الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

الشريحة المستهدفة

كبـــار القـــــدْر

كُتَيّب المُدَرّب

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مبادئ عامة في السلامة الرقمية

الشريحة المستهدفة

كبـــار القـــــدْر

كُتَيّب المُدَرّب

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.

المبادرة الوطنيّة للسلامة الرقميّة

Digital Safety National Initiative

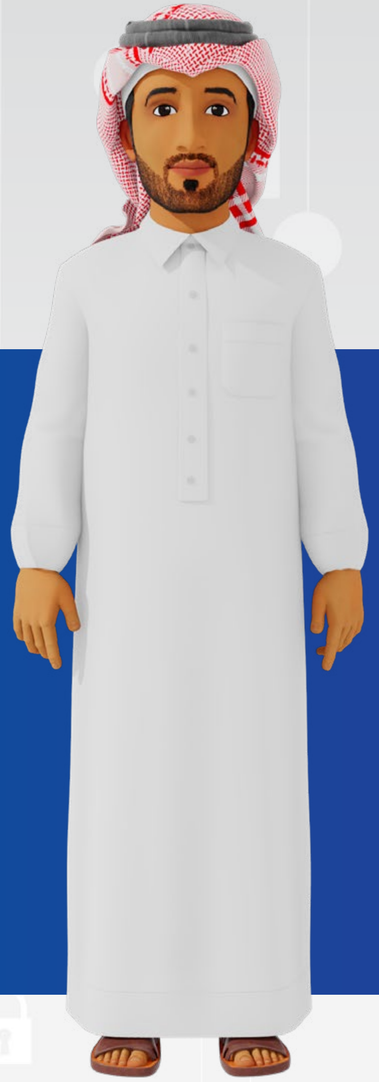
تعريف المبادرة

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

تعمل المبادرة 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:

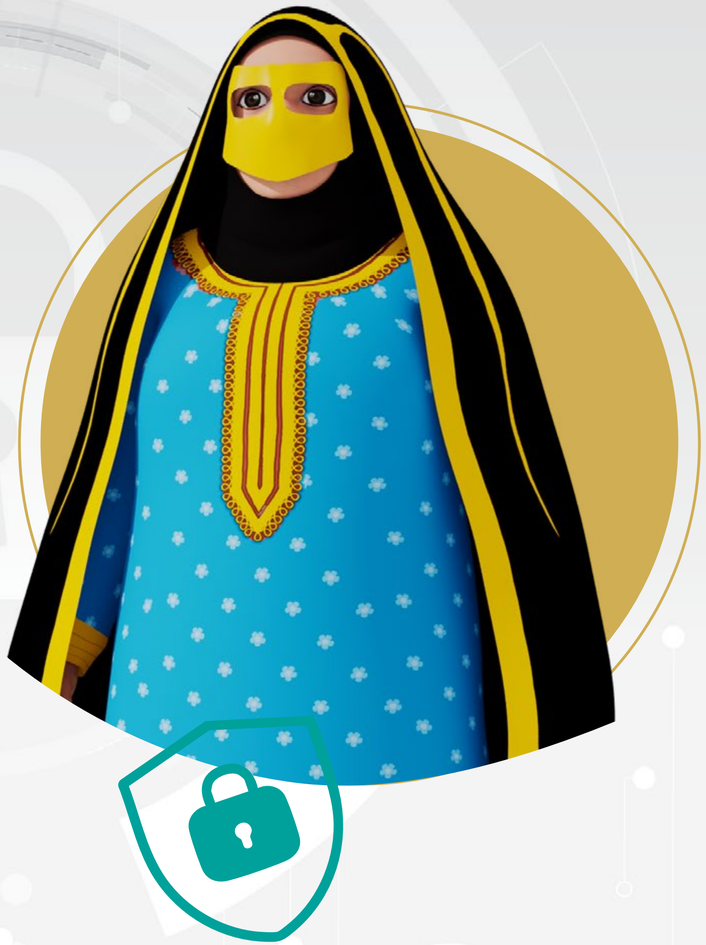


- كبار القَدْر
- المرأة والأسرة
- ذوو الاحتياجات الخاصة
- طلبة الجامعات
- العمالة الوافدة
- مؤسسات المجتمع المدني
- القطاع المالي والمصرفي

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

التهديدات السيبرانية الشّائعة

كبار القَدْر والجرائم الإلكترونية

يُعدُّ كبار القَدْر هدفًا رئيسيًّا للمهاجمين السيبرانيين بشكلٍ عامّ لعدة أسباب:

