الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

الشريحة المستهدفة

المرأة والأسرة

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

الشريحة المستهدفة

المرأة والأسرة

كُتَيِّب المُدَرِّب

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

حقوق الملكية الفكرية

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

00974 404 663 62
00974 404 663 79
academy@ncsa.gov.qa
www.ncsa.gov.qa/

يناير 2025م
الدوحة، قطـر

تمهيد

السَّلامة الرقميَّة ركيزة أساسيَّة لضمان أمْن المعلومات، وحماية الأفراد والمجتمعات من التهديدات السيبرانية المتزايدة باستمرار.

تم تصميم هذا الكُتَيِّب بهدف توعية كبار القَدْر بمبادئ السلامة الرقمية، وأفضل الممارسات التي تساعدهم على تفادي المخاطر السيبرانية؛ حيث يهدف هذا الكُتَيِّب إلى تعزيز وعيهم حول تهديدات سيبرانية، مثل التصيد الاحتيالي، والبرمجيَّات الضَّارَّة، وتمكينهم من حماية بياناتهم وأجهزتهم بشكلٍ فعّالٍ.

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

تعريف المبادرة

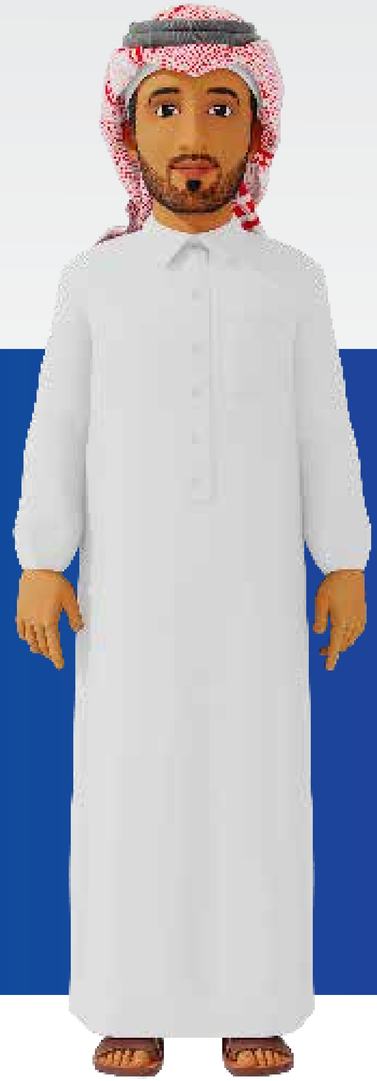
مجموعة من فعاليات التوعية في مجال السلامة الرقمية والأمن السيبراني؛ تستهدف المجتمع المحلي على اختلاف الشرائح العُمرية والاجتماعية والقطاعات المهنية.

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

الشرائح المستهدَفة

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

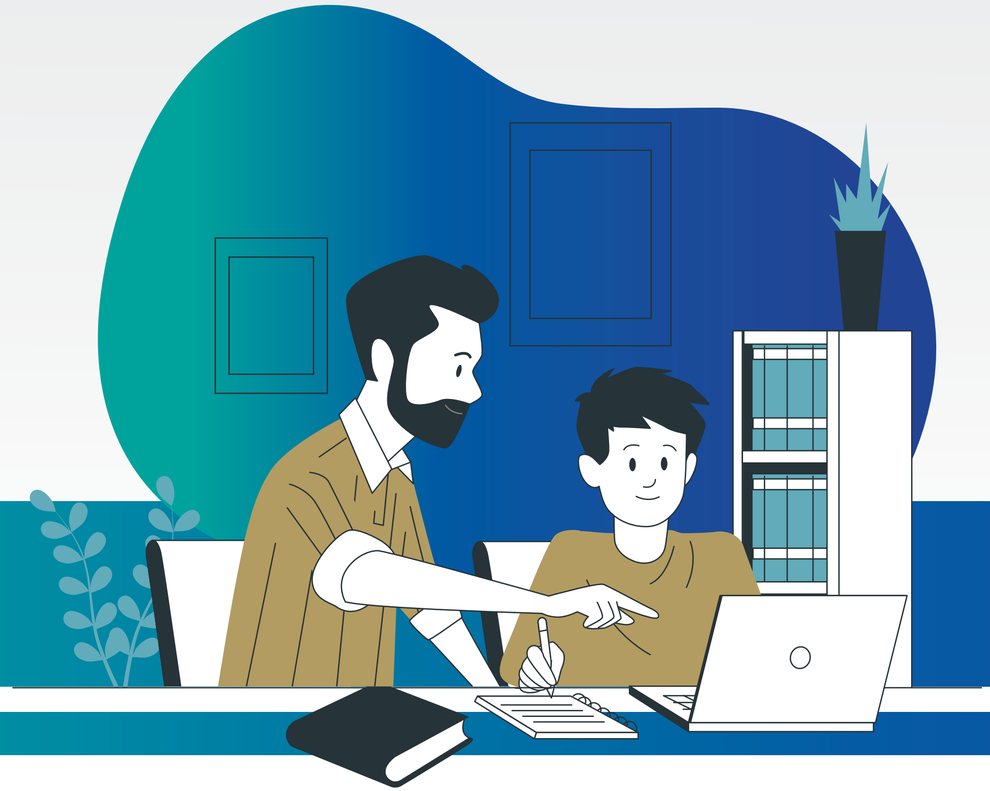
- كبار القَدْر
- المرأة والأسرة
- ذوو الاحتياجات الخاصة
- طلبة الجامعات
- العمالة الوافدة
- مؤسسات المجتمع المدني
- القطاع المالي والمصرفي



