الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

أمان منصات التواصل الاجتماعي

الشريحة المُستهدَفة
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 منصات التواصل الاجتماعي

الشريحة المُستهدَفة

كبـــار القَـــــدْر

كُتَيّب المُدَرّب

تمهيـــــد

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 عبر منصات التواصل الاجتماعي؛ حيث يهدف هذا الكتيّب إلى تعزيز وعيهم بأبرز هذه التهديدات؛ وكيف يمكن الوقاية منها، ممَّا يجعل السلامة الرقمية أولويةً حيويةً لهم.

وتُعدّ هذه الجهود جزءًا 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 نَشْر 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:

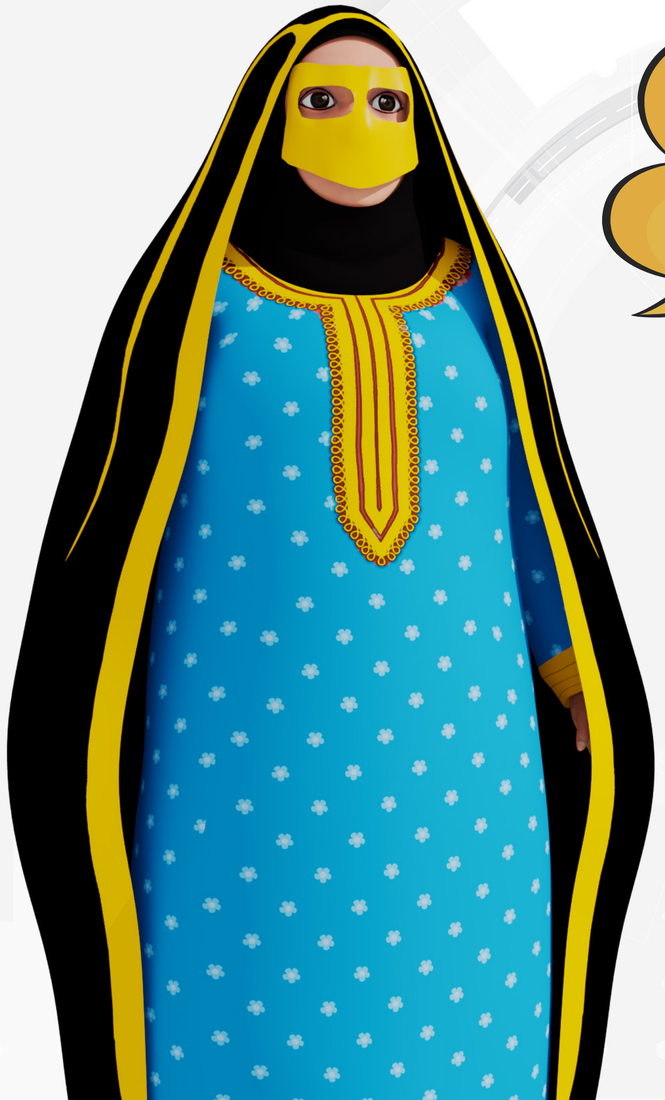
- كبار القَدْر
- المرأة والأسرة
- ذوو الاحتياجات الخاصة
- طلبة الجامعات
- العمالة الوافدة
- مؤسسات المجتمع المدني
- القطاع المالي والمصرفي

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

منصّات التواصل الاجتماعي



ما هي منصات التواصل الاجتماعي؟

مواقع أو تطبيقات تسمح بالتواصل مع الآخرين، سواء عن طريق الكتابة أو الصور أو الفيديو، وتُستخدَم مِن قِبَل ملايين الناس حول العالَم.

- فيسبوك (Facebook) للمحادثات ومشاركة الصور والمنشورات
- واتساب (WhatsApp) للرسائل الفورية والمكالمات
- تيليجرام (Telegram) للدردشات والمجموعات الخاصة والعامة
- إنستغرام (Instagram) للمشاركة الصور ومقاطع الفيديو القصيرة
- منصة X (تويتر سابقًا) لمتابعة الأخبار والتعليقات القصيرة

الفــروق الأساســية

لـكل منصـة أسـلوبها الخـاص فـي العـرض والتواصـل، وبعضها أكثر تركيزًا على العائلة، بينما يُستخدَم البعض الآخر لنَشْر الأخبار أو أحدث توجُّهات المجتمع العام.

واتساب (WhatsApp):
رسائل خاصة ومجموعات مُغلَقة

فيسبوك (Facebook):
منشورات ومتابعة الأصدقاء وصفحات عامة

إنستغرام (Instagram):
صور ومقاطع قصيرة (Reels)

تيليجرام (Telegram):
مجموعات عامة وقنوات بمحتوى واسع

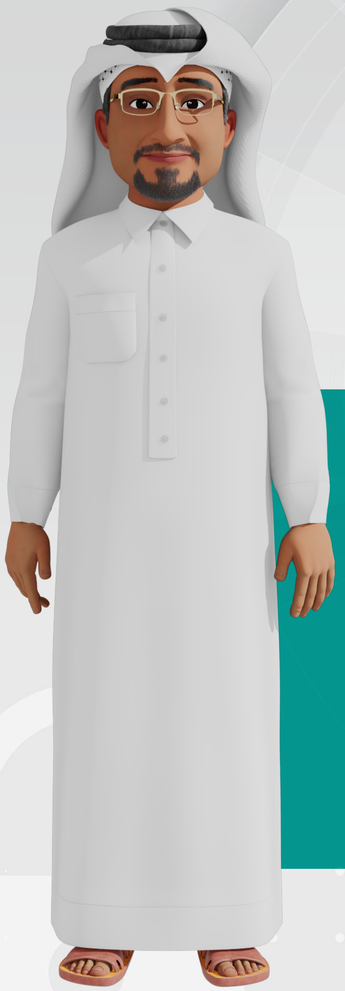
(X):
محتوى سريع ومختصر وتحديثات لحظية

خصوصية البيانات الشخصية

بمجرد إنشاء حساب، قد يتم عَرْض بعض المعلومات تلقائيًّا، ما لم يتم تعديل إعدادات الخصوصية.

البيانات التي يمكن أن تكون ظاهرة للآخرين:

- الاسم الكامل وصورة الحساب
- رقم الهاتف المرتبط بالحساب (في بعض المنصات)
- قائمة الأصدقاء أو المتابعين
- الصور التي يتم نَشْرها بشكل علني
- التعليقات التي يتم تركها على صفحات عامة



التفاعلات اليومـــية

ما يبدو كتفاعل بسيط (إعجاب - تعليق - مشاركة)،
قد يُستخدم لاحقًا مِن قِبَل المخترقين أو المحتالين.

أمثلة على تفاعلات قد تَحمل خطرًا:

- الضغط على روابط مجهولة داخـــل المنشورات
- المشاركة فـــي مسابقات وهمية تتطلَّب بيانـــات
- التعليق علـــى منشورات مُزيَّفة تحاول استـدراج المستخدميـــن
- إرسال الرموز أو الصـــور للغرباء فـــي الرسائـــل
- الانضمـــام لمجموعات غير واضحة المصـــدر

كيف يُستخدَم الملف الشخصي في الاحتيال؟

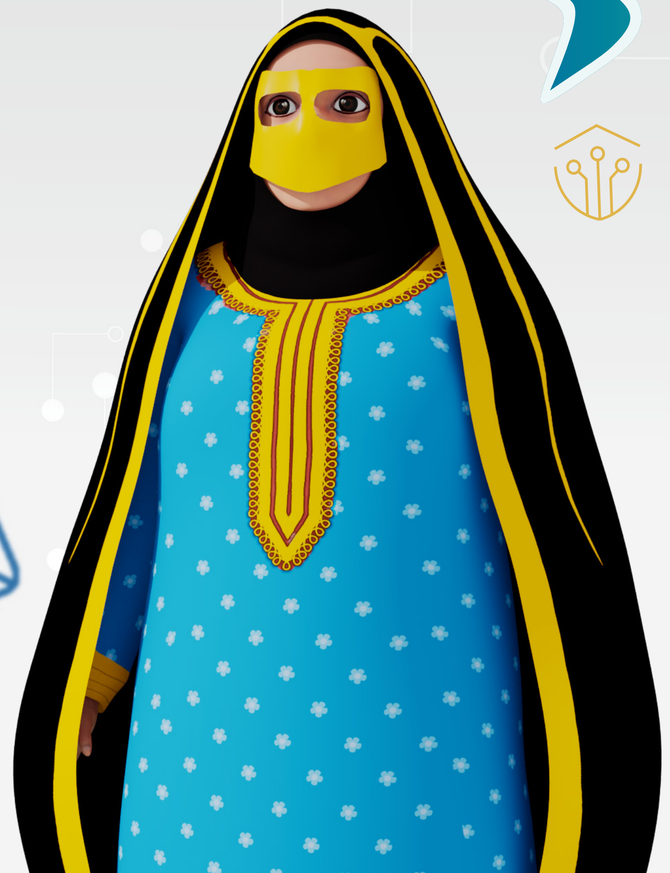
قد يقوم أحدهم بجَمْع معلومات من ملفك الشخصي، ثم استخدامها لانتحال هويتك أو خداع أقربائك.

طرق استغلال الملف الشخصي:

- استخدام صورتك واسمك لإنشاء حساب مزيف
- ربطك بحسابات مُزيَّفة لجمع بياناتك
- تتبُّع نشاطك اليومي واستخدامه في الابتزاز
- إرسال رسائل للآخرين باسمك لطلب المال
- استغلال المنشورات القديمة لفبركة محادثات

خصوصية الصور والموقع الجغرافي

الصور التي تُنشَر على المنصات قد تحمل معلومات خفية عن المكان أو الأشخاص الموجودين فيها.

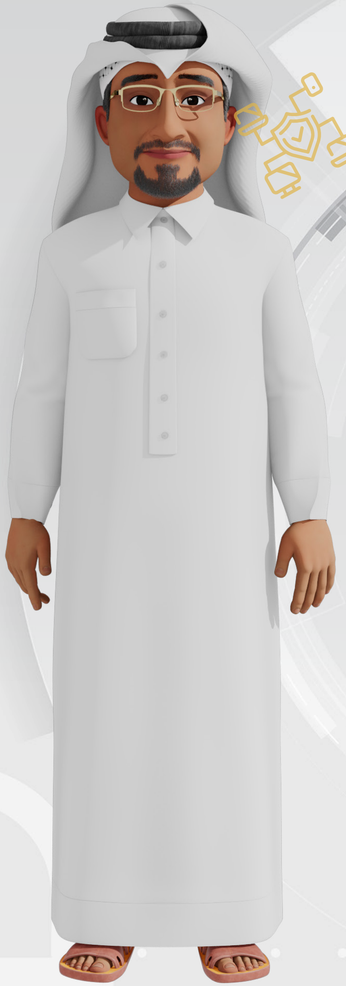


مخاطر مرتبطة بالصور والموقع:

- الكشف عن عنوان المنزل أو مكان الوجود
- تتبُّع التحركات اليومية من خلال المنشورات
- ظهور أطفال العائلة أو كبار القَدْر في صور علنية
- إمكانية نَسْخ الصورة واستخدامها في حسابات مزيفة
- تحميل الصور وتعديلها دون عِلْم صاحبها

التوازن بين التواصل والمتابعة الآمِنَة

من المهم أن يَستفيد كبار القَدْر من هذه المنصات، مع الحفاظ على مستوى جيّد من الحذر.



مبادئ التوازن بين الإفـادة والحـذر

- متابعة الحسابات والمجموعـــات المفيدة فقـــط
- مشاركة الصور والمنشـــورات مع الأصـــدقاء الموثوقين
- تجنُّب إضافة أيّ شخص لا تعرفه
- مراجعة إعدادات الخصوصية كـــلّ فترة
- التوقف عن استخدام الحساب عند الشك بأيّ نشاط غريـــب

السؤال التفاعلي الأول

1 - ما المعلومات التي قد تكون ظاهرة لأيّ شخص يزور حسابك؟

أ. صورة الحساب والمنشورات العامة

ب. رقم البطاقة الشخصية

ج. عنوان المنزل

د. الرمز السري للحساب

السؤال التفاعلي الثاني

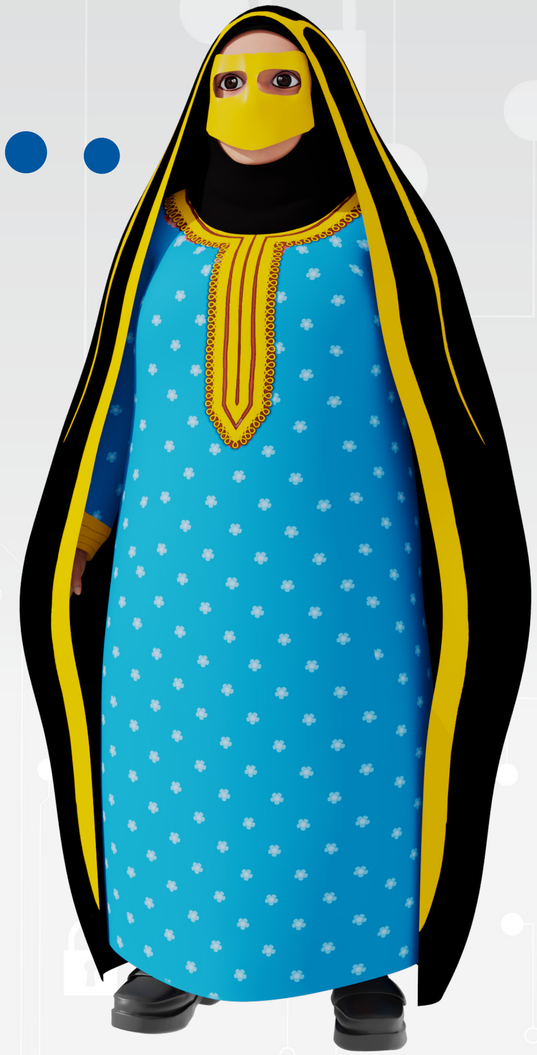
2 - لماذا قد يُستخدم حسابك في عمليات احتيال؟

أ. لأنك نشيط جدًّا

ب. لأنك لا تَرُدّ على الرسائل

ج. لأنك تكتب باللغة العربية

د. لأنك تُشارك معلومات كثيرة علنًا



السؤال التفاعلي الثالث

3 - ما هي الخطوة الأولى لحماية منشوراتك من الغرباء؟

تعديل إعدادات الخصوصية

أ. حذف الحساب

ب. تغيير اسمك

ج. تعديل إعدادات الخصوصية

د. تعطيل الهاتف

السؤال التفاعلي الرابع

4 - ما السبب الذي يجعل مشاركة الصور من الهاتف أمرًا يحتاج إلى تفكير؟

أ. لأن الصور تُضْعِف الشبكة

ب. لأن الصور قد تُظْهِر موقعك أو أشخاصًا آخرين

ج. لأن الصور تَشْغل مساحة في الهاتف

د. لأن الصور تُسبِّب تعليق الحساب

التهديدات الرقمية على منصات التواصل الاجتماعي

انتحال الشخصيات داخل المنصات

يقوم البعض بإنشاء حسابات مُزيَّفة تحمل أسماء وصور أشخاص حقيقيين، ويستخدمونها لخداع الآخرين.

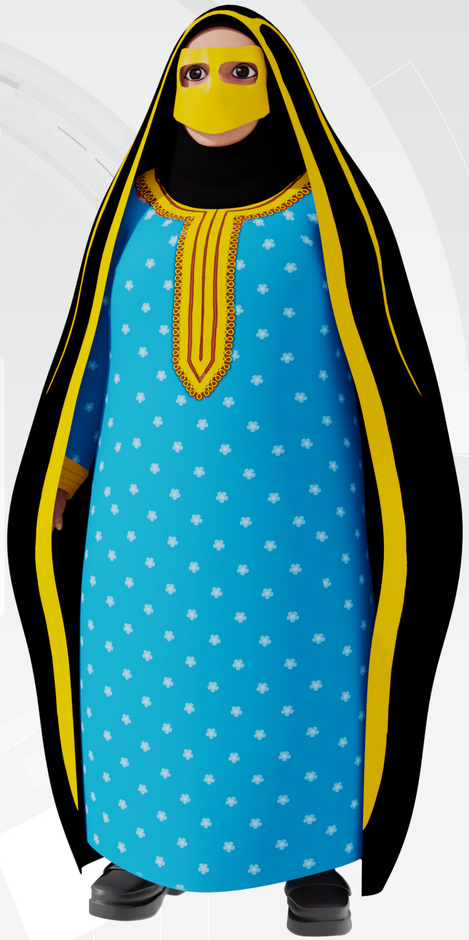
أهداف هذا النوع من الانتحال:

- إرسال رسائل لأصدقاء الضحية لطلب المال أو معلومات
- نشر محتوى مسيء باسم الضحية لتشويه سُمعته
- زرع روابط خبيثة داخل المنشورات والرسائل
- استخدام الحساب للتواصل مع الغرباء وانتحال هوية
- جمع تبرعات مُزيَّفة باسم صاحب الحساب

الروابط الاحتيالية

يتم إرسال روابط تبدو طبيعية، لكنَّها تؤدي إلى مواقع مُزيَّفة تهدف إلى سرقة الحساب أو تحميل برامج خبيثة.

خصائص الروابط الاحتيالية:



- روابط قصيرة أو غير واضحة المصدر
- تأتي داخل رسالة من صديق تم اختراق حسابه
- تؤدي إلى صفحات تطلب بيانات الدخول أو رقم الهاتف
- ترافقها عبارات تحفيزية مثل "شاهِد هذا الفيديو"، أو "مبروك الجائزة"
- تبدأ بتحميل تطبيق دون إذن

الرسائل الاحتيالية

تقوم بعض محاولات الاحتيال على انتحال صفة قريب أو صديق عبر حساب جديد، مع سَرْد قصة طارئة بهدف الحصول على مبلغ مالي سريع.

تظهر هـذه المحاولات مــن خــلال عـلامـات واضحـة، أبـرزها:

ظهور الرسالة مِن رقم أو حساب جديد يُقدِّم نفسه كأحد أفراد العائلة

تضمُّنها نَبْرَة إلحاح ورَبْط الطلب بظرف طارئ

الإصرار على عدم إبلاغ أيّ شخص آخر

استخدام لغة وُدِّية أو عاطفية لتعزيز الثقة

طلب تحويل مالي عبر وسائل سريعة مثل الحوالات أو الخدمات الفورية، يليه اختفاء الحساب مباشرة بعد العملية

التحديات والمسابقات المزيفة

تنتشر منشورات تُعلن عن جوائز أو مسابقات بسيطة، وتطلب من المشاركين إدخال بياناتهم أو مشاركة المنشور.

أشكال هذه المسابقات

- "اربح هاتفًا جديدًا، اكتب تم وشارك الرابط"
- "جاوب على هذا السؤال وسنختارك للفوز"
- "تم اختيارك عشوائيًّا للحصول على بطاقة هدية"
- روابط إلى صفحات مزيّفة تشبه المتاجر الكبرى
- جمع بيانات مثل الاسم، الرقم أو العنوان بهدف الاحتيال لاحقًا

اختـــــراق الحســـابات

بعد اختراق الحساب، يبدأ المحتال باستخدامه لنشر محتوى مزيّف، أو مراسلة الآخرين وطلب معلومات.

مؤشرات اختراق الحساب

- تغيّر الصورة أو الاسم فجأة
- إرسال رسائل إلـــى الأصدقاء دون عِلْمك
- ظهور منشورات لم تكتبها
- الخروج المتكرر من الحساب دون سبب
- وصول رسائل تحذيرية من المنصة حول نشاط مريب

المجموعات المُزيَّفة

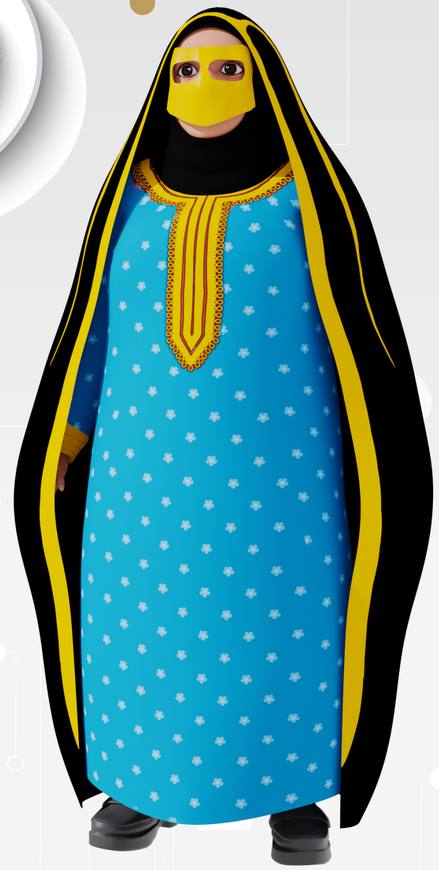
يتم إنشاء مجموعات في واتساب WhatsApp أو تيليجرام Tele-gram أو فيسبوك Facebook تُظْهِر اهتمامًا بموضوع معيّن، لكنّ الغرض منها هو جمع معلومات الأعضاء.

خصائص هذه المجموعات

- عدم وضوح هوية المشرف أو المُؤسِّس
- طرح أسئلة شخصية على شكل استطلاعات
- إرسال روابط لمواقع خارجية مشبوهة
- طلب مشاركة بيانات مثل رقم الهوية أو العنوان
- محاولة جَذْب الأعضاء بعناوين جذابة مثل: "مساعدات"، "خصومات"، "فرص عمل"

طلـبات الصـداقة

استـقبال طلبـات صداقـة مـن
أشخاص مجهولين قـد يَفتح بابًا
لمحـاولات احتيـال أو مراقبـة



علامات تدل على أن الحساب غير حقيقي:

الاسم غريب أو مُكرَّر

صورة الحساب مأخوذة من الإنترنت أو غير واضحة

وجود عدد كبير من الأصدقاء دون تفاعل

الحساب جديد، ولا يحتوي على منشورات حقيقية

عدم وجود أيّ اهتمام مشترك أو سبب منطقيّ للإضافة

الاستطلاعات والاختبارات الترفيهية

تنتشر بعض "الاختبارات الترفيهية"، أو "تحليل الشخصية" على فيسبوك Facebook أو غيره، لكنّها في الواقع تجمع بيانات المستخدِم

أشكال هذه الاختبارات

- "ما هو عمرك الحقيقي؟ جاوب الآن"
- "مَن يشبهك مِن المشاهير؟"
- "ما هو بُرجك؟ أدخل اسمك وتاريخ ميلادك"
- تطلب منك مَنْح التطبيق صلاحية الوصول للحساب
- تُستخدم لاحقًا لسحب البيانات أو استهدافك بإعلانات ورسائل خبيثة

استغلال الصور والمعلومات

أي محتوى تنشره يمكن أن يُؤخَذ مِن قِبَل الآخرين، ويُستخدم بطرق لم تقصدها، مثل النشر غير المصرَّح به أو الفبركة

طرق استغلال الصور والمحتوى

- إنشاء حسابات مُزيَّفة بنفس الاسم والصورة
- تعديل الصورة وإعادة نَشْرها
- استخدام الصورة في منشورات خادعة أو إعلانات وهمية
- دَمْج الصور مع محتوى مُسيء
- جَمْع الصور لاستخدامها لاحقًا في الابتزاز أو التشهير

السؤال التفاعلي الخامس

5 - كيف يمكن لشخص انتحال هويتك على منصات التواصل؟

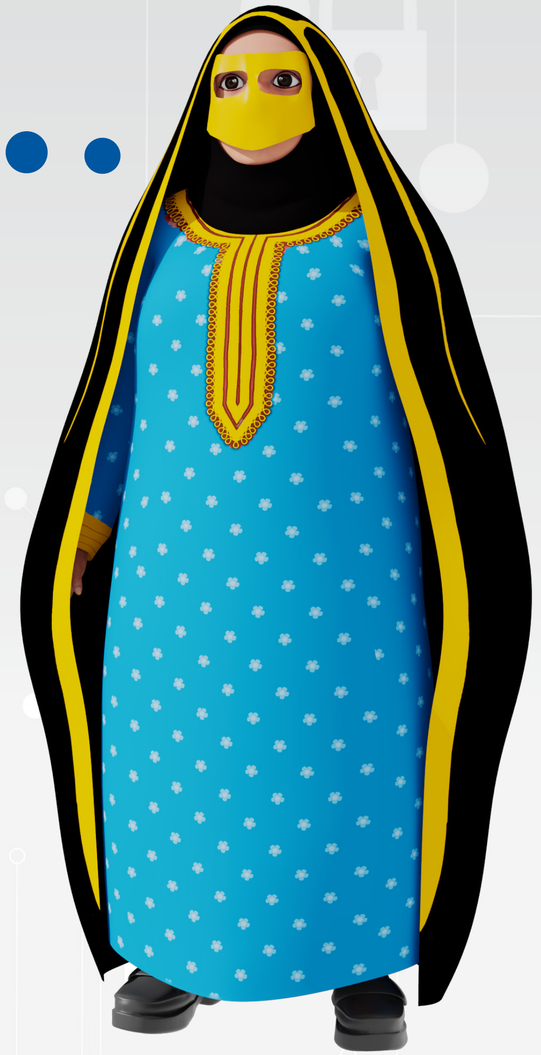
أ. من خلال إرسال فيديوهات تعليمية

ب. بإنشاء حساب باسمك وصورتك

ج. من خلال طلب صداقتك فقط

د. عبر الاتصال الهاتفي

السؤال التفاعلي السادس



6 - ما أبرز علامة على أن الحساب قد تعرَّض للاختراق؟

أ. إذا تم تغيير اللغة فقط

ب. إذا توقفت الإشعارات

ج. إذا أُرسلت منشورات لم تكتبها

د. إذا اختفى شريط القوائم

السؤال التفاعلي السابع

7 - لماذا يُنصَح بعدم المشاركة في "تحليل الشخصية" أو الاختبارات الترفيهية؟

أ. لأنها طويلة ومُمِلَّة

ب. لأنها تُبطِّئ الجهاز

ج. لأنها تُستخدَم لجمع معلوماتك

د. لأنها تُقلِّل عدد الأصدقاء

السؤال التفاعلي الثامن

8 - ما الطريقة الأكثر أمانًا للتعامل مع طلبات صداقة غير معروفة؟

أ. قبولها فورًا

ب. مشاركتها مع الأصدقاء

ج. إرسال تحية أولًا

د. تجاهلها أو حذفها

خطوات حماية الحسابات

كلمة المرور

كلمة المرور هي خط الدفاع الأول، واستخدام كلمات ضعيفة أو مكررة يجعل الحساب عرضة للاختراق بسهولة.

خصائص كلمة المرور الآمنة:

- تحتوي على حروف كبيرة وصغيرة وأرقام ورموز
- لا ترتبط بالاسم أو تاريخ الميلاد
- لا تُستخدم نفسها في أكثر من حساب
- مواقع جغرافية (أنا هنا - وصلت الآن)
- يتم تغييرها دوريًّا كل عدة أشهر

المصادقة الثنائية

التحقُّق بخطوتين يعني أنه حتى لو عرف أحدهم كلمة المرور، فلن يتمكّن من الدخول إلا باستخدام رمز يُرسَل إلى هاتفك أو بريدك.

فوائد التحقق بخطوتين:

- حماية إضافية عند محاولة الدخول إلى الحساب
- تنبيه فوري إذا حاول أحدهم فَتْح حسابك
- يُقلّل فرص الاختراق بنسبة كبيرة
- يمكن تفعيله في معظم التطبيقات(فيسبوك - واتساب - إنستغرام)
- يساعد على استرجاع الحساب بسهولة في حال نسيان كلمة المرور

إعدادات الخصوصية

تُتيح معظم المنصات إمكانية التحكُّم في مَن يرى منشوراتك، ومَن يمكنه التواصل معك.

خيارات الخصوصية الآمنة

- جعل المنشورات مرئية "للأصدقاء فقط"
- تحديد مَن يمكنه الإشارة إليك في الصور والمنشورات
- إخفاء رقم الهاتف أو البريد الإلكتروني عن الجميع
- تعطيل مشاركة المنشورات مِن قِبَل الغرباء
- مَنْع الآخرين من إرسال طلبات الصداقة

تجـنُّب الروابـــط المختصـرة

تُستخدم الروابط أحيانًا كفخّ للدخول إلى صفحات احتيالية، حتى لو أُرسلت من صديق

كيفية التعرف على الروابط المشبوهة:

- لا تحتوي اسم موقع معروف
- تُرسَل داخل رسائل مفاجئة أو غير متوقّعة
- تبدأ بإعلانات مغرية مثـل "اربح الآن"
- تنقلك إلى صفحة تطلب معلوماتك فورًا
- تظهر من حساب تم اختراقه مسبقًا

التحقق من هوية المرسل

حتى إن بدا الشخص مألوفًا، من الضروري التأكُّد من هويته قبل إرسال أيّ معلومات أو الرد على طلباته

أساليب التحقق

- طَرْح سؤال لا يَعرفه إلا الشخص الحقيقي
- طلب مكالمة صوتية قصيرة للتأكُّد
- مراجعة المحادثات السابقة إن وُجِدَتْ
- الانتباه لنوعية اللغة والأسلوب المستخدم
- التواصل مع الشخص من رقم أو حساب آخر معروف مسبقًا

التعامل مع الحسابات المخترقة

في حال شعرت أن حسابك أو حساب صديقك قد تم اختراقه، فإنّ سرعة التصرّف مهمة لمنع الضرر

خطوات التعامل مع الاخـــتراق

- تفعيل التحقق بخطوتين
- تغيير كلمة المرور فورًا
- إبلاغ المنصة (فيسبوك، واتساب...) عن الحساب
- تسجيل الخروج من جميع الأجهزة
- تنبيه الأصدقاء بعدم التفاعل مع الحساب حتى يتم تأمينه

سرية الرسائل والمحـــادثات

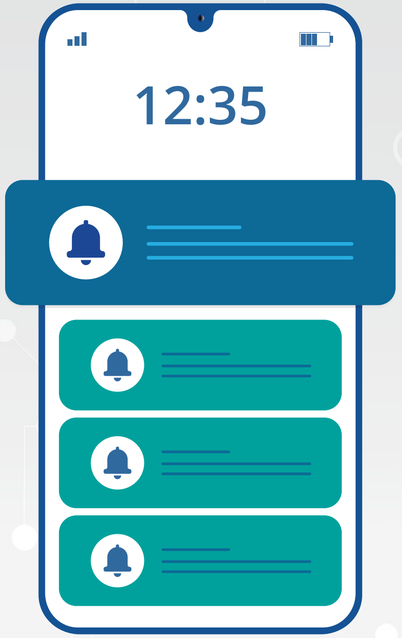
المـراسلات الخاصـة يجـب أن تبقـى بينـك وبيـن الشـخص المعنـيّ فقـط، وعـدم مشـاركة أيّ معلومـة شـخصية مـع غيـر الموثوقيـن

نصائح لتأمين المحادثات

- تجنّب إرسال صور أو معلومات شخصية في المحادثات غير المُؤمَّنة
- حذف الرسائل المشبوهة أو غير المريحة
- تجنّب نقل أكواد أو أرقام تحقّق لأيّ شخص
- استخدام المحادثات المشفّرة إذا كانت المنصة تُوفّر ذلك
- عدم الرد على الرسائل التي تبدأ بطلب أو تهديد

مراجعة النشاطات والإشعارات

من الجيد الدخول إلى إعدادات الحساب ومتابعة النشاطات الجديدة، لرَصْد أيّ سلوك غير معتاد.



مؤشرات تُظهر وجود خطر محتمل:

- محاولات تسجيل دخول من أماكن غير مألوفة
- تفعيل إعدادات لم تَقُم بها بنفسك
- رسائل تأكيد أو تغييرات لم تطلبها
- إغلاق مفاجئ للحساب أو طلب رمز جديد
- رسائل من الأصدقاء حول منشورات أو رسائل لم تُرسلها

السؤال التفاعلي التاسع

9 - ما الذي يجعل كلمة المرور قوية وآمِنَة؟

أ. أن تحتوي على حروف وأرقام ورموز

ب. أن تكون سهلة الحفظ مثل: 123456

ج. أن تكون نفس كلمة المرور في كلّ الحسابات

د. أن ترتبط بتاريخ الميلاد

السؤال التفاعلي العاشر

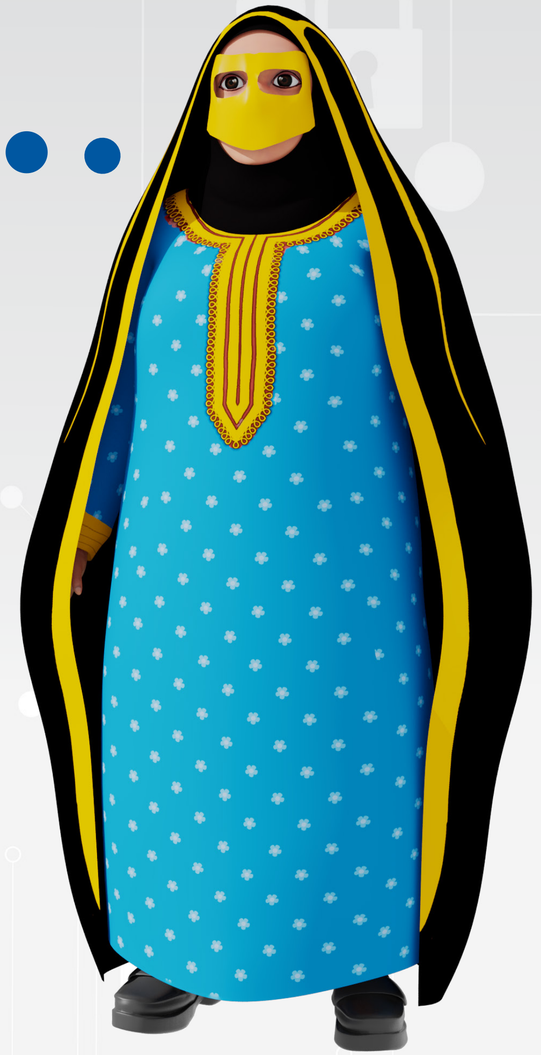
10 - ما فائدة التحقق بخطوتين؟

أ. تسريع الدخول إلى الحساب

ب. إيقاف الإعلانات

ج. حذف الحساب تلقائيًّا عند الخطأ

د. منع الآخرين من فتح الحساب حتى مع معرفة كلمة المرور



السؤال التفاعلي الحادي عشر

11 - ما هو أفضل تصرُّف عند استلام رسالة من شخص يطلب معلومات خاصة؟

أ. إرسال ما يطلبه مباشرة

ب. الرد عليه وتحذيره

ج. التحقُّق من هويته أولًا

د. وَضْعه في مجموعة عائلية

السؤال التفاعلي الثاني عشر

12 - ماذا تفعل إذا اكتشفت أن أحد الأصدقاء تعرّض للاختراق؟

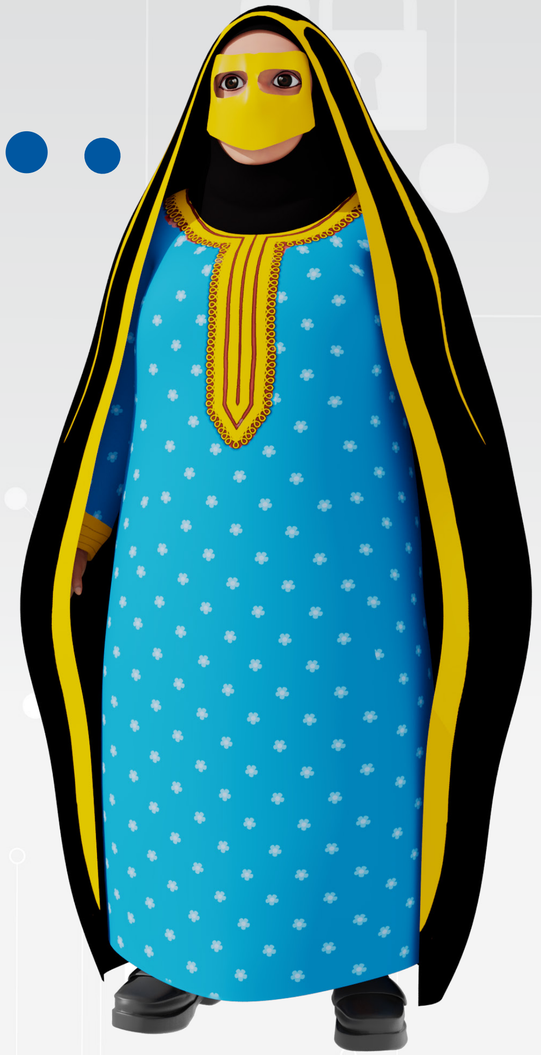
أ. حذف التطبيق

ب. إبلاغ المنصة وتنبيه الآخرين

ج. إرسال رسالة تهنئة له

د. إعادة مشاركة منشوراته

السؤال التفاعلي الثالث عشر



13 - كيف تُراجع نشاطات حسابك للتأكُّد من عدم وجود اختراق؟

أ. تدخل إلى الإعدادات وتتابع أماكن تسجيل الدخول

ب. تنتظر أن يُخبرك أحد

ج. تفتح الحساب في وقت متأخر فقط

د. تطلب من الغرباء التحقُّق

إجابات الأسئلة التفاعلية

01	**إجابة السؤال التفاعلي الأول** أ) صورة الحساب والمنشورات العامة
02	**إجابة السؤال التفاعلي الثاني** د) لأنك تشارك معلومات كثيرة علنًا
03	**إجابة السؤال التفاعلي الثالث** ج) تعديل إعدادات الخصوصية
04	**إجابة السؤال التفاعلي الرابع** ب) لأن الصور قد تُظهر موقعك أو أشخاصًا آخرين
05	**إجابة السؤال التفاعلي الخامس** ب. بإنشاء حساب باسمك وصورتك
06	**إجابة السؤال التفاعلي السادس** ج) إذا أُرسلت منشورات لم تكتبها
07	**إجابة السؤال التفاعلي السابع** ج) لأنها تُستخدم لجمع معلوماتك

إجابات الأسئلة التفاعلية

08	**إجابة السؤال التفاعلي الثامن** د) تجاهلها أو حذفها
09	**إجابة السؤال التفاعلي التاسع** أ) أن تحتوي على حروف وأرقام ورموز
