الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

الهندسة الاجتماعية والتصيد الاحتيالي

الشريحة المُستهدَفة
كبـــار القَـــدْر

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبـادئ عامة في السلامة الرقميـة
الهندسة الاجتماعية والتصيد الاحتيالي

الشريحة المُستهدَفة

كبـــار القَـــــدْر

كُتَيّب المُدَرّب

المبادرة الوطنية للسلامة الرقمية

تمهيد

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

تم تصميم هذا الكُتَيّب بهدف توعية كبار القَدْر بمبادئ السلامة الرقمية، وأفضل الممارسات التي تساعدهم على تفادي المخاطر السيبرانية؛ حيث يهدف هذا الكتيّب إلى تعزيز وعيهم بأبرز هذه التهديدات؛ مثل: التصيد الاحتيالي، والهندسة الاجتماعية؛ 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 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

التصيّـــد الاحتيالـــي

مفهوم التصيّد الاحتيالي

محاولة إقناع الشخص بأنّ الرسالة أو الاتصال واردٌ من جهةٍ رسميةٍ بهدف الحصول على معلومات سرية.

السمات الرئيسية

- تقليد الرسائل أو المواقع الرسمية في الشكل والمحتوى
- استخدام لغة مُطمئنة أو مُقْلِقَة لدَفْع الشخص إلى الرَّدّ
- الاعتماد على الخداع النفسي بدلًا من الأساليب التقنية
- استهداف فئات أكثر ثقة أو أقل استخدامًا للتقنيات الحديثة
- الانتشار الواسع بسبب سهولة التنفيذ وتكرار القوالب

رسائل واتساب Whatsapp الاحتيالية

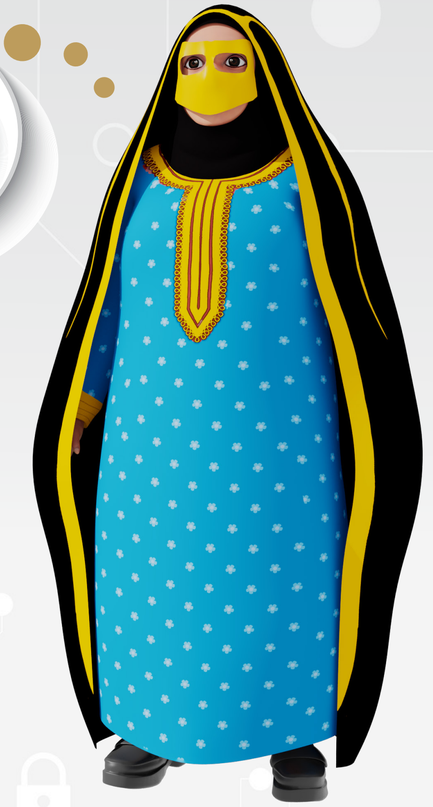
يُستخدم واتساب Whatsapp لإرسال رسائل تحمل أسماء مؤسسات معروفة، وتُطلب فيها معلومات شخصية بدعوى وجود تحديث أو مشكلة ما.

الخصائص الشائعة لهذه الرسائل

- تحتوي على شعارات حقيقية أو مأخوذة من مواقع رسمية
- تبدأ بتحية عامة غير موجّهة بالاسم
- تتضمّن رابطًا يشير إلى صفحة شبيهة بموقع معروف
- يطلب الرابط إدخال بيانات حساسة مثل الاسم أو الرقم البنكي

الرسائل النصية القصيرة الاحتيالية

تصل هذه الرسائل إلى الهاتف المحمول، وغالبًا ما تحتوي على نصوص قصيرة وعاجلة تطلب التفاعل بسرعة.



العناصر المكررة في هذه الرسائل

- استخدام عبارات مثل: "أوْقَفْنا حسابك"، "ربحت معنا"، "تم شحن الطرد"...
- إدراج روابط مختصرة بصيغة يصعب التحقق منها
- استخدام أسلوب مباشر دون تقديم تفاصيل كافية
- استهداف الضغط النفسي من خلال تحديد مُهْلة زمنية قصيرة
- توجيه الشخص إلى صفحة تطلب منه إدخال بياناته أو تحميل تطبيق

الاتصالات الهاتفية الاحتيالية

يُجري المحتال مكالمة هاتفية، ويُقدِّم نفسه على أنه موظَّف رسمي، مستغلًا اللغة الواثقة لتبرير طلبه للمعلومات.