أدوات التوعية

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

- دليل السلامة الرقمية
- كتيبات توعية
- ألعاب سيبرانية
- فيديوهات توعية
- ألعاب تعليمية مبتكَرة
- ورش توعية



السَّلامة الرقميَّة للآباء

البيانات الشخصية

البيانات

تُشير إلى أيّ معلومات أو حقائق يمكن جَمْعها وتحليلها، وتشمل: الأرقام، النصوص، الصور، وغيرها. وتلعب البيانات دوراً مهماً في اتخاذ القرارات وتطوير التقنيات.

البيانات الشخصية

هي أيّ معلومات تتعلَّق بفرد معيَّن يمكن تحديد هويته من خلالها، وتشمل هذه المعلومات: الاسم، العنوان، رقم الهاتف، البريد الإلكتروني، المعلومات المالية، أو حتى العناوين الإلكترونية.

أمثلة على البيانات الشخصية

01 رقم الهوية الوطنية.

02 المعلومات الطبية والصحية.

03 بيانات الحسابات المصرفية.

04 الأنشطة عبر الإنترنت.

سرقة الهوية الرقمية

تحدث سرقة الهوية الرقمية عندما يقوم شخص غير مصرَّح له بالوصول إلى معلومات هويَّة شخص آخر على الإنترنت واستخدامها بشكلٍ غير قانوني لتحقيق مكاسب شخصية أو مالية، وتشمل هذه المعلومات بيانات الحسابات الشخصية، كلمات المرور، أو المعلومات المالية.

أمثلة على البيانات المسروقة

- أرقام بطاقات الائتمان.
- كلمات المرور.
- الأرقام القومية أو الاجتماعية.
- المعلومات البنكية.

كيف تحدث سرقة الهويَّة الرقمية؟

01

التصيد الاحتيالي

يتم خداع الضحية للكشف عن معلومات حساسة عبر رسائل أو مواقع وهمية تبدو شرعية.

02

البرمجيات الخبيثة

تثبيت برمجيات ضارَّة على أجهزة المستخدمين لجَمْع البيانات الشخصية دون علمهم.

03

اختراق قواعد البيانات

يستهدف المهاجمون الشركات أو المؤسَّسات لسرقة كميات كبيرة من بيانات المستخدمين المخزَّنة على خوادمها.

04

هجمات القوة الغاشمة

محاولة اختراق الحسابات من خلال تجربة ملايين التركيبات من كلمات المرور المحتَمَلة.

نتائج سرقة الهويَّة الرقمية

خسائر مالية

يمكـن للمجرمين اسـتخدام البيانات المسـروقة لسرقة الأمـوال مـن الحسـابات المصرفية أو إجراء عمليات شراء احتيالية.

1

التزوير

استخدام الهوية المسروقة فـي أنشـطة غير قانونيـة، مثل التوقيع على عقود أو فتح حسابات جديدة باسم الضحية.

2

الإضرار بالسُّمعة

قـد يتـم اسـتخدام الهويَّـة المسـروقة لتنفيـذ أنشـطة غيـر مشـروعة؛ ممـا يـؤدّي إلـى إلحـاق ضَـرر بسُـمعة الضحيـة.