نقص المعرفة التقنية: غالباً ما يَفتقر كبار القَدْر إلى المعرفة الكافية بالتهديدات السيبرانية، مثل التصيد الاحتيالي، والبرمجيات الخبيثة

حداثة العهد بالتكنولوجيا: يضطر كبار القَدْر الآن لاستخدام الخدمات الحكومية الرقمية، لا سيما المصرفية، والتواصل عبر الإنترنت لقضاء احتياجاتهم؛ فأصبحوا أهدافًا أسهل للهجمات

الثقة العالية: يميل كبار القَدْر إلى أن يكونوا أكثر ثقة، وأن يستجيبوا للاتصالات المزيَّفة (مثل المكالمات الهاتفية أو رسائل البريد الإلكتروني)، دون التحقُّق

معلومات

الخسائر المالية الناجمة عن الاحتيال ضدّ كبار القَدْر (فوق 60 عامًا) في الولايات المتحدة الأمريكية بلغت أكثر من 3.4 مليار دولار أمريكي في 2023، بزيادة قدرها 11 % عن العام السابق.

تُقدَّر نسبة الشكاوى التي تَقدَّم بها الأمريكيون فوق سنّ الستين إلى مركز جرائم الإنترنت بنسبة 14 % من إجمالي الشكاوى خلال عام واحد.

سيناريوهات واقعية لجرائم إلكترونية

احتيال مصرفي برسائل مزيَّفة من البنوك

يتلقَّى الضحية رسالة نصيَّة أو بريداً إلكترونياً منتحلاً لهوية بنك معروف؛ يطلب منه تحديث بياناته الشخصية. وبمجرد إدخال البيانات، يتمّ سرقة الحساب المصرفي

سيناريوهات واقعية لجرائم إلكترونية

اختراق حسابات وسائل التواصل الاجتماعي

يتلقّى الضحية رسالة مباشرة عبر منصات التواصل الاجتماعي، تحتوي على رابط مشبوه يدّعي أنه من إدارة المنصة. بعد الضغط على الرابط، يتم الاستيلاء على الحساب

سيناريوهات واقعية لجرائم إلكترونية

هجوم تصيُّد من خلال شركة شحن وهمية

يتلقَّى الضَّحية رسالة تقول إن لديه شحنة تحتاج لدفع رسوم أو تحديث بيانات. فإذا أدْخَل بيانات بطاقته، تتم سرقتها

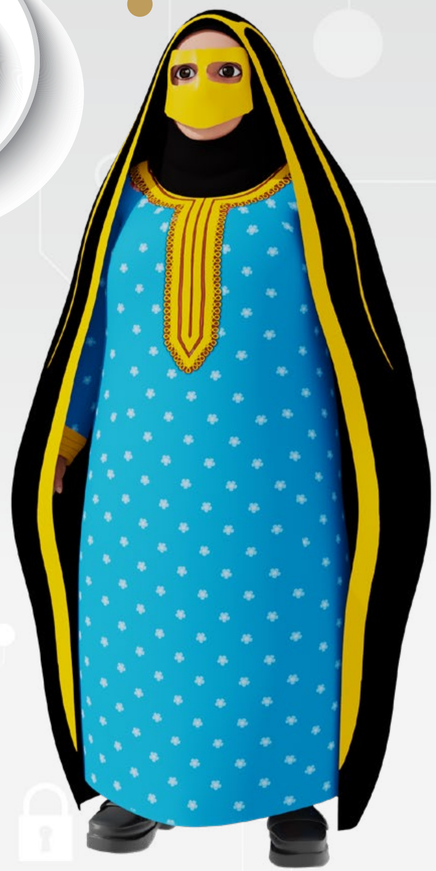
معلومات

بلغ متوسط التكلفة العالمية لاختراق البيانات (Data Breach) نحو 4.45 مليون دولار أمريكي في عام 2023.

سيناريوهات واقعية لجرائم إلكترونية

اختراق شبكة Wi-Fi المنزلية

يستغل القراصنة ضعف إعدادات الأمان في شبكة Wi-Fi منزلية، ما يُمكّنهم من اعتراض الاتصالات، والوصول إلى الأجهزة الشخصية، وسرقة البيانات الخاصة



السؤال التفاعلي الأول

1 ما هو التصرُّف الصحيح عند تلقّي مكالمة من شخص يدَّعي أنه من البنك، ويطلب منك معلومات الحساب؟

أ. | إعطاؤه المعلومات فورًا لتجنُّب أيّ مشكلة.