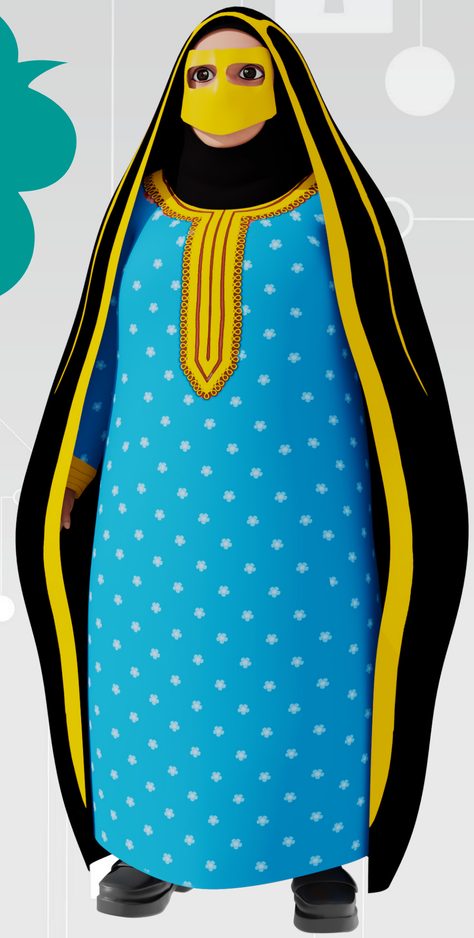
الأسلوب المستخدَم

- التظاهر بالانتماء إلى بنك أو جهة حكومية
- التطرُّق إلى قضية حساسة مثل تحويل مشبوه أو مشكلة قانونية
- الحديث بلُغَة رسمية وهدوء مبالغ فيه
- محاولة إغلاق الحديث قبل أن يتمكّن الشخص من الاستشارة أو التأكُّد
- تقديم طلب مباشر للحصول على بيانات الحساب أو رمز التحقُّق

المواقع الإلكترونية المُزيَّفة

يتم إعداد صفحات إلكترونية تحاكي مواقع البنوك أو الجهات الحكومية من حيث التصميم والعناوين، مع تغييرات طفيفة.

السمات التي تُميِّز هذه المواقع



- التشابه الكبير في الألوان والشعارات والعناوين
- استخدام روابط تتضمن حروفًا إضافية أو تغييرات بسيطة في التهجئة
- عدم وجود شهادة أمان (https) أو رمز القفل بجانب الرابط
- تضمين نموذج لتسجيل الدخول أو تحديث البيانات
- جَمْع البيانات المُدخلة مباشرة وإرسالها للمخترقين

رسائل الجوائز والهدايا المُزيَّفة

تُرسَل هذه الرسائل بهدف إقناع الشخص بأنه فاز بجائزة قيِّمَة، ويُطلَب منه بيانات لاستلامها.

العناصر الأساسية لهذه الرسائل

- عرض جائزة غير متوقعة (هاتف، مبلغ مالي، رحلة)
- طلب إدخال بيانات شخصية عبر رابط خارجي
- إنهاء الاتصال أو المراسلة فور استلام البيانات أو المبلغ
- تكرار عبارات التحفيز مثل "مبروك، أنت الرابح"
- إدراج مبلغ رمزي مقابل "تكاليف الشحن"

انتحال هوية مؤسسات رسمية

يستخدم المحتالون أسماء جهات رسمية للتواصل، مما يمنحهم مصداقية مُزيَّفة لدى المتلقي

المظاهر المستخدمة

ذِكْر أسماء مثل البنك، الشرطة، المحكمة، شركات معروفة

إرسال خطابات رسمية التصميم أو مكالمات بلغة قانونية

الحديث عن مخالفات، تجميد حساب، أو تحقيق قانوني وهمي

استخدام التهديد غير المباشر لدفع الشخص للاستجابة

توجيه الطلب بسرعة قبل أن يُتاح للضحية التحقُّق

التصيّد عبر وسائل التواصل الاجتماعي

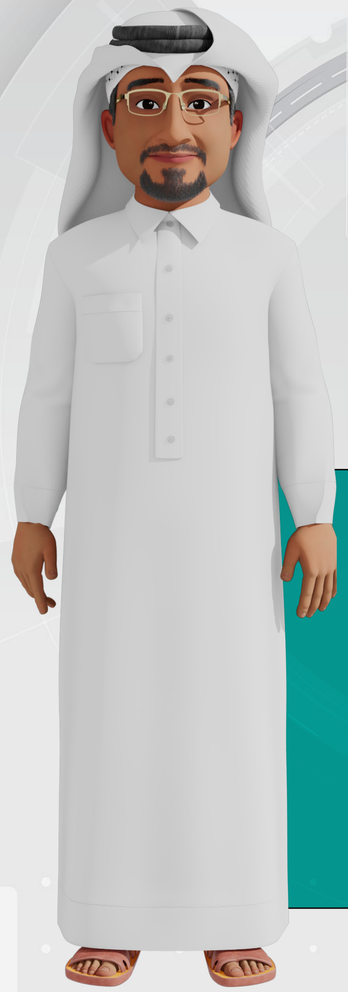
يتم استخدام التطبيقات الاجتماعية كوسيلة للوصول إلى الضحية من خلال حسابات حقيقية أو مُزيَّفة.

الأساليب الشائعة

- إرسال رسالة من حساب لصديق يقول "أحتاج مساعدتك"
- مشاركة روابط تبدو طبيعية مثل "انظر هذا الفيديو"
- طلب تحويل مبلغ مالي من خلال محادثة مباشرة
- انتحال شخصية مؤسسات وتقديم عروض مُزيَّفة
- استخدام أساليب ودية ولغة عادية لبناء الثقة قبل الاحتيال

رسائل تنتحل شخصية الأقارب

تُرسل الرسالة من رقم مجهول، ويدّعي صاحبها أنه أحد الأبناء أو الأقارب، غالبًا بهدف الحصول على تحويل مالي عاجل.