3

مخاطر سرقة الهويَّة الرقمية

سرقة بيانات الهويَّة الرقمية تهديد خطير يُواجِه المستخدمين على الإنترنت، وتحدث عندما يحصل شخص ما بشكلٍ غير قانوني على المعلومات الشخصية لشخصٍ آخر، ويمكن الحماية من هذا التهديد من خلال:

- تقليل المعلومات الشخصية المنشورة على الإنترنت.
- كتابة كلمات مرور قوية وتغييرها بشكلٍ دوريّ.
- عدم فتح الروابط المرفقة في رسائل البريد الإلكتروني الواردة من مجهولين.

حقائق ومعلومات

يتطلَّب تأمين البيانات الشخصية على الإنترنت اتِّباع ممارسات أمنية، مثل: استخدام كلمات مرور قوية وتحديث التطبيقات بشكلٍ منتظمٍ.

التصيد الاحتيالي

هو نوع من الهجمات الإلكترونية التي يستخدم فيها المهاجمون رسائل بريد إلكتروني أو مواقع ويب مزيَّفة لخداع الأشخاص للكشف عن معلومات حساسة، مثل كلمات المرور، أو بيانات الحسابات المصرفية.

كيف يعمل التصيد الاحتيالي؟

01

الرسائل الاحتيالية

يُرسِل المهاجم بريداً إلكترونياً يبدو أنه من مصدر موثوق، مثل بنك أو شركة معروفة.

02

المواقع المزيَّفة

تحتوي الرسالة على رابط يقود إلى موقع مزيَّف يبدو مشابهاً للموقع الأصلي؛ حيث يُطلَب من الضحية إدخال معلوماته الشخصية.

03

استغلال المعلومات

بمجرد أن يُقدِّم الضحية بياناته، يتم استخدامها لسرقة الأموال أو الوصول إلى حساباته الخاصة.

التبرُّع عبر الإنترنت والتصيد الاحتيالي

قد تكون دعوات التبرُّع عبر الإنترنت أداةً للتصيد الاحتيالي، وللوقاية منها يُفضَّل اتِّباع النصائح التالية:

01 تحقَّق من موقع المؤسسة الخيرية، وتأكَّد من وجود معلومات واضحة حول كيفية التبرُّع وبيانات الاتصال والعنوان.

02 تأكَّد من إدراج المؤسسة الخيرية رسمياً في سجلَّات الجهات المعنيَّة، مثل هيئة تنظيم الأعمال الخيرية في قطر.

03 تجنَّب التبرُّع عن طريق التحويلات البنكية، وتأكَّد عند التبرُّع عبر الإنترنت أن صفحة الويب تبدأ بـ"https".

التبرُّع عبر الإنترنت والتصيد الاحتيالي

04 تجنَّب التبرُّع بالعملات المشفَّرة؛ فقد تكون مؤشراً على الاحتيال.

05 راجِع حسابك المصرفي بعد التبرُّع للتأكُّد من خصم المبلغ المحدَّد فقط، واحتفظ بسجلّ التبرعات.

06 احذر من المناشدات التي تحتوي على تفاصيل قليلة أو وعود بجوائز وهدايا مقابل التبرُّع.

علامات تؤكِّد تعرُّض الأجهزة الإلكترونية للاختراق

01 تلقِّي إشعارات عبر البريد الإلكتروني حول محاولات تسجيل الدخول إلى الحسابات رغم عدم فعل ذلك.

02 بطء الجهاز وارتفاع حرارته، وتأخُّر تنفيذ الأوامر التي يتلقَّاها من المستخدِم.

03 ظهور نوافذ منبثقة تحتوي على رسائل مزعجة.

04 فتح نوافذ المتصفِّح وعلامات التبويب والتطبيقات الموجودة على جهاز المستخدِم الخاص من تلقاء نفسها.

05 تلقِّي رسائل بريد عشوائية في صندوق الوارد.

06 إعادة توجيه المستخدِم المستهدَف باستمرار إلى مواقع الويب غير المرغوب فيها.

