطات الأمن الشَّخصيّ

عليكم إجراء تحديث دَوْريّ للبرامج، واستخدام جدار الحماية.

عليكم التَّواصُل الرَّقميّ بحَذر، واستخدام كلمات مرور قويَّة.

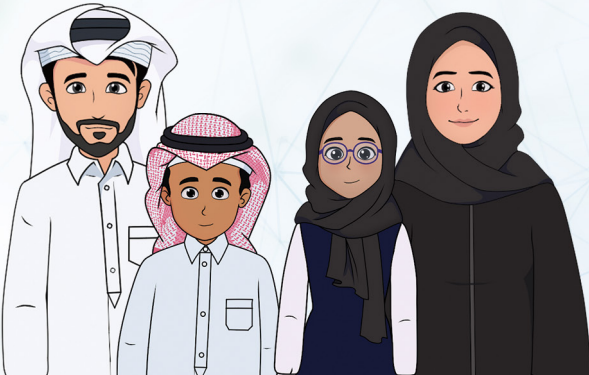
تذكروا دائمًا عمل نَسْخ احتياطيّ دَوْريّ للبيانات.

تجنَّبوا فَتْح أيّ رابط أو مُرفَق بريد إلكترونيّ من مصدرٍ مجهولٍ.



الكشف عن البرامج الضَّارَّة وإزالتها

- إذا شككتم بوجود برامج ضارَّة على حواسيبكم فتوقَّفُوا عن التَّسوُّق الإلكترونيّ.
- عليكم تحديث برامج الحماية من الفيروسات وبرامج التَّجَسُّس.
- التَّحقُّق من المُتَصَفِّح لمعرفة ما إذا كان به أدوات لحَذْف البَرامج الضَّارَّة.
- الاستعانة بالدَّعْم الفَنِّيّ من الشَّركة المُصَنِّعَة.



هجوم الفِدْيَة

Ransomware

قُمْ بالتَّحقُّق من جهاز التَّوجيه Router - وحماية كلمة المرور الخاصَّة به.

قُمْ بالتَّحقُّق من استخدام خيار أمان (WPS2) للشَّبَكة اللاسلكيَّة.

قُمْ بالتَّحقُّق من تحديثات نظام التَّشْغيل وتحديث التَّطبيقات التَّلقائيّ.

جدار الحماية Firewall
وأذونات المِلفَّات

جدار الحماية يمنع الاتِّصالات المشبوهة.

لا يستطيع جدار الحماية حمايتنا من الاحتيال الإلكترونيّ والبريد المُزْعِج.

يتمتَّع كلُّ مُستخدِمٍ للحاسوب بوُجود مِلَفّ شَخْصيّ وأُذْونات خاصَّة به.

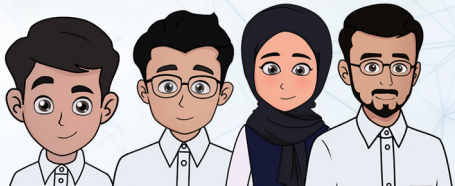
البَصْمَة الرَّقميَّة

البَصْمَة الرقميَّة هي ما نقوم به من تَصفُّح واتِّصالات وأعمال أخرى عبر الإنترنت.

للبَصمَات الرَّقميَّة نَوْعَان: البَصمَات النَّشطة، والبَصمَات المجهولة.

تُعدُّ منشوراتنا على مواقع التَّواصُل الاجتماعيّ بَصْمَة رقميَّة نَشِطَة.

البَصمَات الرَّقميَّة المجهولة نتركها دون قَصْدٍ؛ مثل المواقع التي تُحدِّد موقعنا الجغرافيّ.



تَصفُّح الشَّبكات الاجتماعيَّة بأمان

علينا أن لا نُشَارِك أيّ معلومات خاصَّة؛ مثل الرَّقم الشَّخصيّ أو تاريخ ومكان الميلاد.

علينا أن نتحقَّق من هُويَّة الأشخاص الذين نتواصل معهم.

علينا عدم مشاركة تفاصيل حياتنا الشَّخصيَّة عبر الإنترنت.

علينا مَنْع المُتَنَمِّرينَ، وأَخْذ الحَذَر من عددِ الصَّدَاقات الزَّائدة.