الخطوات التي يعتمدها المحتال في هذا النوع

- تقديم نفسه بأنه حفيد أو قريب مع تغيير الرقم
- الادّعاء بأنه في موقف طارئ يتطلب مساعدة مالية
- مَنْع الشخص من التحقُّق من هويته بحجة "السرية" أو "الحرج"
- استخدام معلومات عامة مثل الاسم الأول لإقناع الضحية
- طلب التحويل إلى رقم حساب أو خدمة دفع سريع

حملات التبرع الاحتيالية

يتم إنشاء حملات مُزيَّفة على شكل منشورات أو رسائل، ويُطلَب فيها المساعدة لحالات إنسانية غير حقيقية.

الطرق المستخدمة

- عرض صورة مُؤثّرة أو فيديو لحالة طبية أو كارثة
- استخدام لهجة إنسانية ومُؤثّرة لطلب التبرع
- تقديم رقم حساب بنكي أو رقم جوّال شخصي
- عدم وجود أيّ جهة موثقة خلف الحملة
- اختفاء الرسائل أو الصفحات بعد استلام الأموال

السؤال التفاعلي الأول

1- ما هو التصرف الصحيح عند تلقّي بريد إلكتروني يطلب تحديث معلوماتك البنكية؟

- أ. إرسالها فورًا
- ب. الضغط على الرابط للتحقق
- ج. حذف الرسالة دون مراجعة
- د. مراجعة الجهة الرسمية من خلال موقعها أو الاتصال المباشر

السؤال التفاعلي الثاني

2- أي مما يلي يُعدّ مؤشرًا على أنّ الرسالة احتيالية؟

أ. تحتوي على شعارات رسمية

ب. تُطلَب فيها معلومات خاصة بشكل مباشر

ج. مكتوبة بلغة مهذّبة

د. تأتي من بريد إلكتروني رسمي

السؤال التفاعلي الثالث

3- إذا اتصل بك شخص وقال: إنه من الشرطة، ويطلب تحويل مبلغ لتجنُّب مخالفة، فكيف تتصرف؟

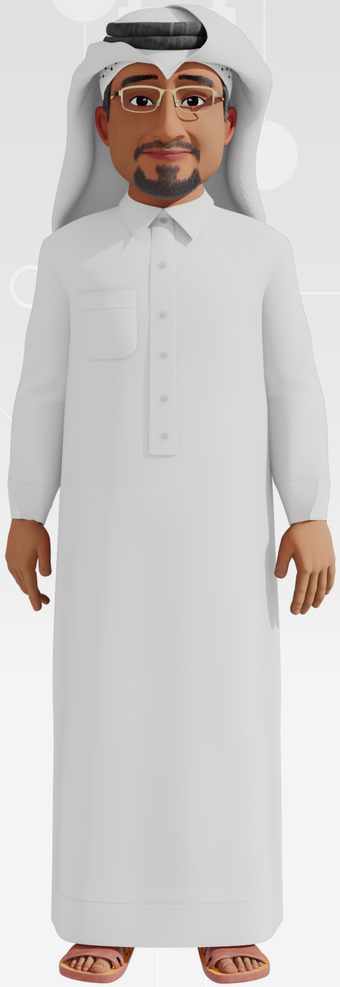
أ. تسأل عن تفاصيل المشكلة وتُحوِّل المبلغ فورًا

ب. تتواصل مع الشرطة بنفسك عبر الأرقام الرسمية

ج. تُخبره بأنك مشغول وتغلق

د. تطلب منه إرسال الطلب عبر البريد الإلكتروني

السؤال التفاعلي الرابع



4- كيف يمكنك تمييز الموقع المزيف من الموقع الحقيقي؟

أ. من حجم الصفحة وتصميمها

ب. من سرعة التحميل

ج. من العنوان الإلكتروني وشهادة الأمان

د. من عدد الصور والشعارات

السؤال التفاعلي الخامس

5- ما أول خطوة يجب اتخاذها عند استلام رسالة من رقم جديد يَدّعي أنه حفيدك ويطلب تحويل مالي؟

أ. الرد مباشرة وسؤاله عن المبلغ

ب. إجراء مكالمة تأكيد مع العائلة

ج. تحويل المبلغ بدافع الحرج

د. إرسال رسالة عبر واتساب WhatsApp فقط

الهندسة الاجتماعية

مفهوم الهندسة الاجتماعية

مجموعة من الحِيَل التي يستخدمها المحتال للتَّلاعب بالشخص نفسيًّا من أجل الحصول على معلومات سرية، دون الحاجة إلى تقنيات مُعقَّدة.

السمات الأساسية

- بناء علاقة ثقة مُزيَّفة مع الضحية
- استغلال حُسن النية والرغبة في المساعدة
- استخدام موقف اجتماعي أو عاطفي لدَفْع الشخص إلى التجاوب
- إدخال الضحية في حوار يبدو طبيعيًّا، ثم التدرج بطلب المعلومات
- التظاهر بالاهتمام أو المعرفة السابقة لتقوية الانطباع المزيّف

الفرق بين الهندسة الاجتماعية والتصيّد الاحتيالي

الهندسة الاجتماعية تختلف عن التصيّد من حيث الطريقة؛ حيث إنها تُركّز على التأثير المباشر على الشخص، وليس على الرابط أو الموقع.

الاختلافات الأساسية

- التصيّد يتم عبر رسالة أو رابط إلكتروني، الهندسة الاجتماعية تعتمد على المحادثة المباشرة
- الهندسة الاجتماعية تُستخدم في الواقع اليومي، الهاتف، أو اللقاءات، أكثر من البريد الإلكتروني
- المحتال في الهندسة الاجتماعية يُقدّم نفسه على أنه شخص حقيقي يتفاعل معك
- يتم بناء الاحتيال على مراحل وليس في رسالة واحدة
- تشمل أحيانًا لقاءات أو اتصالات طويلة قبل محاولة السرقة

استخدام العاطفة

يعتمد المحتال في الهندسة الاجتماعية على إثارة مشاعر محددة لدى الضحية لدَفْعه إلى اتخاذ قرارات سريعة.

المشـــاعـر الأكـــــثر استخـــدامًا

- الخوف: من مشكلة قانونية، تهديد، أو تجميد حساب
- الثقة: من خلال الحديث بلغة رسمية أو مهنية
- الإلحاح: وضع الضحية تحت ضغط الوقت
- الإحراج: من خلال طلب شخصي يصعب رفضه
- العطف: بإظهار الحاجة الماسة للمساعدة

التدرج في الطلبات

لا يبدأ المحتال بطلب كلمة المرور مباشرة، بل يستخدم أسلوبًا تدريجيًّا، يبدأ بأمور بسيطة، ثم ينتقل إلى ما هو حسّاس.

مراحل التدرج

يبدأ بطلب غير ضارّ مثل الاسم
أو تأكيد رقم الهاتف

يستمر بإظهار التعاون والاهتمام

يطلب في الخطوة التالية
تفاصيل أكثر دقة

يُقدّم مُبرِّرات مقنعة لكل طلب

يُنهي المحادثة بعد حصوله
على ما يريد دون إثارة الشك

انتحال صفة رسمية

يتقمَّص المحتال دور موظف في جهة معروفة، مثل البنك أو الدعم الفني؛ ليكسب ثقة الضحية بسرعة.

الوسائل التي يعتمدها

- استخدام لغة متخصّصة تُوحي بالخبرة
- ذِكْر أسماء جهات معروفة لإضفاء المصداقية
- الادعاء بوجود خطأ تقني يستوجب الدخول إلى الحساب
- توفير "معلومات" عامة لإقناع الضحية بأنه يعرفه
- استخدام أدوات تكنولوجية مثل البريد الرسمي المزوّر أو عرض الشاشة

المكالمات الهاتفية والشخصية المُـزيَّفة

يتـم التواصـل مـع الضحيـة مـن خـلال مكالمـة هاتفيـة أو حتـى لقـاء شـخصي مباشـر، مـع تقديـم سـيناريو مقنـع.

الخصائص المتكررة

- يرتدي المحتال لباسًا رسميًّا أو يُعرِّف بنفسه كموظف دعم
- يزور المنزل بحجة الصيانة أو متابعة اشتراك خدمي
- يطلب من الشخص إدخال رمز أو فتح جهازه لتحديث النظام
- يتظاهر بتقديم المساعدة الفنية لحلّ مشكلة معينة
- يغادر فور الحصول على البيانات أو الوصول إلى الجهاز

حِيَل الدعم الفني

يتصل المحتال، ويدّعي أنه من فريق الدعم الفني لشركة الهاتف أو مزوّد الإنترنت، ويتحدَّث بلغة فنية لإقناع الضحية.

الخطوات المعتادة

- الإشارة إلى مشكلة في الاتصال أو حساب الخدمة
- طلب الدخول إلى جهاز الحاسوب أو الهاتف
- استخدام أدوات تحكُّم عن بُعد (مثل تطبيقات الدعم)
- إقناع الضحية بإعطاء رموز أو كلمات مرور
- استخدام الجلسة للوصول إلى البيانات أو تغيير كلمات المرور

علامات تكشف الدعم الفني المُزيَّف

- الاتصال غير المسبوق من شخص يطلب التحكم بجهازك
- الطلب الفوري لإعطاء كلمات مرور أو رموز تحقُّق
- التحدث بلُغة تقنية مُفْرِطة لإرباك المستمع
- الإصرار على تنفيذ خطوات معينة بسرعة
- عدم وجود توثيق رسمي للطلب أو للمكالمة

الهندسة الاجتماعية عبر تطبيقات المراسلة

تُستخدم تطبيقات مثل واتساب أو تيليجرام لبناء علاقة مُزيَّفة، ثم خداع الشخص لاحقًا، خاصةً في حالات التواصل الأولي.

المراحل التي يتبعها المحتال

- بَدْء الحديث باسم مستعار أو حساب مزيف
- استخدام صور وعبارات تُوحي بالثقة
- التحدُّث بهدوء وودّ، مع خلق صلة اجتماعية
- الانتقال إلى الحديث عن "فرصة"، "مشكلة"، أو "طلب مساعدة"
- طرح طلب مباشر للحصول على المال أو البيانات

الهندسة الاجتماعية الموجَّهة لكبار القَدْر

كثيرٌ من محاولات الهندسة الاجتماعية تَستهدف كبار القَدْر لأسباب ترتبط بالخبرة والتفاعل الرقمي.

أبرز العوامل التي تُشجّع المحتالين

- الاحترام والثقة الممنوحة للمؤسسات الرسمية
- قلّة الاطلاع على الأساليب الحديثة في الخداع
- سرعة الاستجابة للمواقف الإنسانية
- الافتقار إلى التحقُّق الدقيق في التواصل الرقمي
- وجود مشاعر قوية تجاه العائلة والأبناء تُسهّل الاستغلال

حوادث واقعية شائعة للهندسة الاجتماعية

تم تسجيل العديد من الحالات الواقعية التي تعرَّض فيها كبار القَدر لهجمات هندسة اجتماعية أدَّت إلى فقدان

الأنماط المتكررة

- مكالمة هاتفية تدّعي وجود مشكلة بنكية ثم سرقة الحساب
- زيارة ميدانية لمنزل الضحية بهدف "فحص الاتصال"
- رسالة من حفيد مزيف يطلب تحويلًا ماليًّا عاجلًا
- دعم فني وهمي يطلب التحكم في الهاتف
- استدراج عبر محادثة طويلة تؤدي إلى الكشف عن بيانات حساسة

السؤال التفاعلي السادس

6- ما العنصر الأساسي الذي تعتمد عليه الهندسة الاجتماعية؟

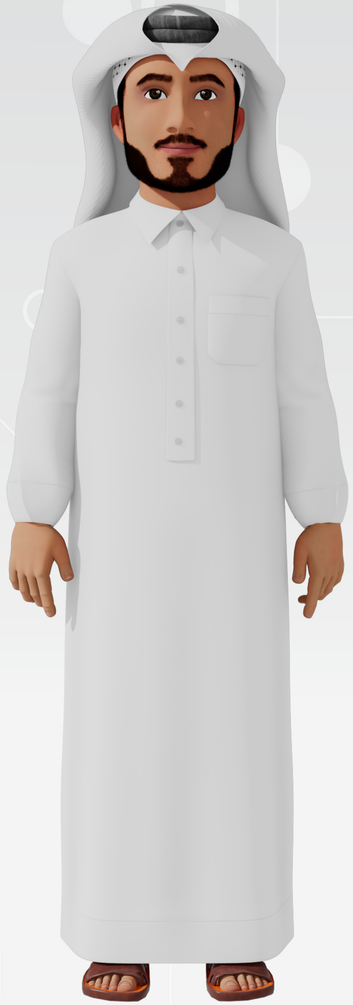
أ. المعرفة التقنية العالية

ب. التشفير والبرمجة

ج. التأثير النفسي وبناء الثقة

د. اختراق الشبكات

السؤال التفاعلي السابع



7- في أيّ الحالات الآتية يُحتمَل وجود محاولة هندسة اجتماعية؟

أ.	شخص يطلب رقم هاتفك في الشارع
ب.	موظف مجهول يتصل بك، ويطلب رمز تحقُّق
ج.	رسالة من شركة تطلب بريدك الإلكتروني
د.	كل ما سبق

السؤال التفاعلي الثامن

8- لماذا قد ينجح المحتال في إقناع الضحية بمشاركة معلوماته؟

أ. استخدام لهجة رسمية ومهنية

ب. تقديم معلومات عامة تبدو صحيحة

ج. الضغط العاطفي أو التهديد

د. جميع ما سبق

السؤال التفاعلي التاسع

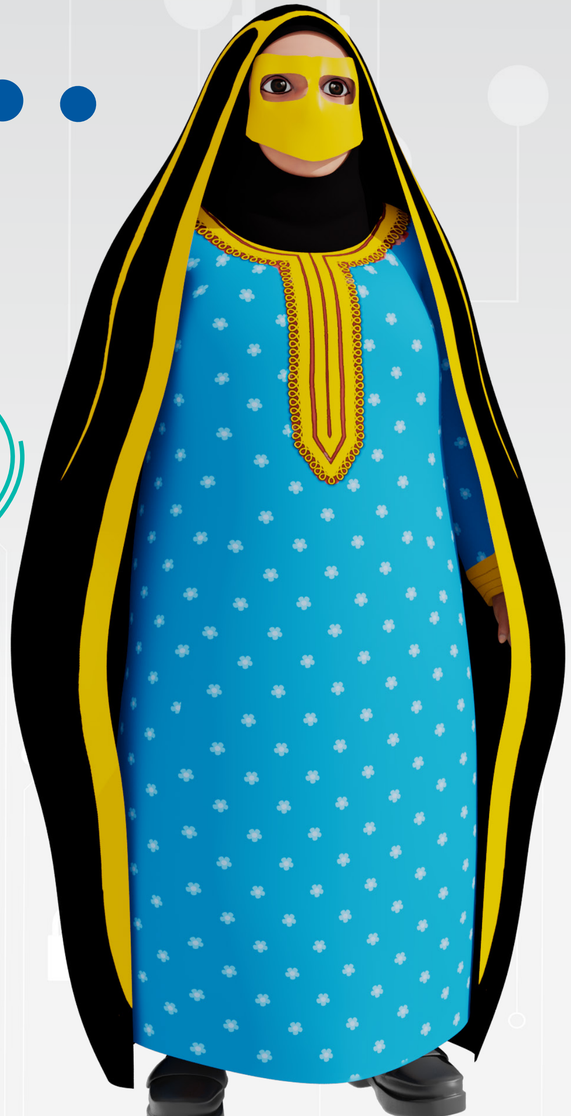
9- ما السلوك الأكثر عُرضة للاستغلال في الهندسة الاجتماعية؟

أ. استخدام الإنترنت يوميًّا

ب. حفظ كلمات السر في دفتر

ج. الثقة المطلقة في الموظفين أو الغرباء

د. تحديث الأجهزة بانتظام



السؤال التفاعلي العاشر

10- ما نوع الحيلة التي تبدأ بتواصل شخصي وودي ثم تتحول إلى طلب حساس؟

- أ. التصيّد الاحتيالي
- ب. الدعم التقني الحقيقي
- ج. الهندسة الاجتماعية
- د. الفيروسات الرقمية

الوقاية من الهندسة الاجتماعية والتصيّد الاحتيالي

المبادئ العامة للوقاية الرقمية

فَهْم أن الخداع لا يأتي دائمًا من الغرباء، بل قد يظهر من أشخاص يُقلّدون أقارب أو مؤسسات

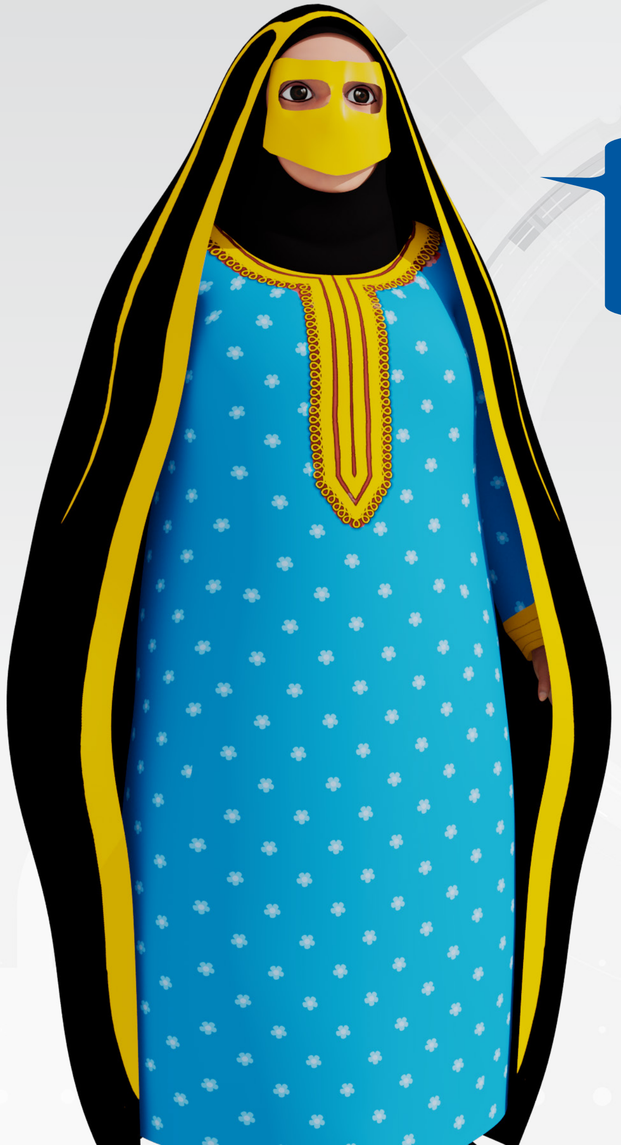
التوقُّف للحظة والتفكير قبل اتخاذ أيّ إجراء

عدم التفاعل السريع مع الرسائل أو المكالمات غير المتوقعة

الرجوع إلى العائلة أو شخص موثوق عند الشك

تجنُّب مشاركة المعلومات إلا بعد التأكُّد من هوية الطرف الآخر

التأكد من هوية المرسِل أو المتصل



أغلب عمليات الاحتيال تبدأ من جهة مجهولة تدّعي أنها معروفة. التحقق من هوية الطرف الآخر أمرٌ أساسيٌّ.

أساليب تساعد على التحقق من الهوية

- مراجعة الرقم الهاتفي عبر مُحرّك البحث أو الاتصال المباشر بالجهة الرسمية
- التأكّد من أن البريد الإلكتروني أو الحساب تابع لجهة موثوقة
- ملاحظة الفروقات الصغيرة في العناوين أو الصياغة
- استخدام مصادر رسمية (موقع إلكتروني رسمي أو رقم خدمة العملاء)
- سؤال المرسِل عن معلومات لا يعرفها إلا الطرف الحقيقي

التعامل مع الروابط والمرفقات

تُستخدم الروابط كأدوات خفية لنقل الشخص إلى صفحات مُزيَّفة أو تحميل برمجيات ضارَّة، لذلك من الضروري الانتباه قبل التفاعل معها.

الاحتياطات التي تتعلّق بالروابط والمرفقات

- عدم الضغط على الروابط في الرسائل المجهولة
- فَحْص الرابط بالنظر إلى بدايته (https) وتطابقه مع العنوان الأصلي
- فتح المواقع عبر الكتابة اليدوية بدلًا من النقر
- استخدام برنامج حماية (مضاد فيروسات) للمساعدة في الكشف عن التهديدات
- حذف الرسائل التي تحتوي مرفقات غير معروفة المصدر

خطوات وقائية على المستوى الشخصي

تطبيق عدد من العادات اليومية البسيطة يمكن أن يُقلّل من احتمالية الوقوع ضحية للهندسة الاجتماعية والتصيّد الاحتيالي.