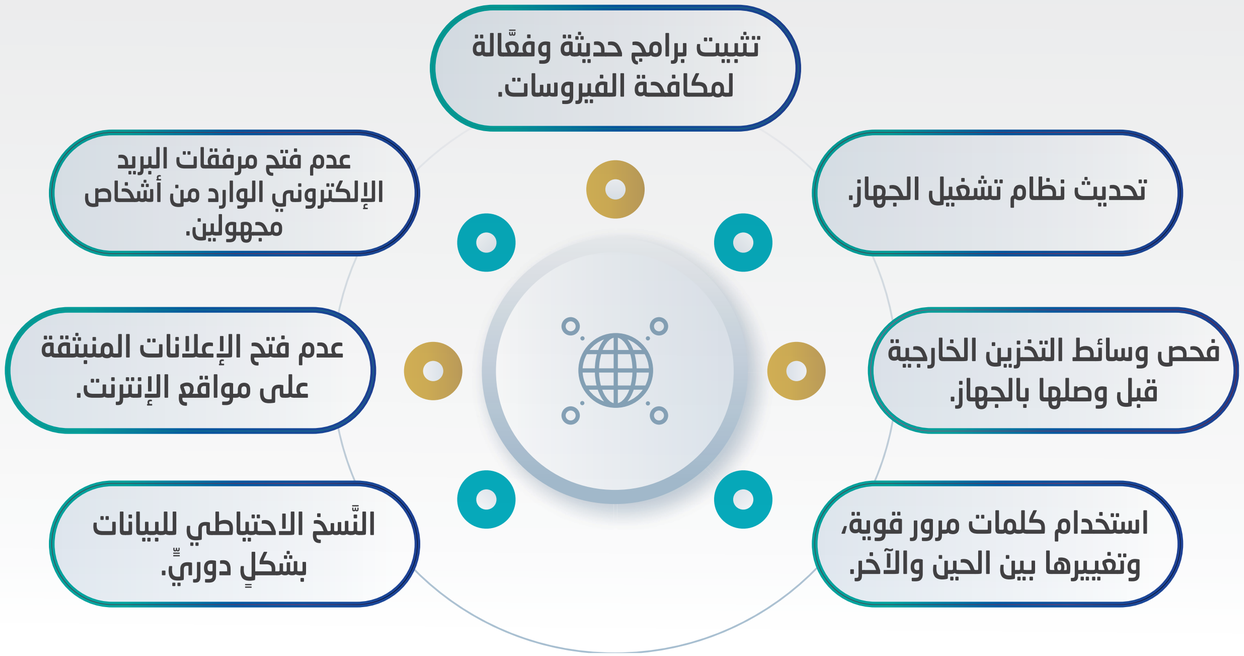
برمجيات الفدية (Ransomware)

- هي نوع من الهجمات السيبرانية التي تستهدِف الأفراد والمؤسَّسات.
- تعمل هجمات برمجيات الفدية على تشفير البيانات، ومَنْع المستخدِم من الوصول إليها إلا بعد دَفْع فدية مالية.
- في حال عدم دَفْع الفدية قد يقوم المهاجِم بإتلاف البيانات.

احذر!

تجنَّب تحميل برامج مكافحة الفيروسات أو برامج الأمان من مصادر غير رسمية؛ فقد تكون هذه البرامج نفسها تحتوي على برمجيات ضارة.

الحماية من برمجيات الفدية (Ransomware)



احذر!

تجنَّب الرَّد على الرسائل النصية التي تطلب منك معلومات شخصية أو مالية؛ فغالباً ما تكون هذه الرسائل جزءاً من عملياتٍ احتياليةٍ.

التَّنمُّر الإلكتروني وطرق وقاية الأطفال منه

- يُعدّ التَّنمُّر الإلكتروني أحد أخطر التَّحدّيات التي يُواجهها الأطفال في العالَم الرقميّ؛ حيث يمكن أن يُسبِّب لهم أضراراً نفسية واجتماعية طويلة الأمد.
- ويتمثل التَّنمُّر الإلكتروني في نَشْر التعليقات السلبية، أو الصُّور المسيئة، أو الرسائل المزعجة التي تهدف إلى إزعاج الأطفال أو إحراجهم عبر الإنترنت.

طرق الوقاية من التَّنمُّر الإلكتروني

تعزيز الوعي

تعليم الأطفال كيفية التعرُّف على التَّنمُّر الإلكتروني، وتشجيعهم على التحدُّث عند مواجهته.

المراقبة والإرشاد

مُتابعة نشاط الأطفال على الإنترنت بشكلٍ وُدّي، مع توجيههم إلى استخدام المنصات بشكلٍ آمِن.