10	**إجابة السؤال التفاعلي العاشر** د) منع الآخرين من فتح الحساب حتى مع معرفة كلمة المرور
11	**إجابة السؤال التفاعلي الحادي عشر** ج) التحقق من هويته أولًا
12	**إجابة السؤال التفاعلي الثاني عشر** ب) إبلاغ المنصة وتنبيه الآخرين
13	**إجابة السؤال التفاعلي الثالث عشر** أ) تدخل إلى الإعدادات وتتابع أماكن تسجيل الدخول

المراجع

1. Baltezarevic, Radoslav & Baltezarevic, Ivana. Social Media Impersonation as a Cybersecurity Threat. International Topkapi Congress IV, October 2024, on site: https://www.researchgate.net/publication/384657784_SOCIAL_MEDIA_IMPERSONATION_AS_A_CYBERSECURITY_THREAT

2. Cybersecurity and Infrastructure Security Agency (CISA). Use Strong Passwords., on site: https://www.cisa.gov/secure-our-world/use-strong-passwords

3. Cybersecurity Asia. The rise of cybercrime targeting older adults., on site: https://cybersecurityasia.net/rise-cyber-crime-targeting-older-adults/

4. Ernest, Nonum et al. Social Engineering: Understanding Human Factors in Cyber Security. International Journal of Convergent and Informatics Science Research, May 2025, on site: https://harvardpublications.com/hijcisr/article/view/326

5. IBM. What is malware?, on site: https://www.ibm.com/think/topics/malware

6. Information Commissioner's Office (ICO). What is personal data?, on site:https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/

7. Kosinski, Matthew. IBM. What is phishing?, on site: https://www.ibm.com/think/topics/phishing

8. National Cyber Security Centre (NCSC). Phishing., on site: https://www.ncsc.gov.uk/guidance/phishing

9. National Cyber Security Centre (NCSC). Turn on 2-step verification (2SV)., on site: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email

10. Okechukwu, Chinyere & Bachmann, Pavel. Digital Marketing Risks for Aging Populations: The Threat of Online Scams to Older Adults., September 2025, on site: https://www.researchgate.net/publication/396233133_Digital_Marketing_Risks_for_Aging_Populations_The_Threat_of_Online_Scams_to_Older_Adults

11. Orłowska, Agnieszka. Cybersecurity and Cyberthreats in Social Media., December 2022, on site: https://www.researchgate.net/publication/367048439_Cybersecurity_and_Cyberthreats_in_Social_Media

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

16555 - 40466379 - 51045944

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