ممارسات شخصية مفيدة للحماية

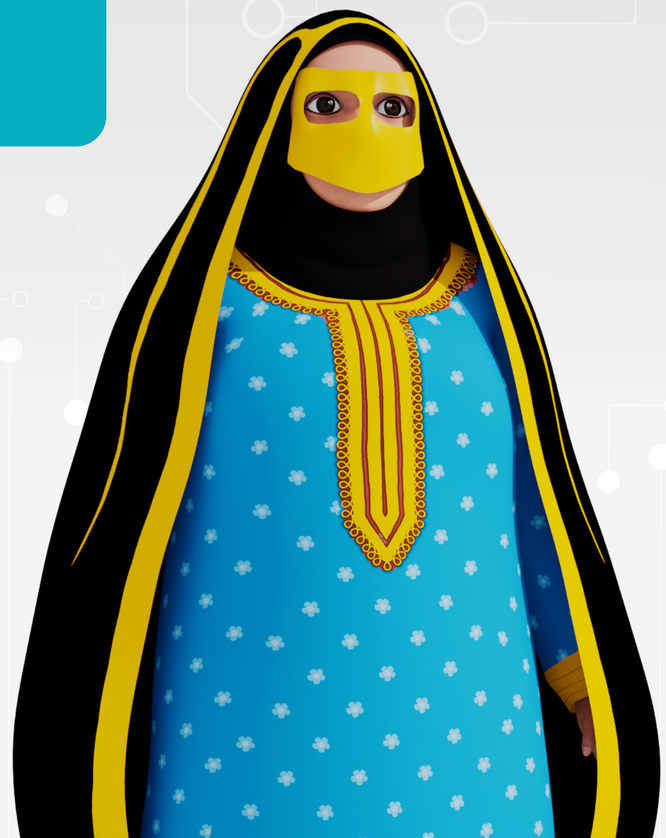
- عدم حفظ كلمات السر في دفاتر أو أوراق مكشوفة
- استخدام أرقام سرية لا ترتبط بالاسم أو تاريخ الميلاد
- تغيير كلمات المرور دوريًّا
- عدم الحديث عن الأمور المالية أو البنكية مع أيّ شخص مجهول
- تجنّب نشر معلومات خاصة على الحسابات العامة في الإنترنت

التحقُّق من الرسائل والمكالمات

الرسائل والمكالمات الاحتيالية تهدف إلى خلق شعور بالضغط على الضحية؛ لذا فإن التمهُّل والتحقُّق يساعدان في كشفها

أساليب عملية للتحقق

- الاتصال بالجهة المزعومة من خلال رقمها الرسمي قبل التجاوب
- البحث في الإنترنت عن محتوى الرسالة أو الرقم للتأكُّد إن كان محتالًا معروفًا
- مراجعة الرسالة مع أحد أفراد العائلة
- تجنُّب الرد على أيّ طلب مالي يأتي من شخص لا تعرفه شخصيًّا
- ملاحظة الأسلوب المستخدم: هل هو تهديدي؟ عاطفي؟ مبالغ فيه؟



حماية الحسابات الشخصية

- تسجيل الخروج بعد استخدام الحسابات خاصة في الأماكن العامة
- استخدام كلمة مرور قوية تحتوي على حروف وأرقام ورموز
- تحديث كلمات المرور بانتظام وعدم إعادة استخدامها
- تفعيل خاصية التحقُّق بخطوتين (رمز يصل للهاتف)
- تجنُّب الدخول إلى الحسابات من أجهزة أو شبكات عامة

التعامل مع محاولات الدعم الفني المُزيَّفة

بعض المحتالين يتواصلون على أنهم من فِرَق الدعم الفني لمزوّدي الإنترنت أو الخدمات الرقمية.

الإشارات التي تدل على أن الدعم مزيف

- الاتصال غير المسبوق من شخص يطلب التحكم بجهازك
- الطلب الفوري لإعطاء كلمات مرور أو رموز تحقُّق
- التحدث بلُغة تقنية مُفْرِطة لإرباك المستمع
- الإصرار على تنفيذ خطوات معينة بسرعة
- عدم وجود توثيق رسمي للطلب أو للمكالمة

التصرُّف عند الشك بعملية احتيال

عند الشعور أن الرسالة أو الاتصال غير طبيعي، هناك خطوات يمكن اتباعها لتجنُّب الضرر أو التفاعل مع الهجوم.

الإجراءات الأساسية عند الاشتباه

- إنهاء المكالمة أو حذف الرسالة فورًا
- التواصل مع أحد الأبناء أو الأقارب لمراجعة الوضع
- عدم الرد أو فتح الروابط المصاحبة
- مراقبة الحسابات البنكية والحسابات الإلكترونية؛ للتأكد من عدم التلاعب بها
- الإبلاغ عن الحادثة للجهات المعنية

التثقيف المستمر

- المشاركة في جلسات توعية أو ورش عمل محلية
- متابعة نشرات توعية من مؤسسات رسمية
- الاستفادة من أفراد العائلة في شرح المصطلحات الجديدة
- قراءة المقالات المبسطة التي تتناول الموضوع

السؤال التفاعلي الحادي عشر

11- ما أول إجراء يساعد على التحقق من هوية جهة أرسلت لك رسالة؟

أ. الرد مباشرة

ب. الضغط على الرابط

ج. مراجعة الجهة عبر موقعها الرسمي أو رقمها

د. مشاركة الرسالة في مجموعة واتساب WhatsApp

السؤال التفاعلي الثاني عشر

12- أيّ من العوامل التالية يُعتبر خطوة وقائية مفيدة؟

أ. استخدام كلمات سر متشابهة

ب. الدخول إلى الحسابات من الأجهزة العامة

ج. تفعيل التحقق بخطوتين للحسابات

د. حفظ كلمات السر في دفتر قريب من الجهاز

السؤال التفاعلي الثالث عشر

13- ما السلوك الذي قد يُعَرِّض الشخص لمحاولة احتيال؟

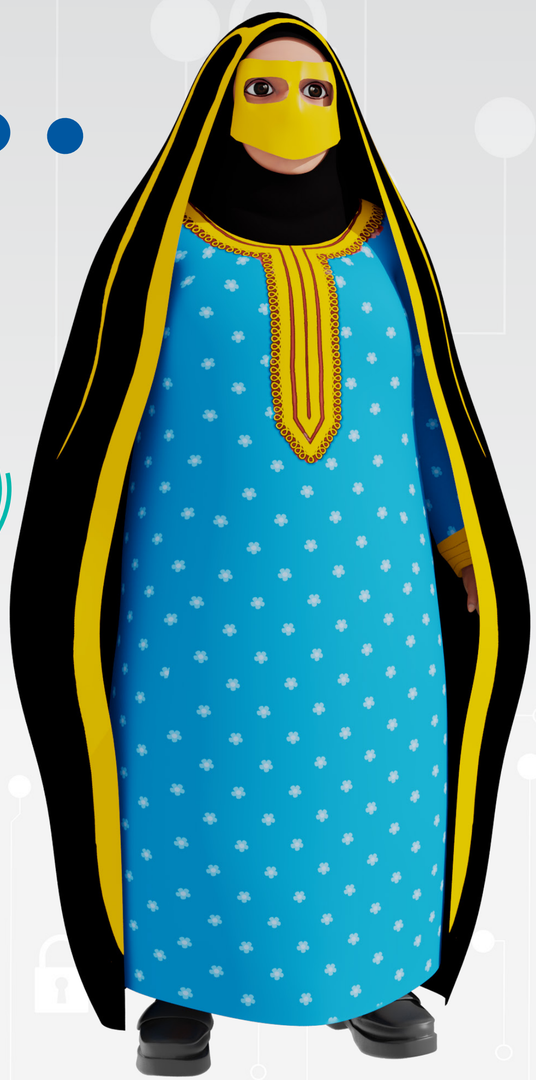
أ. الرد على أرقام مجهولة تطلب تحويلًا ماليًّا

ب. استخدام كلمات مرور طويلة

ج. تجاهل الرسائل التي تطلب معلومات حساسة

د. التواصل مع الأسرة عند الشك

السؤال التفاعلي الرابع عشر



14- كيف يمكن التعامل مع مكالمة دعم فني غير متوقعة؟

أ. إعطاء تفاصيل الدخول فورًا

ب. بمتابعة الخطوات دون نقاش

ج. إنهاء المكالمة والتحقق من الجهة الرسمية

د. السماح بالتحكم في الجهاز عن بُعد

إجابات الأسئلة التفاعلية

01	**إجابة السؤال التفاعلي الأول** د. مراجعة الجهة الرسمية من خلال موقعها أو الاتصال المباشر
02	**إجابة السؤال التفاعلي الثاني** ب. تُطلب فيها معلومات خاصة بشكل مباشر
03	**إجابة السؤال التفاعلي الثالث** ب. تتواصل مع الشرطة بنفسك عبر الأرقام الرسمية
04	**1. إجابة السؤال التفاعلي الرابع** ج. من العنوان الإلكتروني وشهادة الأمان
05	**إجابة السؤال التفاعلي الخامس** ب. إجراء مكالمة تأكيد مع العائلة
06	**إجابة السؤال التفاعلي السادس** ج. التأثير النفسي وبناء الثقة
07	**إجابة السؤال التفاعلي السابع** د. كل ما سبق

إجابات الأسئلة التفاعلية

08	**إجابة السؤال التفاعلي الثامن** د. جميع ما سبق
09	**إجابة السؤال التفاعلي التاسع** ج. الثقة المطلقة في الموظفين أو الغرباء
10	**إجابة السؤال التفاعلي العاشر** ج. الهندسة الاجتماعية
11	**إجابة السؤال التفاعلي الحادي عشر** ج. مراجعة الجهة عبر موقعها الرسمي أو رقمها
12	**إجابة السؤال التفاعلي الثاني عشر** ج. تفعيل التحقق بخطوتين للحسابات
13	**إجابة السؤال التفاعلي الثالث عشر** أ. الرد على أرقام مجهولة تطلب تحويلًا ماليًّا
14	**إجابة السؤال التفاعلي الرابع عشر** ج. إنهاء المكالمة والتحقق من الجهة الرسمية

المراجع

1. Cybersecurity and Infrastructure Security Agency (CISA). Malware, phishing, and ransomware., on site: https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

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

3. 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

4. Federal Trade Commission (FTC). Fake prize, sweepstakes, and lottery scams., on site: https://consumer.ftc.gov/articles/fake-prize-sweepstakes-and-lottery-scams

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

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

7. National Cyber Security Centre (NCSC). Spot phishing scams., on site: https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams

8. U.S. General Services Administration, Office of Inspector General (GSA OIG). Scam Alert: Beware of fake websites that mimic legitimate official U.S. government websites., on site: https://www.gsaig.gov/news/scam-alert-beware-fake-websites-mimic-legitimate-official-us-government-websites

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