إعدادات الخصوصية

ضَبْط إعدادات الخصوصية على وسائل التواصل الاجتماعي لتقليل الوصول غير المرغوب فيه.

عدم الرَّدّ على المتنمرين

تعليم الأطفال عدم الرَّدّ على الرسائل المسيئة، وحَظْر الحسابات المُزعِجَة.

طرق الوقاية من التَّنمُّر الإلكتروني

توثيق الأدِلَّة

الاحتفـــاظ بأدلَّـة على التَّنمُّر الإلكترونيّ (مثل لقطات الشاشة) للإبلاغ عنها للجهات المختصَّة.

الاستعانة بالمختصِّين

التَّحدُّث مع المستشارين أو خبراء الصِّحَّة النفسية إذا تأثرت الحالة النفسية للطفل.

استخدام برامج الحماية

تثبيت برامـج للتَّحكُّـم الأبوي التي تُراقـــب الأنشطـــة وتَحُـدّ من المخاطر.

العادات الرقمية الآمِنَة للعائلات

في ظلّ التَّطوُّر الرقميّ المتسارع، أصبحت العادات الرقمية الآمِنَة ضرورة للحفاظ على سلامة العائلات وحمايتها من المخاطر الإلكترونية. تُساعد هذه العادات في تعزيز استخدام التكنولوجيا بشكلٍ مسؤولٍ وآمِن لجميع أفراد الأسرة.

أهمّ العادات الرقمية الآمِنة للعائلات

وضع قواعد رقمية مشتركة

تحديد أوقات استخدام الأجهزة الإلكترونية، ونوعية المحتوى المسموح بمشاهدته.

مراقبة الأنشطة الرقمية

متابعة نشاط الأطفال على الإنترنت دون انتهاك خصوصيتهم، لضمان بقائهم بعيدًا عن المخاطر.

التثقيف المستمر

توعية جميع أفراد الأسرة حول التهديدات الإلكترونية، مثل التصيد الاحتيالي والتَّمَّر الإلكترونيّ.

استخدام أدوات الرقابة الأبوية

تثبيت تطبيقات أو برامج للتحكُّم في المحتوى وضبط إعدادات الخصوصية.

التواصل المفتوح

إنشاء بيئة داعمة لتشجيع الأطفال على التحدُّث بحُرِّيَّة عن تجاربهم الرقمية.

أهمّ العادات الرقمية الآمِنة للعائلات

تحديث البرامج بانتظام

الحرص على تحديث أنظمة التشغيل والتطبيقات لتجنُّب الثغرات الأمنية.

استخدام كلمات مرور قوية

تعليم أفراد الأسرة إنشاء كلمات مرور قويَّة وعدم مشاركتها مع الآخرين.

الحذر من الغرباء

توجيه الأطفال لتجنُّب التفاعل مع الغرباء عبر الإنترنت، والإبلاغ عن أيّ سلوك مُخالِف.

تقليل الاعتماد على الشبكات العامة

توجيه الأسرة لاستخدام شبكات إنترنت آمِنَة، خاصَّة عند إجراء المعاملات المالية، أو مشاركة البيانات الحسَّاسة.

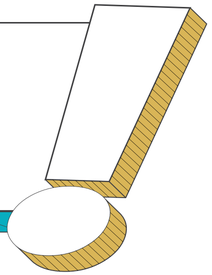
السلامة الرقمية للأطفال

أخطاء يرتكبها المستخدمون تُوقِعهم ضحايا للاحتيال عبر الإنترنت

- التصفُّح على شبكة Wi-Fi العامة دون استخدام شبكة افتراضية خاصة (VPN).
- مشاركة كثيرٍ من المعلومات الشخصية على وسائل التواصل الاجتماعي.
- تشابه كلمات المرور لعدد من الحسابات عبر الإنترنت.
- عدم تثبيت تحديثات البرامج تلقائياً؛ مما يزيد من فرص تسلُّل الفيروسات إلى نظام التشغيل.

أخطاء يرتكبها المستخدمون تُوقِعهم ضحايا للاحتيال عبر الإنترنت

- فتح الروابط من رسائل البريد الإلكتروني دون التحقُّق من موثوقيَّتها.
- الانسياق وراء الرسائل البريدية التي تحتوي على فرص هدايا وجوائز دون التحقُّق منها.
- تجاهُل ميزات الأمان الأساسية، ومن بينها المصادقة الثنائية.
- التسوُّق الإلكتروني من خلال مواقع غير موثوقة.



