الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

أمـــان الأجهـــزة المحمـــولة

الشريحة المستهدفة
كبـــار القـــدْر

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مبادئ عامة في السلامة الرقمية
أمان الأجهزة المحمولة

الشريحة المستهدفة

كبـــار القـــــدْر

كُتَيّب المُدَرّب

المبادرة الوطنية للسلامة الرقمية

الفهرس	رقم الصفحـة

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 في أثناء استخدام الأجهزة المحمولة، وأفضل الممارسات التي تساعدهم على تفادي مخاطرها السيبرانية؛ حيث يهدف هذا الكُتَيّب إلى تعزيز وعيهم بأبرز هذه التهديدات؛ مثل اختراق البيانات، وسرقة الهوية الرقمية، والبرمجيَّات الضَّارَّة.

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

المبادرة الوطنيّة للسلامة الرقميّة

Digital Safety National Initiative

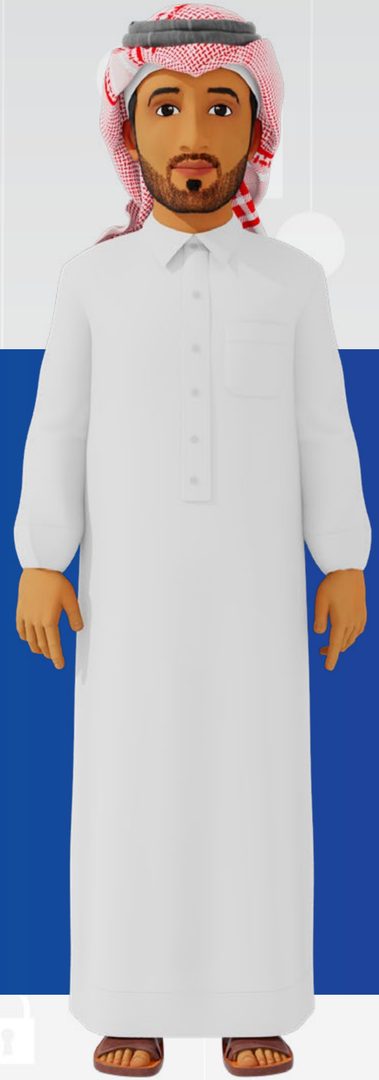
تعريف المبادرة

مجموعة من فعاليات التوعية في مجال السلامة الرقمية والأمن السيبراني؛ تَستهدف 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:

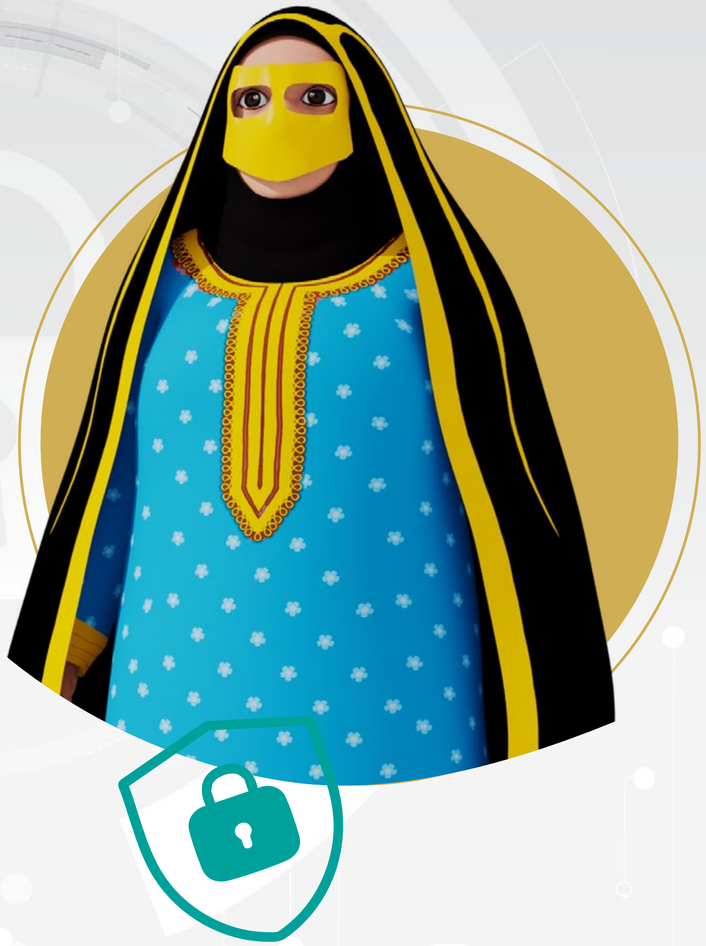


- كبار القَدْر
- المرأة والأسرة
- ذوو الاحتياجات الخاصة
- طلبة الجامعات
- العمالة الوافدة
- مؤسسات المجتمع المدني
- القطاع المالي والمصرفي

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



المحور الأول

مخاطر الأجهزة المحمولة

ما هي الأجهزة المحمولة؟

الأجهزة المحمولة هي الأدوات الإلكترونية التي يمكن حَمْلها بسهولة واستخدامها في أيّ مكان.

أنواع الأجهزة المحمولة الشائعة:

- الأجهزة اللوحية
- الهواتف الذكية
- أجهزة القراءة الإلكترونية
- بعض الساعات الذكية التي تتّصل بالهاتف

لماذا تُعتبر الأجهزة المحمولة هدفًا للمحتالين؟

لأنها تحتوي على معلومات شخصية ومهمة؛ ولأن استخدامها الواسع يجعلها وسيلة مُفضَّلة للوصول إلى الأشخاص.

أسباب استهداف الأجهزة المحمولة:

- تخزين الأرقام والصور والمحادثات
- وجود تطبيقات بنكية وحسابات إلكترونية
- ضَعْف الحماية في بعض الأجهزة القديمة
- سهولة خداع المستخدمين عبر التطبيقات والروابط
- إمكانية تتبُّع الموقع أو التحكُّم عن بُعْد في بعض الحالات

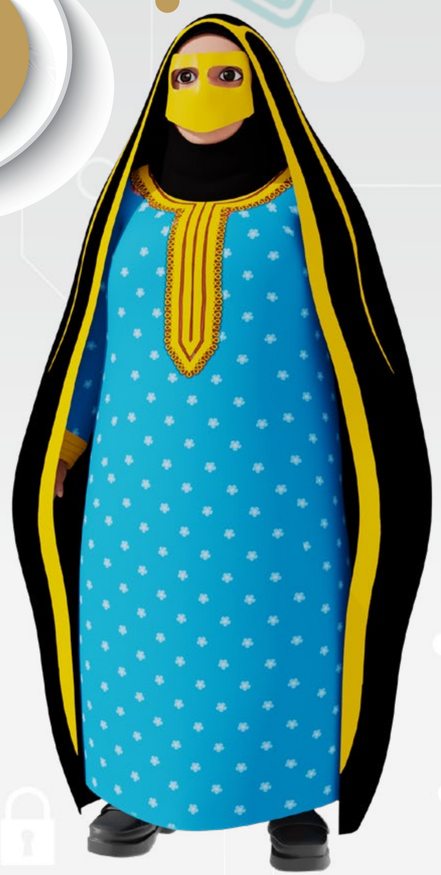
أنواع البيانات التي يُخزّنها الجهاز المحمول

الجهاز المحمول لا يقتصر على المكالمات، بل يُخزّن الكثير من المعلومات الحساسة التي يمكن استغلالها في حال اختراق الجهاز.

البيانات الشائعة المخزنة في الأجهزة:

- الأسماء وأرقام الهواتف
- الصور والمقاطع الشخصية والعائلية
- كلمات المرور للحسابات المختلفة
- ملفات العمل أو الوثائق الرسمية
- رسائل (واتساب WhatsApp ، SMS)
- مواقع التنقل والسجل الجغرافي

تهديدات الأجهزة المحمولة



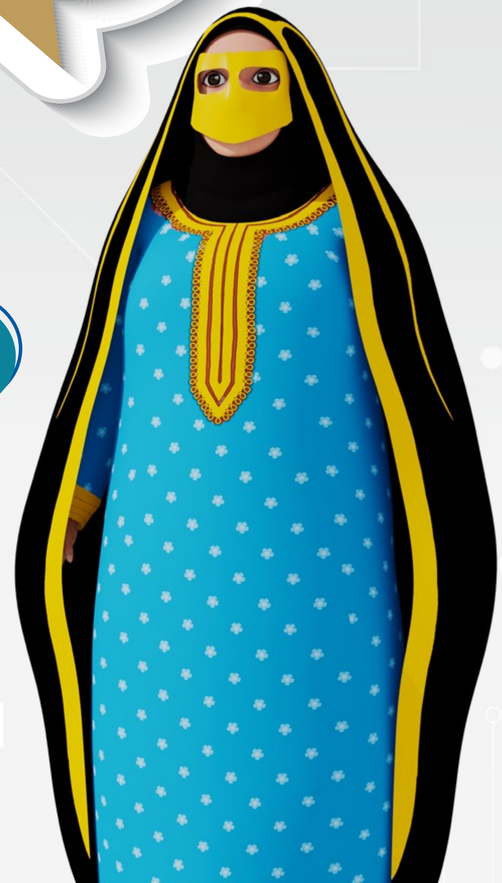
هنـاك مجموعـة متنوّعـة مـن المخاطـر التـي تُهـدِّد سلامـة الأجهزة المحمولة ومحتوياتها، ويمكن أن تَحْدث دون أن يشعر بهـا المسـتخدم.

التهديدات الشائعة للأجهزة المحمولة:

- الفيروسات والبرمجيات الخبيثة
- التنصُّت على المكالمات أو الكاميرا
- سرقة البيانات من خلال التطبيقات
- تتبُّع الموقع الجغرافي دون إذن
- التوصيل بشبكات Wi-Fi ضارَّة أو مُختَرقة

كيف يُمكن أن يتعرَّض الجهاز للاختراق؟

يحدث الاختراق عندما يتمكَّن شخص غير مصرَّح له من الدخول إلى الجهاز أو الوصول إلى محتوياته دون عِلْم صاحبه.



الطرق الشائعة لاختراق الهواتف:

- تحميل تطبيقات مزيَّفة تحتوي على برمجيات خبيثة
- الضغط على روابط احتيالية داخل رسائل أو مواقع
- الاتصال بشبكات Wi-Fi غير آمِنَة
- مشاركة معلومات الدخول أو كلمات المرور مع الغرباء
- فقدان الهاتف بدون كلمة مرور

مخاطر فقدان الجهاز أو سرقته

في حال فقدان الجهاز المحمول أو سرقته، فإن كل البيانات الموجودة عليه تكون مُهدَّدة، خصوصًا إذا لم يكن مُؤمَّنًا جيدًا.

المشكلات الناتجة عن فقدان الهاتف:

- الوصول غير المصرّح به إلى الحسابات البنكية
- الاطلاع على الصور والمحادثات الخاصة
- إرسال رسائل باسمك إلى الآخرين
- فتح البريد الإلكتروني أو التطبيقات الحساسة
- استخدام بطاقة SIM لإجراء مكالمات أو تحويلات

معلومة

يمكن حماية بياناتك عبر تمكين خيار مَسْح البيانات تلقائيًّا بَعْد عدَّة مُحاولات فاشلة لإدخال كلمة المرور.

السؤال التفاعلي الأول

1- ما نوع البيانات التي قد تكون مُهدّدة في حال اختراق الأجهزة المحمولة؟

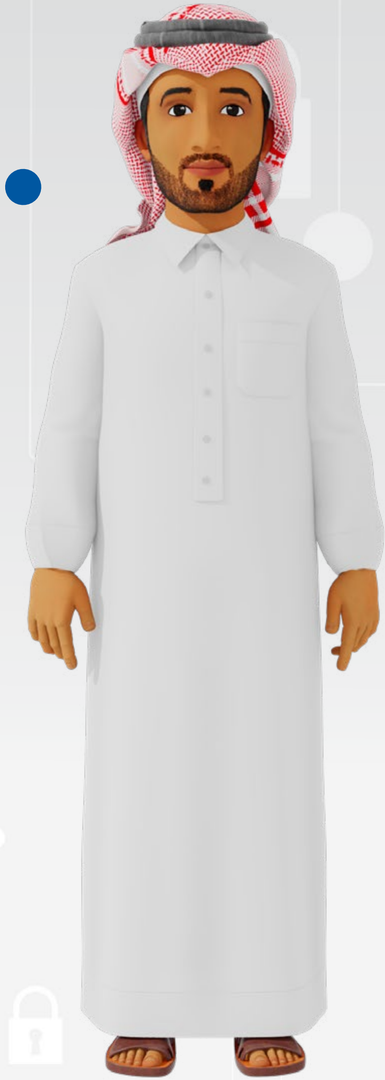
أ. | فقط الصور

ب. | أرقام الهواتف فقط

ج. | كلّ البيانات المخزَّنة مثل الصور، الحسابات، المحادثات

د. | التطبيقات المثبّتة فقط

السؤال التفاعلي الثاني



2- ما الذي يُميّز متجر التطبيقات الرسمي عن غير الرسمي؟

أ. | التطبيقات فيه أرخص

ب. | يُوفّر تطبيقات أكثر حجمًا

ج. | يخضع للمراقبة الأمنية والفحص

د. | لا يسمح بتنزيل الألعاب

السؤال التفاعلي الثالث

3- مَا أوَّل خطوة تساعد على حماية الأجهزة المحمولة من المخاطر؟

أ. وَضْع قفل شاشة وكلمة مرور

ب. فتح الروابط دون تحقّق

ج. تحميل التطبيقات من أيّ موقع

د. عدم استخدام الإنترنت

السؤال التفاعلي الرابع

4- ما فائدة التحديثات التي تصل إلى الأجهزة المحمولة؟

أ. تغيير شكل الجهاز

ب. زيادة سرعة الإنترنت

ج. تقليل حجم التطبيقات

د. تحسين الحماية وسد الثغرات الأمنية

البرمجيات الضارَّة

بعض التطبيقات التي تبدو عادية قد تحتوي بداخلها برمجيات ضارَّة تهدف إلى سرقة المعلومات أو مراقبة الأجهزة.

- طرق انتشار هذه التطبيقات
- التحميل من مواقع غير رسمية أو روابط في الرسائل
- إعلانات مُضلّلة تَعِد بخدمات مجانية أو جوائز
- تقليد تطبيقات شهيرة بأسماء مشابهة
- طلب صلاحيات مُفْرِطة مثل الوصول للكاميرا أو الميكروفون
- العمل في الخلفية دون عِلْم المستخدم

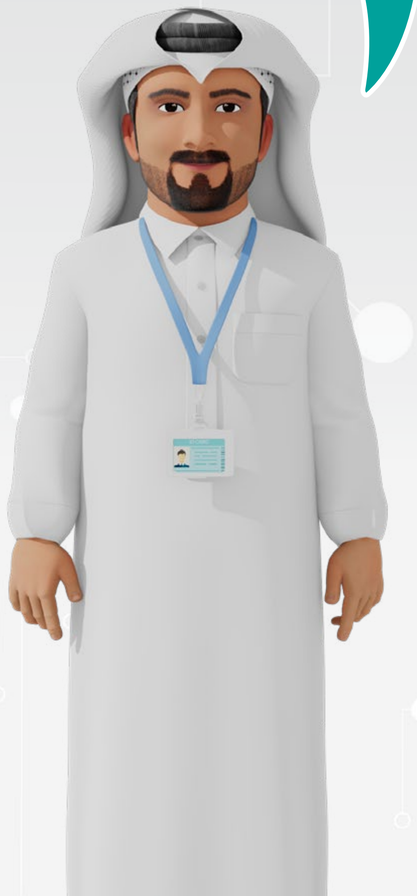
التنزيلات التلقائية والبرمجيات المخفية

أحيانًا يقوم الجهاز بتحميل ملفات أو تطبيقات دون عِلْم المستخدِم، خاصةً عند زيارة مواقع مشبوهة.

كيف تحدث التنزيلات التلقائية؟

- من خلال الضغط على إعلانات معينة داخل المتصفح
- عند الدخول إلى مواقع غير آمِنَة
- عبر الروابط القصيرة التي تبدأ التحميل تلقائيًّا
- من خلال النوافذ المنبثقة التي تطلب "تأكيد فوري"
- باستخدام رسائل احتيالية مزروعة داخل تطبيقات ضعيفة الحماية

روابط الاحتيال في الرسائل النصية



قد تصل رسالة تحتوي على رابط، يبدو بسيطًا، لكنَّه يُؤدي إلى موقع يسرق بيانات الجهاز أو يُثبّت برنامج تجسُّس.

الخصائص الشائعة لهذه الروابط:

- تأتي من أرقام غير معروفة أو مجهولة المصدر
- تحتوي على رسائل مثل "جائزتك جاهزة"، "تم إيقاف حسابك"، "اضغط لتحديث معلوماتك"
- تكون مختصرة بشكل يصعب التحقُّق منه
- بمجرد الضغط، يُطلب إدخال بيانات شخصية أو بنكية
- قد تؤدي إلى تنزيل تطبيق ضارّ على الجهاز

الرسائل الاحتيالية داخل المتصفحات

في أثناء تصفُّح الإنترنت، قد تظهر رسائل تُشبه تنبيهات النظام أو إشعارات رسمية لكنَّها مزيَّفة تمامًا.

أمثلة على هذه الرسائل:

- "رصيدك سينتهي قريبًا، اضغط للتجديد"
- "تم اكتشاف فيروس على جهازك، اضْغَط لحذفه"
- "تطبيقك غير مُحدَّث، اضغط الآن"
- "ربحت جائزة كبرى! اضغط للمطالبة بها"

تحتوي جميعها على روابط تؤدي إلى تحميل برامج غير موثوقة

التصيّد من خلال تطبيقات المحادثة

يستخدم البعض تطبيقات مثل واتساب WhatsApp أو تيليجرام Telegram لإرسال روابط أو رسائل احتيالية بهدف الوصول إلى الجهاز.

آليات التصيُّد داخل التطبيقات:

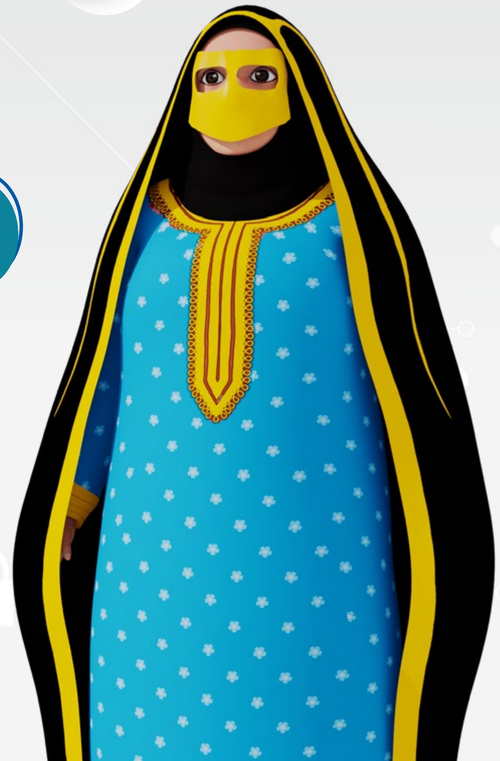
- إرسال رسائل من أرقام غير محفوظة تدّعي أنها من الأقارب أو الأصدقاء
- مشاركة روابط تبدو عادية لكنّها تؤدي إلى مواقع مزيفة
- استخدام حسابات مُختَرقة تطلب تحويلات مالية
- استخدام صور أو مقاطع لإقناع الضحية بالمشاركة أو الرد
- عرض عروض "مغرية" تتطلب تثبيت تطبيق معين

الإعلانات المُضلّلة في التطبيقات المجانية

تُوفّر بعض التطبيقات المجانية مساحة للإعلانات، ويقوم بعض المحتالين بوضع إعلانات مُزيَّفة تَستدرج المستخدم.

أنواع الإعلانات الخطرة داخل التطبيقات:

- إعلان عن وظيفة أو جائزة وهمية
- إعلان لتحميل تطبيق يُظهر أنه "مُسرِّع للجهاز" أو "يُوفّر الإنترنت"
- إعلان يطلب إدخال رقم الهاتف للاشتراك
- إعلان يقود إلى متجر تطبيقات غير رسمي
- إعلانات تظهر فجأة وتُغلَق بصعوبة



الاتصال بشبكات Wi-Fi عامَّة

الإنترنت المجاني في الأماكن العامة قد لا يكون آمنًا، وقد يُستخدَم في عمليات مراقبة أو اختراق.

مخاطر استخدام Wi-Fi العامة:

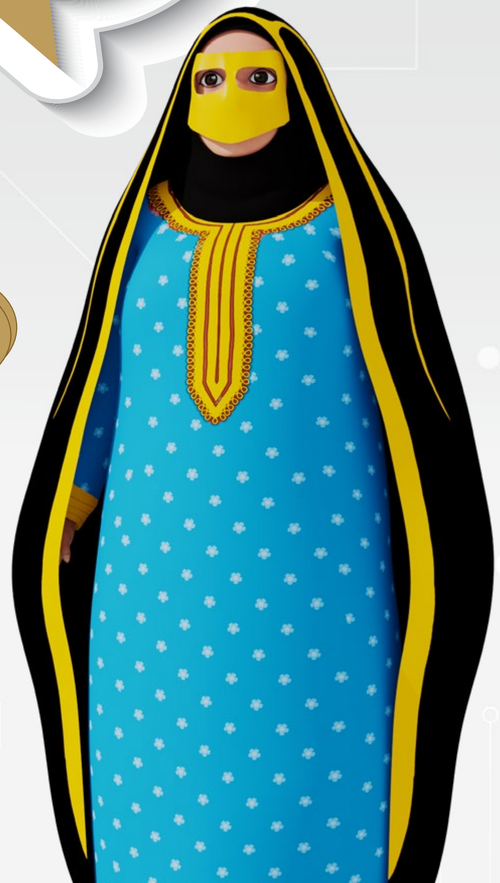
- مراقبة نشاط الجهاز وتحديد موقعه
- إمكانية التجسُّس على نشاط الجهاز
- سرقة البيانات التي يتم إرسالها أو استقبالها
- إدخال المستخدِم إلى شبكة تحتوي على برمجيات خبيثة
- فقدان السيطرة على الجهاز في بعض الحالات
- خداع المستخدِم بعرض شبكة باسم مُزيَّف
- استخدام اتصالك في عمليات غير قانونية دون عِلْمك
- الوصول إلى كلمات المرور عند إدخالها في مواقع غير مشفَّرة

التتبُّع الجغرافي والتجسُّس

بعض التطبيقات أو الروابط تُفعّل خاصية تتبُّع الموقع أو تفتح الكاميرا والميكروفون دون إذن واضح..

أساليب التجسس:

- تثبيت تطبيق تجسُّس يُرسل الصور والمحادثات إلى شخص آخر
- التقاط الصور دون عِلْم المستخدِم
- تحديد مكان وجود الشخص لحظة بلحظة
- تسجيل نشاط الجهاز وإرساله إلى جهة خارجية
- تشغيل الميكروفون والاستماع إلى المكالمات أو الأصوات



اختراق الكاميرا والميكروفون

يمكن لبعض البرامج اختراق الجهاز وتشغيل الكاميرا أو الميكروفون في الخلفية دون أن يظهر شيء للمستخدِم.

مؤشرات قد تدلّ على هذا النوع من الاختراق:

- انخفاض غير طبيعي في بطارية الجهاز
- ظهور ضوء الكاميرا دون فتح التطبيق
- سخونة الجهاز دون استخدام
- ضوضاء غير معتادة أثناء المكالمات
- ظهور تطبيقات غير معروفة في الجهاز

سرقة الصور والملفات

عند تثبيت تطبيق خبيث أو فتح رابط مُزيَّف، قد يتم نَسْخ الصور والملفات الشخصية الموجودة في الجهاز إلى خادم خارجي.

الملفات التي يمكن سرقتها:

- الصور العائلية والخاصة
- مستندات الهوية أو التقارير الطبية
- الملاحظات وكلمات المرور المحفوظة
- ملفات العمل المُخزَّنة على الجهاز
- الفيديوهات والتسجيلات الصوتية

السؤال التفاعلي الخامس

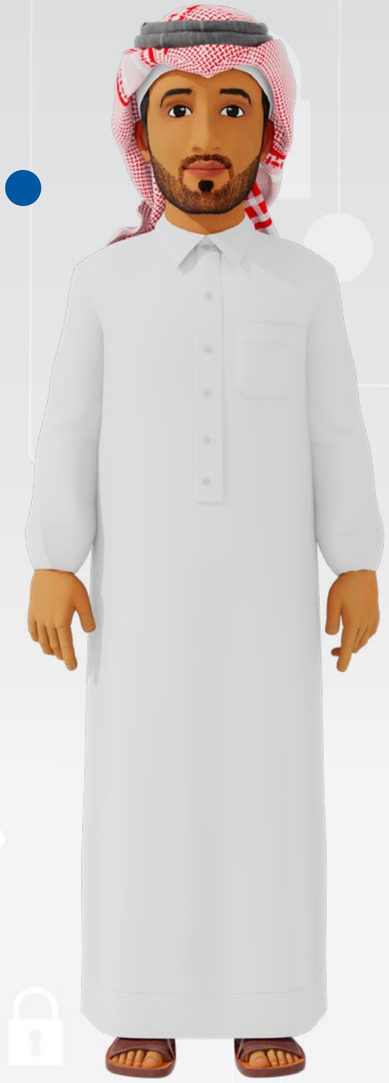
5- ما الطريقة التي تُستخدم لنقل برمجيات التجسس داخل الأجهزة المحمولة؟

أ. | تحديث الجهاز

ب. | تنزيل تطبيق من متجر رسمي

ج. | شحن الجهاز بالكهرباء

د. | تثبيت تطبيق من رابط خارجي مشبوه



السؤال التفاعلي السادس

6- كيف يمكن أن يُؤدّي الاتصال بشبكة Wi-Fi عامة إلى الاختراق؟

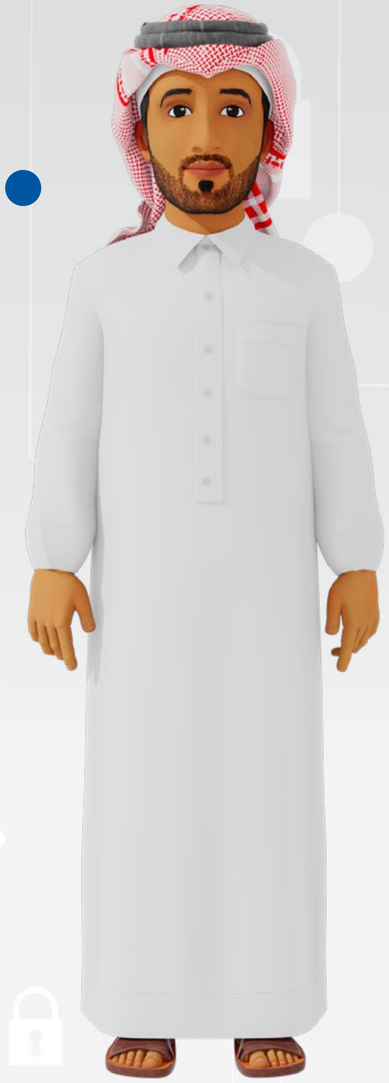
أ. | تمكين المخترق مِن مُراقبة ما يتم إدخاله

ب. | توفير استهلاك البيانات

ج. | تسريع التصفُّح

د. | زيادة جودة الصوت

السؤال التفاعلي السابع



7- ما الذي يدلّ على أنّ الكاميرا أو الميكروفون يعملان دون إذن؟

أ. | سطوع الشاشة

ب. | ظهور إعلانات في المتصفح

ج. | حرارة غير معتادة واستهلاك البطارية

د. | توقف الإنترنت مؤقتًا

السؤال التفاعلي الثامن

8- ما نوع الرسائل التي تظهر داخل المتصفّح وتُعد خَطِرة؟

أ. إشعار تحديث حقيقي من متجر التطبيقات

ب. إشعار بفوز بجائزة دون سابق مشاركة

ج. رسالة بريد إلكتروني من صديق

د. إشعار بتحديث الطقس

السؤال التفاعلي التاسع

9- ما الذي يجعل الإعلانات داخل بعض التطبيقات تُشكِّل خطرًا؟

أ. تعرض منتجات حقيقية

ب. تؤدي إلى روابط تحميل خبيثة

ج. توفّر محتوًى تعليميًّا

د. تكون بطيئة في التحميل

المحور الثاني

أمان الأجهزة المحمولة

ما المقصود بأمان الأجهزة المحمولة؟

الإجراءات التي تُحافظ على المعلومات داخل الأجهزة، وتمنع وصول أيّ شخص غير مُصرَّح له إليها.

عناصر الأمان الأساسية:

- حماية الجهاز بكلمة مرور طويلة ومُعقَّدة أو بَصْمة
- تأمين التطبيقات وحسابات البريد والبنك
- مَنْع تثبيت البرمجيات الضَّارَّة
- الحفاظ على خصوصية الصور والملفات
- تشفير الملفات والبيانات المهمة
- تفعيل المصادقة الثنائية (2FA) للحسابات المهمة
- تأمين الاتصال بالإنترنت والشبكات اللاسلكية

مثال: يمكن استخدام ميزة "Find My Device" لقفل الجهاز ومسح البيانات عند فقدانه.

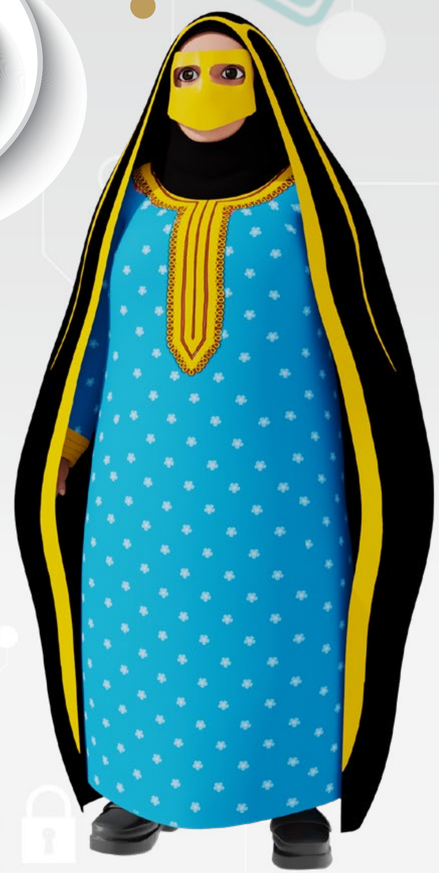
إعداد قفل شاشة آمِن

تأميـن شاشـة القفـل يُعـدّ أول حاجـز يحمـي الجهـاز مـن أيّ شـخص يحـاول فتحـه دون إذن.

أنواع قفل الشاشة المتاحة:

- رمز PIN رقمي مكوّن من 4 إلى 6 أرقام
- النمط (رسم مسار على الشبكة)
- بصمة الإصبع أو بصمة الوجه
- كلمة مرور مُعقَّدة (أرقام وحروف)
- إعدادات تَمنع ظهور الإشعارات على الشاشة المقفلة

التحديثات الدورية للنظام



تقوم الشركات المُصنِّعة بإصدار تحديثات أمنية تساعد على إصلاح الثغرات وسدّ الطرق التي يستغلها المحتالون.

فوائد التحديثات المنتظمة:

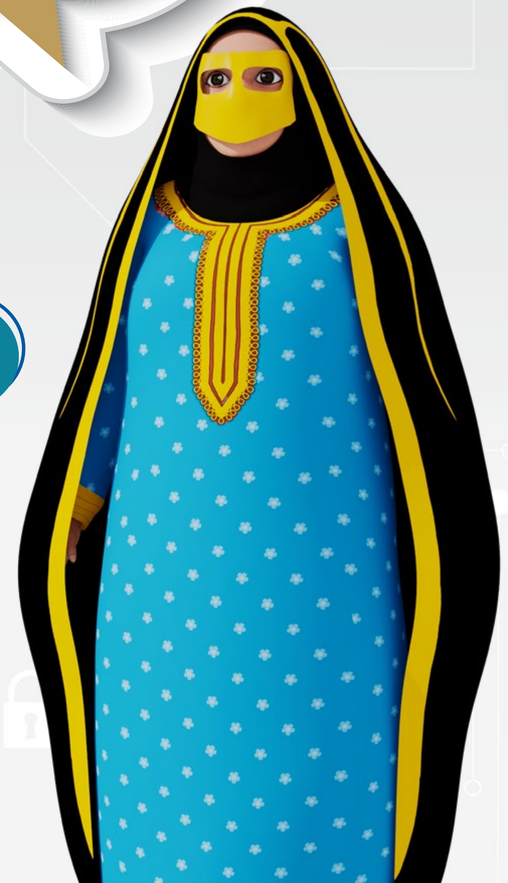
- تحسين حماية الجهاز من الفيروسات
- إصلاح المشكلات التقنية التي تُهدِّد الأمان
- تحديث إعدادات الخصوصية تلقائيًّا
- دعم التطبيقات بأحدث أدوات الحماية
- تقليل فرص استغلال الجهاز مِن قِبَل المهاجمين

النَّسخ الاحتياطي المنتظم

النسخ الاحتياطي يعني حفظ نسخة من البيانات المهمة في مكان آمِن لاستعادتها عند الحاجة.

أسباب تدعو لإجراء نسخ احتياطي:

- الحماية من فقدان البيانات في حال سرقة الجهاز
- استعادة الملفات عند تلف الجهاز أو تغييره
- توفير نسخة من جهات الاتصال
- إمكانية الوصول إلى الصور والوثائق من أيّ جهاز آخر
- تسهيل الانتقال إلى جهاز جديد دون فقدان المحتوى



استخدام برامج الحماية (مضادّ الفيروسات)

تُوفّر تطبيقات الحماية وسيلة إضافية لرَصْد التهديدات قبل أن تَصِل إلى الجهاز.

مهام برامج الحماية:

- فحص التطبيقات قبل تثبيتها
- تنبيه المستخدِم عند محاولة الوصول إلى البيانات
- حَظْر الروابط المشبوهة تلقائيًّا
- فَحْص الرسائل النصية والمرفقات
- تتبُّع موقع الجهاز في حال فقدانه

متجر التطبيقات الرسمي وغير الرسمي

يُفضَّل تحميل التطبيقات من المتاجر الرسمية؛ لأنها تخضع لرقابة أمنية، بخلاف المتاجر غير المعروفة التي قد تُوزّع تطبيقات خطرة.

- **الفَرْق بين المصدر الموثوق وغير الموثوق:**

المتاجر الرسمية Google Play - App Store

المتاجر غير الرسمية: مواقع خارجية، روابط مشبوهة

التطبيقات الرسمية تَمُرّ بفَحْص أمني قبل نَشْرها

التطبيقات من مصادر مجهولة قد تحتوي على برمجيات تجسس

التحميل من روابط مباشرة يرفع مستوى الخطر

تحميل التطبيقات بأمان

اختيار مصدر موثوق للتطبيقات هو أحد الأُسُس الأساسية لحماية الجهاز من التطبيقات المزوّرة أو الضارة.

الممارسات الآمنة لتحميل التطبيقات:

- تحميل التطبيقات فقط من متجر Google Play أو App Store.
- قراءة تقييمات المستخدمين قبل التثبيت
- مراجعة الصلاحيات المطلوبة أثناء التثبيت
- عدم الوثوق بروابط تحميل تصل عبر الرسائل
- تجنّب تثبيت التطبيقات التي تطلب معلومات بنكية

إعدادات الخصوصية في التطبيقات

بعض التطبيقات تطلب صلاحيات غير ضرورية قد تُستخدَم لاحقًا لأغراض ضارّة

الإعدادات التي يمكن التحكم بها:

- إيقاف وصول التطبيق إلى الكاميرا أو الميكروفون
- مَنْع مشاركة الموقع الجغرافي إلا عند الحاجة
- حَظْر صلاحية الوصول إلى الصور أو جهات الاتصال
- مراجعة الأذونات الممنوحة كلّ فترة
- حَذْف التطبيقات التي تتطلب صلاحيات مفرطة

مراقبة التطبيقات التي تطلب صلاحيات مُفْرِطة

بعض التطبيقات تطلب صلاحيات غير منطقية بالنسبة لطبيعة عملها، ما قد يكون مؤشرًا على أنها غير آمِنَة.

- أمثلة على الصلاحيات التي يجب الانتباه لها:

تطبيق آلة حاسبة يطلب الوصول للكاميرا

تطبيق طقس يطلب الوصول إلى جهات الاتصال

تطبيق ألعاب يطلب التحكُّم في المكالمات

تطبيق خلفيات يطلب تتبُّع الموقع

أيّ تطبيق يطلب صلاحيات إدارية عند التثبيت

التعامل مع الرسائل المشبوهة

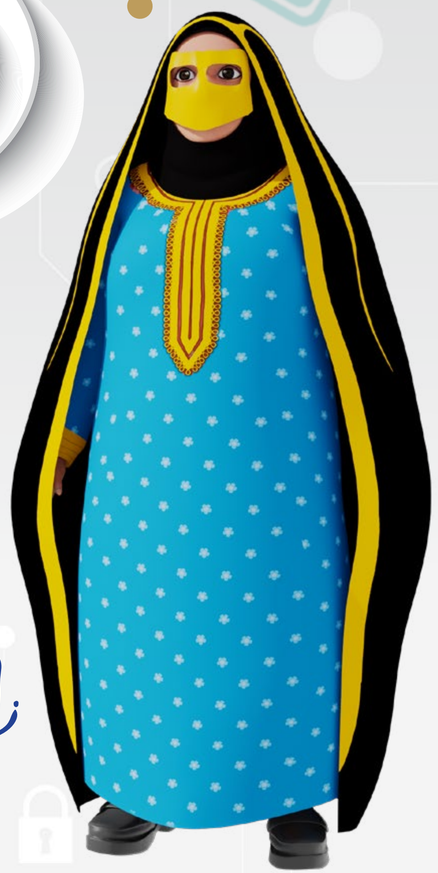
الرسائل الاحتيالية تهدف غالبًا إلى دَفْع المستخدِم للضغط على روابط أو تقديم معلومات خاصة.

طرق التعامل الآمِن:

- عدم الضغط على أيّ رابط غير معروف
- حذف الرسائل التي تحتوي على عروض غير منطقية
- تجاهل الرسائل التي تطلب بيانات شخصية
- الإبلاغ عن الأرقام المشبوهة في تطبيق الرسائل
- عدم الرد حتى ولو بدافع الفضول أو التجريب

ماذا تفعل عند فقدان الجهاز أو الاشتباه باختراقه؟

في حال فقدت جهازك أو شككتَ في أنه مُختَرق، فإنّ اتخاذ خطوات سريعة يساعد في تقليل الأضرار.



الإجراءات المقترحة في هذه الحالة:

- الاتصال بشركة الاتصالات لإيقاف الشريحة
- تسجيل الدخول إلى حساب الجهاز من جهاز آخر لتحديد موقعه أو مسح البيانات
- تغيير كلمات المرور لكل الحسابات المرتبطة بالجهاز
- إبلاغ أحد أفراد الأسرة أو شخص موثوق
- تقديم بلاغ للجهة المختصة إذا كان الجهاز يحتوي على بيانات حساسة

السؤال التفاعلي العاشر

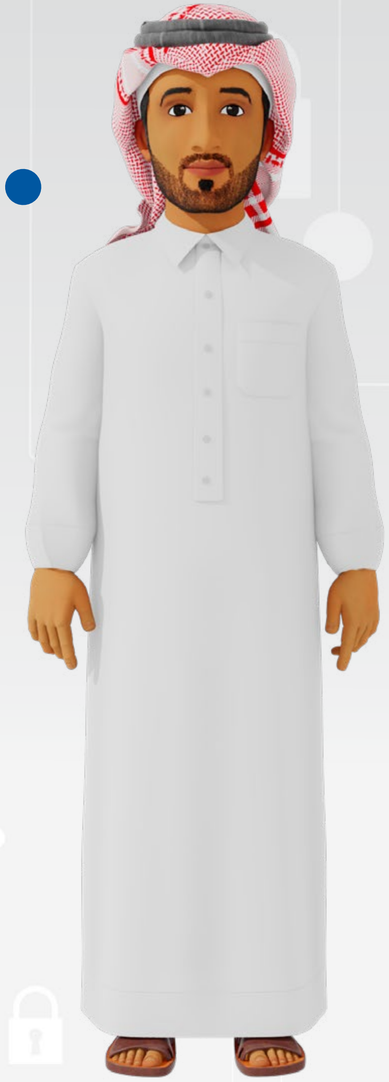
10- ما فائدة قفل الشاشة بكلمة مرور أو بصمة؟

أ. | يجعل الجهاز أبطأ

ب. | يمنع الآخرين من فتح الجهاز بدون إذن

ج. | يُصعّب استخدام الجهاز

د. | يستهلك البطارية بسرعة



السؤال التفاعلي الحادي عشر

11- كيف يساعد التحديث المنتظم للتطبيقات في حماية الجهاز؟

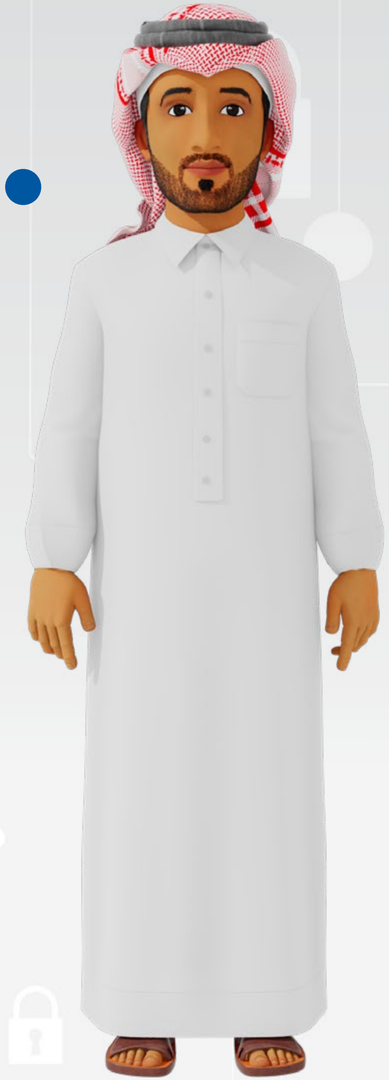
أ. | يُغيّر شكل الرموز

ب. | يزيد مساحة التخزين

ج. | يُعالج الثغرات الأمنية ويُحسّن الحماية

د. | يطيل عمر البطارية

السؤال التفاعلي الثاني عشر



12- ما هو الاستخدام السليم لشبكات Wi-Fi العامة؟

أ. | الدخول لحساب البنك

ب. | تصفح الأخبار فقط دون تسجيل الدخول

ج. | إرسال الملفات الخاصة

د. | تثبيت تطبيقات من الإنترنت

السؤال التفاعلي الثالث عشر

13- عند تثبيت تطبيق جديد، ما الخطوة التي يُنصح بها؟

أ. مراجعة الأذونات المطلوبة بدقة

ب. الموافقة على كلّ الصلاحيات دون قراءة

ج. الضغط على "موافق" فورًا

د. تثبيت التطبيق من أيّ رابط متوفر

السؤال التفاعلي الرابع عشر

14- ما أول تصرُّف عند فقدان الجهاز المحمول؟

أ. شراء جهاز جديد

ب. تجاهل الموضوع .

ج. إبلاغ العائلة وإيقاف الشريحة

د. حذف التطبيقات فقط

إجابات الأسئلة التفاعلية

01 **إجابة السؤال التفاعلي الأول**

ج) كل البيانات المخزنة مثل الصور، الحسابات، المحادثات

02 **إجابة السؤال التفاعلي الثاني**

ج) يخضع للمراقبة الأمنية والفحص

03 **إجابة السؤال التفاعلي الثالث**

د) وضع قفل شاشة وكلمة مرور

04 **إجابة السؤال التفاعلي الرابع**

أ) تحسين الحماية وسد الثغرات الأمنية

05 **إجابة السؤال التفاعلي الخامس**

د) تثبيت تطبيق من رابط خارجي مشبوه

إجابات الأسئلة التفاعلية

06 **إجابة السؤال التفاعلي السادس**

أ) تمكين المخترق من مراقبة ما يتم إدخاله

07 **إجابة السؤال التفاعلي السابع**

ج) حرارة غير معتادة واستهلاك البطارية

08 **إجابة السؤال التفاعلي الثامن**

ب) إشعار بفوز بجائزة دون سابق مشاركة

09 **إجابة السؤال التفاعلي التاسع**

ب) تؤدي إلى روابط تحميل خبيثة

10 **إجابة السؤال التفاعلي العاشر**

ب) يمنع الآخرين من فتح الجهاز بدون إذن

إجابات الأسئلة التفاعلية

11	**إجابة السؤال التفاعلي الحادي عشر** ج) يعالج الثغرات الأمنية ويحسّن الحماية
12	**إجابة السؤال التفاعلي الثاني عشر** ب) تصفح الأخبار فقط دون تسجيل الدخول
13	**إجابة السؤال التفاعلي الثالث عشر** أ.) مراجعة الأذونات المطلوبة بدقة
14	**إجابة السؤال التفاعلي الرابع عشر** ج) إبلاغ العائلة وإيقاف الشريحة

المراجع

1. A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks, on site: https://arxiv.org/abs/2001.09406
2. Best Practices for Device Hygiene, McAfee, on site: https://www.mcafee.com/learn/best-practices-for-device-hygiene/
3. How to Protect Your Phone from Hacking, Numero, on site: https://www.numeroesim.com/blog/ar/%D9%83%D9%8A%D9%81-%D8%AA%D8%AD%D9%85%D9%8A-%D9%87%D8%A7%D8%AA%D9%81%D9%83-%D9%85%D9%86-%D8%A7%D9%84%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82/
4. Mobile Security: Threats and Best Practices, on site: https://scispace.com/pdf/mobile-security-threats-and-best-practices-3nb3lc4htx.pdf
5. Phone Security Best Practices to Protect Your Mobile Data, Okta, on site: https://www.okta.com/en-au/identity-101/phone-security/
6. Protect Mobile Devices (Smartphone, iPad, or Other Tablet), Cornell University, on site: https://it.cornell.edu/device-security/protect-mobile-devices-smartphone-ipad-or-other-tablet
7. Top Mobile Security Threats and Prevention Tips (2022), ASEE Cybersecurity Blog, on site: https://cybersecurity.asee.io/blog/top-mobile-security-threats-prevention-tips/

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

16555 - 6379 - 51045944

www.ncsa.gov.qa academy@ncsa.gov.qa