ب. | إغلاق المكالمة فورًا دون أيّ استفسار.

ج. | التحقُّق من هويَّة المتصل عبر الاتصال بالبنك مباشرةً.

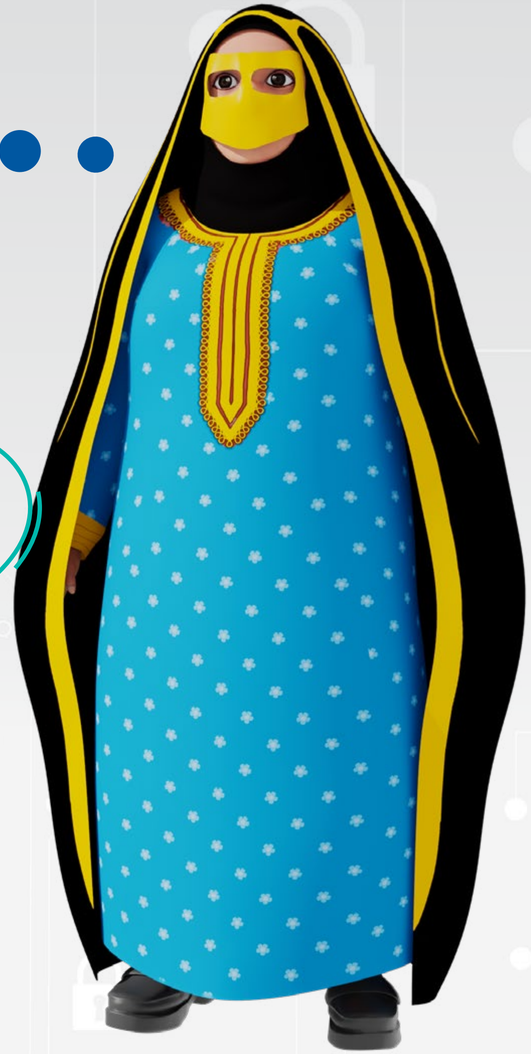
د. | إرسال رقم الحساب عبر رسالة نصية للتأكُّد من صحة الطلب.

مخاطر وسائل التواصل الاجتماعي

نَشْر المعلومات الشخصية على مواقع التواصل الاجتماعي قد يُعرِّض المستخدِم لخطر سرقة بياناته، واستخدامها بشكل غير قانوني

المعلومات الشخصية المنشورة على منصات التواصل الاجتماعي قد يتم استخدامها في جرائم التصيد الاحتيالي

السؤال التفاعلي الثاني



الهندسة الاجتماعية

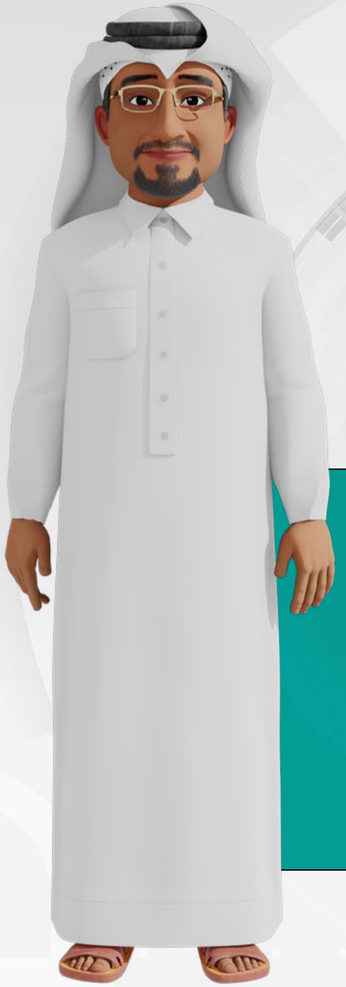
الهندسة الاجتماعية ليست هجوماً سيبرانياً، بل مجموعة من التقنيات والأدوات يستخدمها المهاجمون للإيقاع بالضحايا

من خلال استغلال المشاعر الإنسانية، يقوم المهاجمون بالاحتيال على الضحايا؛ لدفعهم لتقديم معلومات حسّاسة، بهدف استخدامها في الاحتيال

في الهندسة الاجتماعية يستغلّ المهاجمون المشاعر الإنسانية، مثل الخوف والرغبة والحاجة والتعاطف، وغيرها

لنَحْذر!

الرد على المكالمات والرسائل المزيَّفة، وعدم منح رمز OTP لأيّ شخص.

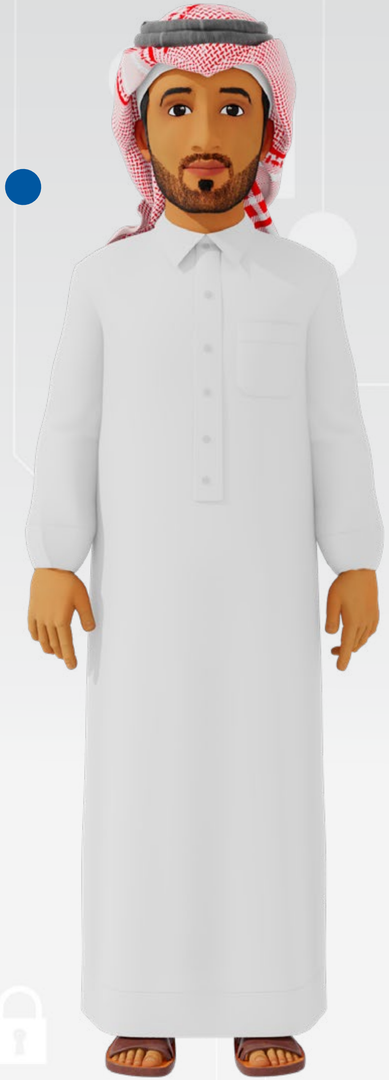


الهندسة الاجتماعية وسرقة البيانات

يهدف المهاجمون من خلال هجمات الهندسة الاجتماعية إلى الحصول على البيانات التالية:

- أرقام الضمان الاجتماعي
- أرقـــام الهواتف
- السجلات المصرفية
- البيانات الشخصية
- بيانات العمل المهمة

السؤال التفاعلي الثالث



3- ماذا تفعل إذا تلقَّيت رسالة واتساب WhatsApp مشبوهة تطلب منك معلومات حساسة؟

أ. الرد فورًا، وإرسال المعلومات المطلوبة

ب. الاستفسار عن المعلومات المطلوبة

ج. التحقُّق من هوية المُرسِل قبل اتخاذ أيّ إجراء

التصيد الاحتيالي «Phishing»

عملية احتيال يقوم من خلالها المهاجمون بانتحال شخصية أو كيان معروف، باستخدام رسالة بريد إلكتروني أو أي شكلٍ آخر من أشكال الاتصال

يستخدم المهاجمون رسائل البريد الإلكتروني لتوزيع الروابط الضارَّة؛ للحصول على بيانات حساسة، مثل: أرقام الحسابات البنكية، أو المعلومات الشخصية الخاصة بالعائلة أو العمل

معلومة

يُمثِّل التصيد الاحتيالي أكثر من 80 % من حوادث الأمن السيبراني المبلغ عنها عالميًّا، وبلغت نسبة حوادث الاختراق المتعلقة بالهندسة الاجتماعية (والتي يُشكِّل التصيد جزءًا كبيرًا منها) 44 % في 2024.

كيف تكشف هجمات التصيد الاحتيالي؟

- أسلوب الكتابة غير المألوف للمُستقبِل
- الأخطاء النحوية والإملائية
- طلب معلومات شخصية وحساسة بشكلٍ غير مألوف
- التناقض في عناوين البريد الإلكتروني والروابط
- المرفقات المشبوهة
- طلب تحميل برامج وروابط
- رسائل الجوائز المغرية

حقائق ومعلومات

نقطة الضعف الرئيسة التي يَستغلّها المهاجمون لاختراق كلمات المرور، هي اعتماد المستخدِمين على كلمات مرور بسيطة ومألوفة، مثل كلمات المرور المكوَّنة من أرقام أو حروف فقط، أو عدم تغييرها بشكلٍ منتظمٍ

كلمات المرور

كلمات المرور هي خط الدفاع الأول في وجه الهجمات الإلكترونية

كلمات المرور القوية تتألف من أكثر من 12 حرفاً

تتضمن كلمات المرور القوية حروفاً إنجليزية صغيرة وكبيرة، وأرقاماً ورموزاً

استخدام كلمات مرور سهلة التخمين قد يؤدي إلى اختراق بياناتك وأجهزتك

نقاط ضعف كلمات المرور

كلمات مرور شائعة، وسهلة التخمين، مثل 12345، أو password

استخدام معلومات شخصية في كتابة كلمة المرور، مثل: العنوان أو تاريخ الميلاد

استخدام حروف أو أرقام فقط

السؤال التفاعلي الرابع

حدِّد الصحيح والخطأ في الممارسات السيبرانية الآتية:

1 استخدام كلمة مرور واحدة لجميع الحسابات يزيد من الأمان.

أ. صحيح

ب. خطأ

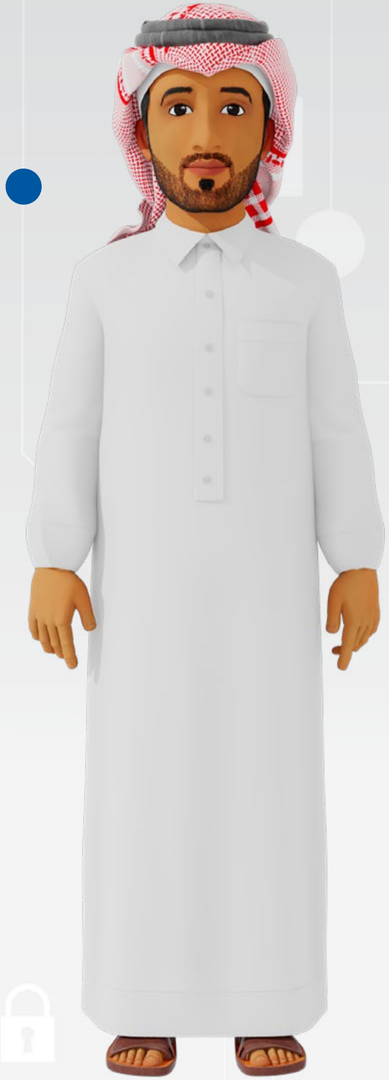
السؤال التفاعلي الرابع

2 استخدام كلمات مرور مكوَّنة من أرقام فقط يُعدّ كافيًا لحماية الحسابات.

أ. صحيح

ب. خطأ

السؤال التفاعلي الرابع

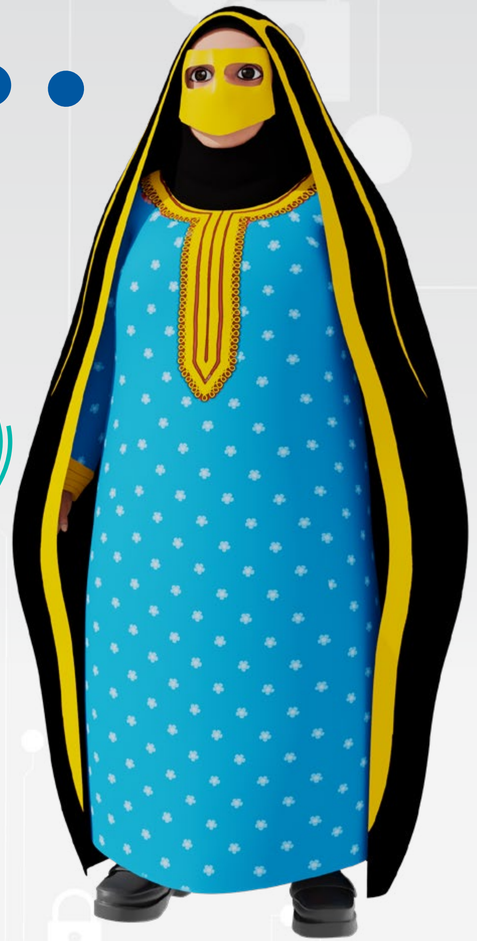


السؤال التفاعلي الرابع

4 اختيار كلمة مرور طويلة وتتنوَّع بين الحروف والأرقام والرموز لا يفيد المُستخدِم، ويصعب تَذكُّرها.

أ. صحيح

ب. خطأ



السؤال التفاعلي الخامس

5 أثناء تصفُّحك للإنترنت، ظهرت لك رسالة تفيد بأنك ربحت جائزةً كبرى، وتطلب منك إدخال بياناتك لاستلامها. ماذا تفعل؟

أ. أُدخِل بياناتي فورًا لأحصل على الجائزة.

ب. أتحقَّق من مصدر الرسالة قبل القيام بأي شيء.

ج. أُشارِك الرابط مع أصدقائي ليحصلوا على الجائزة أيضًا.

د. أتجاهل الرسالة وأخرج من الموقع فورًا.

المحور الثاني

آليات الوقاية والسلامة الرقمية

حماية كلمات المرور

- استخدام برامج إدارة كلمات المرور.
- تمكين المصادقة الثنائية (2FA).
- تغيير كلمات المرور بانتظام.
- الحذر من رسائل التصيد الاحتيالي.
- عدم كتابة كلمة المرور على ورقة أو في ملف
- حفظ كلمة المرور في برنامج إدارة كلمات المرور
- تسجيل الخروج عند الدخول من أجهزة حاسوب مشتركة.

حماية حسابات مواقع التواصل الاجتماعي

ضَبْط إعدادات الخصوصية للحدّ من الوصول غير المصرَّح به إلى معلوماتك

استخدام كلمات مرور قوية ومتميزة

تجنُّب الروابط والرسائل غير الموثوقة

تمكين المصادقة الثنائية لحماية الحسابات

التّعامُل مع حوادث الخَرق

توجد خطوات مُهمَّة للتَّعامُل مع حالات الخرق:

تغيير كلمات المرور: تغيير جميع كلمات المرور لحساباتك المُختَرقة وغير المُختَرقة فوراً

إبلاغ الجهات المعنية: الاتصال بالبنك أو المنصة المُختَرقة، والإبلاغ عن الحادث

تحديث الأجهزة والبرامج: تأكَّد من أن نظام التشغيل وبرامج الحماية مُحدَّثة؛ لتجنُّب الثغرات الأمنية

مُراقَبة الحسابات: متابعة الحسابات المالية بشكلٍ دوريّ؛ تجنُّباً لأيّ نشاط مُخالِف

استخدام برامج مُكافَحة الفيروسات: فَحْص الجهاز باستخدام برامج موثوقة لإزالة أيّ برمجيات خبيثة

تجنّب الروابط المشبوهة

التَّحقُّق من عنوان الرابط قبل النقر عليه، والتأكُّد أنه يبدأ بـ"HTTPS"

عدم الضَّغْط على الرَّوابط التي تصلك عبر رسائل غير متوقعة

الحذر من الإعلانات المنبثقة أو الروابط التي تَعِدُك بجوائز كبيرة

تجنُّب النَّقْر على الروابط من مرسلين مجهولين أو مواقع غير موثوقة

إجابات الأسئلة التفاعلية

01

إجابة السؤال التفاعلي الأول

ج) التحقُّق من هوية المتَّصل عبر الاتصال بالبنك مباشرةً.

02

إجابة السؤال التفاعلي الثاني

ج) حذف الطلب.

03

إجابة السؤال التفاعلي الثالث

ج) التحقق من هُويَّة المُرسِل قبل اتخاذ أي إجراء.

04

إجابة السؤال التفاعلي الرابع

1. خطأ.
2. خطأ.
3. صحيح.
4. خطأ.

05

إجابة السؤال التفاعلي الخامس

د) أتجاهل الرسالة وأخرج من الموقع فورًا.

المراجع

1. Federal Bureau of Investigation (FBI). Internet Crime Report 2023. on site: https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf?utm_source ic3.gov+1
2. Federal Bureau of Investigation (FBI). Internet Crime Complaint Center (IC3) Annual Report 2023. on site: https://www.ic3.gov/PSA/2024/PSA240318?utm_source ic3.gov
3. Hive Systems. 2025 Password Table. on site: https://www.hivesystems.com/password-table?utm_source Hive Systems+1
4. IBM Security. Cost of a Data Breach Report 2024. on site: https://www.ibm.com/think/insights/whats-new-2024-cost-of-a-data-breach-report?utm_source IBM+1
5. Kaspersky. Cybersecurity Statistics: Phishing and Social Engineering. on site: https://www.kaspersky.com/about/press-releases/kaspersky-reports-nearly-900-million-phishing-attempts-in-2024-as-cyber-threats-increase?utm_source kaspersky.com
6. Microsoft. Your Pa$$word Doesn't Matter. on site: https://techcommunity.microsoft.com/blog/microsoft-entra-blog/your-paword-doesnt-matter/731984?utm_source
7. Verizon. Data Breach Investigations Report (DBIR) 2024. on site: https://www.verizon.com/business/en-gb/resources/reports/dbir.html?utm_source

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