احذر!

احترس من الرسائل التي تطلب منك مشاركة بيانات حساسة بشكلٍ عاجلٍ، أو تلك التي تدَّعي أنها من جهات رسمية وتطلب منك معلوماتك الشخصية.

قواعد التصفُّح الآمِن للإنترنت

1. تثبيت برامج حديثة لمكافحة الفيروسات.
2. عدم فتح الإعلانات المنبثقة على صفحات الويب.
3. تحميل البرامج والتطبيقات عن طريق المواقع الموثوقة.
4. عدم إجراء أي عمليات شراء عن طريق مواقع تجارة إلكترونية غير موثوقة.
5. كتابة كلمات مرور قوية وتغييرها باستمرار.
6. عدم فتح مرفقات البريد الإلكتروني الوارد من مجهولين.
7. تفعيل جدار الحماية.

حماية المعلومات الشخصية

عدم مشاركة المعلومات الشخصية

تجنَّب مشاركة البيانات الحساسة عبر الإنترنت.

استخدام برامج حماية موثوقة

استخدام برامج حماية من الفيروسات وبرمجيات التجسُّس.

التحديث الدوري للبرامج والنُّظُم

تحديث البرامج بانتظامٍ لسدّ الثغرات الأمنية.

حقائق ومعلومات

تُشير تقارير شركات الأمن السيبراني إلى أن حجم الهجمات السيبرانية العالمية يتضاعف سنوياً؛ مما يُسلِّط الضوء على أهمية تعزيز التدابير الأمنية.

المصادقة الثنائية

هي طبقة إضافية من الأمان تُستخدم لحماية الحسابات الشخصية، فبدلاً من الاعتماد فقط على كلمة المرور، تُضيف المصادقة الثنائية خطوةً ثانيةً للتأكُّد من هويَّة المستخدِم؛ مما يجعل من الصعب على المتسلِّلين الوصول إلى الحسابات، حتى لو تمكنوا من سرقة كلمة المرور.

كيفية العمل

يتم تحقيق المصادقة الثنائية عن طريق الجمع بين شيئين:

* **1. شيء تعرفه (كلمة المرور)**

  وهو الذي يتم إدخاله عند تسجيل الدخول.

* **2. شيء تملكه (رمز مؤقت أو جهاز)**

  مثل رمز يُرسَل إلى هاتفك المحمول أو تطبيق المصادقة.

أهمية المصادقة الثنائية

المصادقة الثنائية تعزيز لأمان أجهزتك وبياناتك الشخصية.

من خلال المصادقة الثنائية، لا يكفي إدخال كلمة المرور للدخول إلى حساباتك.

قد تكون المصادقة الثنائية من خلال تأكيد تسجيل الدخول باستخدام بصمة اليد أو العين أو الوجه، أو من خلال التأكيد باستخدام رقم الهاتف الجوال.

احذر!

النقر على الإعلانات غير المعروفة أو المشبوهة التي تظهر في أثناء تصفُّح الإنترنت؛ قد يقودك إلى مواقع ضارة أو يؤدي إلى سرقة بياناتك.

إعدادات الخصوصية

تحتوي معظم الخدمات المتوفِّرة على الإنترنت على إعدادات تُتيح لك التحكُّم في عدة أمور، مثل:

مَن يمكنه رؤية ما تنشره، كما هو الحال على منصات التواصل الاجتماعي؛ مما يُتيح لك النشر للأصدقاء فقط، أو لأصدقاء أصدقائك، أو للجميع.

تقييد منشورات محدَّدة على مجموعة من الأشخاص كأفراد الأسرة، فهي تمنحك خيارات جعل منشوراتك عامَّة أو خاصَّة.

تساعد إعدادات خصوصية الهواتف الذكية أيضاً في تقييد حقّ الوصول إلى موقعك وجهات الاتصال والمعلومات الشخصية الخاصة بك.

حقائق ومعلومات

ازداد عدد هجمات الحرمان من الخدمة (DDoS) بشكلٍ ملحوظٍ في السنوات الأخيرة؛ مما أدَّى إلى تعطيل مواقع الويب والخدمات الرقمية بشكلٍ واسعٍ.

أمن الهويَّة الرقمية وأمن كلمات المرور

لحماية الهويَّة الرقمية لا بدّ من استخدام كلمات مرور قوية

01 إنشاء كلمات مرور قوية يصعب تخمينها، ولحمايتها من السرقة يمكن استخدام مدير كلمات المرور لتخزينها بشكلٍ آمِنٍ.

02 اختيار كلمات مرور مؤلَّفة من مزيج من الحروف والأرقام والرموز.

03 في حال الرغبة في إضافة طبقة أمان أخرى، يمكن تفعيل المصادقة الثنائية فهي تُحقِّق ذلك.

04 عدم استخدام أيّ كلمة مرور لحسابات أو خدمات متعددة.

05 تغيير كلمات المرور بشكلٍ دوريّ.

حقائق ومعلومات

التصيد الاحتيالي هو أحد أكثر أساليب الهجمات شيوعاً؛ حيث يتم إغراء المستخدمين لتقديم معلوماتهم الشخصية عبر رسائل مزيَّفة.

إجراءات حماية الهُويَّة الرقمية

مُراقَبة الحسابات المصرفية

يُعدّ التحقُّق من الحساب المصرفيّ عبر الإنترنت بانتظام أمراً ضرورياً لرَصْد أيّ نشاط مُخالِف، واتخاذ الإجراء المناسب لمَنْع وقوع أضرار جسيمة تُؤدّي إلى سرقة الأموال، أو تُؤثّر على السُّمعة الشخصية.

الحذر عند التخلُّص من البيانات المُهمَّة

عند التخلُّص من أوراق أو مستندات تحتوي على معلومات شخصيَّة، ينبغي التخلُّص منها بشكلٍ آمِنٍ؛ منعاً من وصولها إلى أيدي المحتالين.

ينطبق الأمر كذلك على الحواسيب والهواتف، ففي حال الرغبة في بيعها لشراء الجديد منها؛ يجب التأكُّد من مَسْح جميع البيانات الشخصية المخزَّنة عليها.

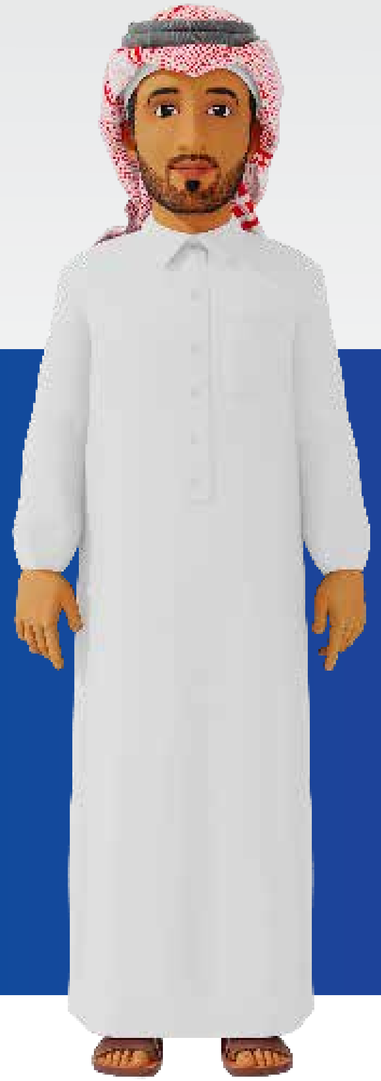
كلمات المرور

خاتمة

تُعدّ السلامة الرقمية مسؤولية شخصية وجماعية تتطلّب الوعي واليقظة، ومن خلال اتّباع نصائح بسيطة لتعزيز السلامة الرقمية للأسرة؛ بدءاً من إدارة كلمات المرور بشكلٍ آمِن، مروراً بحماية البيانات الشخصية، ووصولاً إلى الوقاية من التَّنمُّر الإلكترونيّ، والتعامل مع هجمات التصيد الاحتيالي. تُمثِّل هذه التدابير خطوات أساسيَّة لحماية الأسرة في مُواجهة التحديات الرقمية المتزايدة.

عن طريق الوَعْي والالتزام بهذه الإجراءات المُهمَّة؛ نستطيع جميعاً المُشارَكة في بناء بيئة رقميَّة آمِنَة، وتعزيز الأمن السيبراني والسلامة الرقمية في المجتمع.

قبل أن نختم يُرجَى التفضل بإدراج بياناتكم وتقييم الورشة، وعليه، يُرجَى مسح الرابط الآتي:



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative