الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

حمايـــة الأجهـــزة والبيانـــات

الشريحة المستهدفة

المرأة

كُتَيّب المُدَرّب

الفهرس	رقم الصفحـة
تمهيد	8
المبادرة الوطنية للسلامة الرقمية	10
المحور الأول: أساسيات السلامة الرقمية	13
مفهوم السلامة الرقمية	14
حماية البيانات الشخصية	15
الاستخدام الآمِن للأجهزة الذكية	16
إدارة كلمات المرور	17
المصادقة الثنائية	18
شبكات Wi-Fi العامة	19
مؤشرات الاختراق	20
الإجراءات عند الاختراق	21
أمن البريد الإلكتروني	22
أمن وسائل التواصل الاجتماعي	23

الفهرس	رقم الصفحة
الحماية في أثناء التسوق الإلكتروني	24
التطبيقات والخدمات الرقمية	25
السؤال التفاعلي الأول	26
السؤال التفاعلي الثاني	27
السؤال التفاعلي الثالث	29
السؤال التفاعلي الرابع	29
المحور الثاني: التهديدات الرقمية وأساليب الوقاية	30
التصيّد الاحتيالي	31
الروابط والمواقع المزيفة	32
برمجيات الفدية	33
البرمجيات الخبيثة	34
الهندسة الاجتماعية	35

الفهرس	رقم الصفحة
التزييف العميق	36
سرقة الهوية الرقمية	37
الرسائل الاحتيالية عبر الهاتف	38
مخاطر التطبيقات المجانية	39
البرمجيات المزيَّفة لتحديث النظام	40
التخزين السحابي	41
الإعلانات المُضللة	42
إعدادات الخصوصية	43
التحديثات الأمنية	44
السؤال التفاعلي الخامس	45
السؤال التفاعلي السادس	46
إجابات الأسئلة التفاعلية	47

تمهيد

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

تـم تصميـم هـذا الكُتَيِّـب بهـدف توعيـة المـرأة بمبـادئ السلامة الرقمية، وأفضل الممارسات التي تساعدها على تجنُّـب المَخاطـر فـي البيئـة الرقميـة.

يهـدف الكتيّـب إلـى تعزيـز وعـي المـرأة بأبـرز التهديـدات التقنية التي قد تُواجهها في حياتها اليومية، مثل: التصيّد الاحتيالي، والبرمجيات الخبيثة، وبرمجيات الفدية، والهندسة الاجتماعية، والتزييف العميق، وسرقة الهوية الرقمية.

كما يُقدِّم الكُتَيِّب إرشادات عملية وإجراءات وقائية لحماية الأجهزة الشخصية، وتأمين الحسابات الإلكترونية، والتصرُّف السليم عند ملاحظة أيّ مؤشرات اختراق أو نشاط مريب.

وتُعدّ هـذه الجهـود جـزءًا مـن المبـادرة الوطنيـة للسـلامة 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 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

أساسيات السلامة الرقمية

مفهوم السلامة الرقمية

تُعدّ السلامة الرقمية أساس الاستخدام الآمِن والمسؤول للتقنيات الحديثة؛ إذ تهدف إلى حماية بيانات المرأة الشخصية من المخاطر التي قد تنشأ في أثناء التفاعل مع العالَم الرقمي.

- تُعنَى بالحفاظ على سرّية المعلومات وسلامتها وتوافرها عند الحاجة
- تشمل الممارسات التقنية؛ مثل: التشفير والتحديث. والسلوكية؛ مثل: الحذر من الروابط غير الموثوقة
- تُمكِّن المرأة من استخدام الفضاء الرقمي بثقة ومسؤولية
- تُسْهم في الحدّ من المخاطر قبل وقوعها وليس بعد حدوثها

حماية البيانات الشخصية

تُعدّ البيانات الشخصية من أكثر الأصول حساسية في الحياة الرقمية، وتشمل كلّ ما يمكن أن يكشف عن الهوية أو التفاصيل الشخصية أو تفاصيل العائلة.

تضمّ البيانات الشخصية الأسماء، الصور، أرقام الهواتف، والمعلومات البنكية

يُستحسَن تقليل مشاركتها عبر الإنترنت، وتقييد ظهورها على المنصات العامة

يجب مراجعة إعدادات الخصوصية في التطبيقات بشكلٍ دوري

يجب تخزين النُّسَخ الاحتياطية المشفَّرة للمستندات المُهِمَّة في أماكن آمِنَة

الاستخدام الآمِن للأجهزة الذكية

الأجهزة الذكية أصبحت جزءًا لا يتجزَّأ من حياة المرأة اليومية، ولكنّها في الوقت نفسه مَدْخل أساسي للمخاطر الإلكترونية إذا لم تُؤمَّن جيدًا.

ممارسات الأمان

- وَضْع كلمة مرور قوية، أو بصمة؛ لحماية الجهاز من الوصول غير المُصرَّح به
- تحديث نظام التشغيل والتطبيقات بشكلٍ مُنتظِم لسدّ الثغرات الأمنية
- تجنُّب تحميل التطبيقات من مصادر غير موثوقة
- تفعيل خاصية "العثور على الجهاز"؛ للمساعدة في استرجاعه عند الفقدان

إدارة كلمات المرور

تُعدّ كلمات المرور ركيزة أساسية لحماية الحسابات الرقمية، وهي غالبًا أوّل ما يَستهدفه المهاجمون. لذا فإنّ إدارتها بذكاء تُمثِّل عنصرًا محوريًّا في السلامة الرقمية.

يُستحسَن استخدام برامج متخصصة لإدارة كلمات المرور بأمان

تجنّب استخدام المعلومات الشخصية مثل تاريخ الميلاد أو الاسم

يُفضَّل أن تكون كلمة المرور طويلة، ومُعقَّدة، وتختلف بين الحسابات

تغيير كلمات المرور بشكلٍ دوري، خاصةً بعد أيّ نشاط مريب

المصادقة الثنائية

إضافة طبقة ثانية من الأمان تُمثِّل أحد أهم الممارسات الحديثة في حماية الحسابات؛ حيث تُتِيح التحقُّق بخطوتين مقاومة فعَّالة لمحاولات الاختراق حتى في حال تسريب كلمة المرور.

تعتمد على إدخال رمز تحقُّق يُرسَل إلى الهاتف أو البريد بعد كلمة المرور

تحمي من محاولات الدخول العشوائية أو الخداع الإلكتروني

يُنصَح بتفعيلها في البريد الإلكتروني والحسابات المصرفية ومواقع التواصل

يُفضَّل استخدام تطبيقات المصادقة بدل الرسائل النصية لزيادة الحماية

شبكات Wi-Fi العامة

على الرغم من سهولة الوصول إلى الشبكات العامة في المقاهي والمطارات، فإنها غالبًا ما تكون غير آمِنَة، وقد تُستخدَم لاعتراض البيانات.

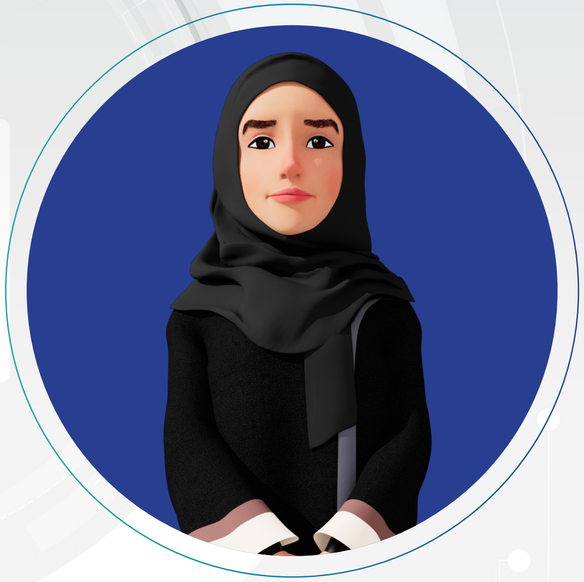
- تجنّب إدخال كلمات المرور أو البيانات البنكية في أثناء الاتصال بشبكة عامة
- استخدام خدمة VPN لتشفير الاتصال عند الضرورة
- تعطيل الاتصال التلقائي بالشبكات غير المعروفة
- التأكُّد من أن الموقع المستخدم يبدأ ببروتوكول https

مؤشرات الاختراق

التعـرُّف المبكّـر علـى علامـات الاختـراق خطـوة أساسـية للتعامـل الفعّـال مـع الخطـر قبـل أن يتفاقـم.

بُطْء مُفاجِئ في أداء الجهاز أو استهلاك مُفْرِط للطاقة

ظهور برامج أو نوافذ غير مألوفة دون تثبيت مسبق



وجود رسائل صادرة من البريد أو الحساب دون عِلْم المستخدِم

ظهور تغييرات مفاجئة في الإعدادات أو إشعارات تسجيل دخول من مواقع غريبة

الإجراءات عند الاختراق

عند ملاحظة أيّ سلوك غير طبيعي في الحسابات أو الأجهزة؛ يجب التصرُّف بسرعة، واتباع خطوات مُهمَّة للحدّ من الضرر.

- فَصْل الجهاز فورًا عن الإنترنت؛ لمنع تسريب البيانات
- تغيير كلمات المرور من جهاز آخر آمِن
- إجراء فَحْص شامل بواسطة برنامج موثوق لمكافحة الفيروسات
- حفظ الأدلة الرقمية، وإبلاغ الجهة التقنية أو مزوّد الخدمة

أمن البريد الإلكتروني

البريد الإلكتروني من أكثر الأدوات استخدامًا في الحياة الرقمية للمرأة، لكنّه في الوقت نفسه من أكثر القنوات التي تُستغَلّ في الهجمات السيبرانية.

- التحقُّق من عنوان المُرسِل قبل فتح أيّ مُرفَق أو رابط
- عدم تحميل الملفات غير المتوقعة حتى من جهات معروفة دون تأكيد مسبق
- تجنّب استخدام البريد الشخصي في التعاملات المهنية أو العامة
- حذف الرسائل مجهولة المصدر فورًا، وعدم الرد عليها

أمن وسائل التواصل الاجتماعي

تُشكِّل منصات التواصل جزءًا أساسيًّا من حياة المرأة الرقمية، لكنّها أيضًا بيئة حسَّاسة يجب التعامل معها بوعي وحرص.

- تفعيل التحقُّق بخطوتين لكل حساب شخصي
- تحديد مَن يمكنه مشاهدة المنشورات أو إرسال الرسائل
- مراجعة التطبيقات المرتبطة بالحساب وإزالة غير الضروري منها
- تجنُّب مشاركة الموقع الجغرافي أو تفاصيل الحياة اليومية بشكلٍ علني

الحماية في أثناء التسوُّق الإلكتروني

أصبحت التجارة الإلكترونية جزءًا متناميًا من حياة المرأة اليومية، مما يستدعي انتباهًا خاصًّا عند إدخال البيانات المالية أو الشخصية.

- الشراء فقط من المتاجر الإلكترونية الموثوقة والمشهورة
- استخدام بطاقات الدَّفْع الافتراضية أو محدودة القيمة قَدْر الإمكان
- التأكُّد من أن الموقع يَستخدم بروتوكول أمان (https) قبل الدفع
- تجنّب إدخال المعلومات المصرفية في أجهزة أو شبكات عامة

التطبيقات والخدمات الرقمية

تتضمَّن الهواتف الذكية عشرات التطبيقات التي تتصل بالإنترنت، وتتعامل مع بيانات المستخدِم، ما يجعل تقييم موثوقيتها أمرًا ضروريًّا.

- قراءة سياسة الخصوصية، وبيان الأذونات قبل تثبيت التطبيق
- مُراقَبة استهلاك البطارية والبيانات لاكتشاف التطبيقات المريبة
- إلغاء الأذونات غير الضرورية مثل الكاميرا أو الموقع
- حَذْف التطبيقات غير المستخدَمة بانتظام

السؤال التفاعلي الأول

1 ما الإجراء الأنسب عند ملاحظة نشاط غير معتاد في حسابك؟

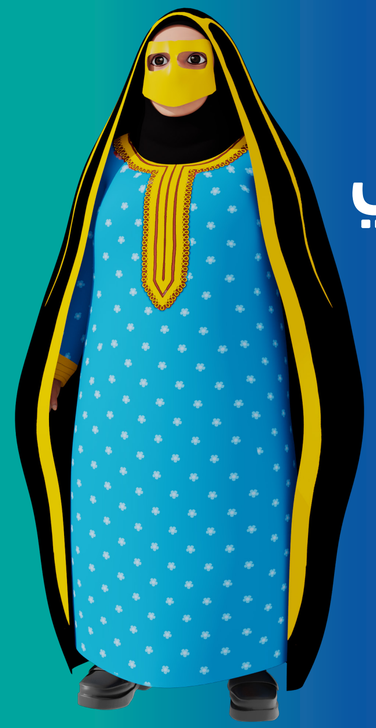
أ. تجاهل الإشعار

ب. تغيير كلمة المرور فورًا من جهاز آمِن

ج. حذف التطبيق دون إجراءات أخرى

د. مشاركة المشكلة مع الأصدقاء

السؤال التفاعلي الثاني



2 أيٌّ مِن الممارسات التالية تُعدّ أكثر أمانًا عند استخدام شبكات Wi-Fi العامة؟

أ. إجراء المعاملات البنكية فور الاتصال

ب. استخدام VPN وتجنّب إدخال بيانات حساسة

ج. مشاركة كلمة المرور مع الآخرين

د. ترك الاتصال التلقائي بالشبكات مفعلًا

السؤال التفاعلي الثالث

3 عند استخدام البريد الإلكتروني، ما الإجراء الأكثر أمانًا عند استلام رسالة تحتوي على مرفق غير مُتوقّع؟

أ. فتح المرفق مباشرة؛ لمعرفة محتواه

ب. إعادة إرسال الرسالة إلى صديقة للتأكُّد من مصدرها

ج. التحقُّق من هوية المرسِل قبل فتح المرفق، أو حذفه عند الشك

د. تجاهل الرسالة، وتركها في صندوق الوارد دون تصرُّف

السؤال التفاعلي الرابع

4 أيٌّ مِن الممارسات التالية يُعدّ الأفضل في أثناء التسوّق الإلكتروني؟

أ. إدخال معلومات البطاقة المصرفية في أيّ موقع يَعْرض تخفيضات

ب. الاتصال عبر شبكة Wi-Fi عامة في أثناء إتمام عملية الشراء

ج. مشاركة بيانات الدفع مع المتجر عبر البريد الإلكتروني لتسريع العملية

د. استخدام بطاقات ذات حدود مالية منخفضة، والتأكد من أمان الموقع قبل الدفع

المحور الثاني

التهديدات الرقمية وأساليب الوقاية

التصيّد الاحتيالي

يُعدّ التصيّد الاحتيالي من أكثر أساليب الخداع شيوعًا، ويعتمد على إرسال رسائل أو روابط تبدو حقيقية، لكنّها تهدف إلى سرقة المعلومات.

تأتي الرسائل الاحتيالية عادةً عن طريق البريد الإلكتروني أو الرسائل النصية أو عبر مواقع مُزيَّفة

تطلب الرسائل الاحتيالية إدخال بيانات مهمة؛ مثل: كلمات المرور، أو أرقام البطاقات والحسابات

تعتمد على أسلوب الإقناع باستخدام عبارات استعجال أو تهديد

يجب تجاهل الرسائل المشبوهة، والتحقُّق من مصدرها قبل أيّ تفاعل

الروابط والمواقع المزيفة

تنتشر المواقع المزيفة التي تُحاكي واجهات المتاجر أو المؤسسات الرسمية؛ لخداع المستخدمين.

قد تحمل أسماء نطاق شبيهة بالمواقع الأصلية مع تغييرات طفيفة

تُستخدَم لجَمْع بيانات تسجيل الدخول أو معلومات الدفع

يمكن التحقُّق من موثوقية الموقع عبر عنوانه (URL) أو الشهادة الأمنية (https)

يُفضَّل الوصول للمواقع مباشرة من مُحرّك البحث، وليس من روابط مُرسَلة

برمجيات الفدية

هي برمجيات خبيثة تقوم بتشفير الملفات، وتطلب فدية مالية مقابل فكّ التشفير.

تصل غالبًا عبر مُرفَقات البريد أو روابط مشبوهة

بعد الإصابة، يُمنَع المستخدِم من الوصول لملفاته

حتى بعد الدفع، لا يوجد ضمان لاسترجاع البيانات

الوقاية تكون من خلال النَّسْخ الاحتياطي المنتظم وتجنُّب المرفقات المجهولة

البرمجيات الخبيثة

تشمل مجموعة من البرمجيات التي تُزرَع داخل الأجهزة؛ بغرض التخريب أو سرقة البيانات.

- قد تختبئ في تطبيقات أو ملفات تبدو طبيعية
- يمكن الوقاية منها عن طريق تثبيت برامج مكافحة الفيروسات وتحديثها باستمرار
- تتسبّب في بُطْء النظام أو سرقة كلمات المرور أو مراقبة الأنشطة
- تجنّب تحميل البرامج من مواقع غير موثوقة

الهندسة الاجتماعية

يستهدف المهاجمون من خلالها سلوك الإنسان بدل الثغرات التقنية، عبر الخداع والتلاعب النفسي.

قد يتظاهر المُهاجِم بأنه موظف دعم أو يعمل في جهة رسمية

يَستخدم أساليب عاطفية مثل الاستعجال أو الإلحاح للحصول على معلومات مهمة

يجمع المعلومات من حسابات التواصل لبناء الثقة مع المستخدِم، ومِن ثَمَّ خداعه

يُنصَح بعدم مشاركة أيّ بيانات دون التحقُّق من هوية الطرف المقابل

التزييف العميق

تقنية قائمة على الذكاء الاصطناعي تُستخدَم لتوليد صور أو فيديوهات مُزيَّفَة تُشبه الحقيقية بشكل كبير.

يمكن أن تُستخدَم لانتحال الهوية أو نشر محتوى مُضلّل

يَصْعُب على المستخدِم العادي اكتشافها دون أدوات تحليل

يُنصَح بعدم إعادة نشر أيّ محتوى قبل التحقُّق من مصدره

استخدام أدوات كشف التزييف وبرامج تحليل الوسائط الرقمية

سرقة الهوية الرقمية

تَحْـدُث عندمـا يتمكّـن أحدهـم مـن الحصـول علـى معلومـات شـخصية واسـتخدامها باسـم الضحيـة.

تشمل سرقة الحسابات، أرقام البطاقات، أو البريد الإلكتروني، وغير ذلك

قدتُستخدَم البيانات في عمليات احتيال مالي أو اجتماعي

تقليل مشاركة البيانات الشخصية يُقلِّل من احتمالية التعرُّض لسرقة الهوية

المراقبة الدورية للنشاطات المالية تساعد في الاكتشاف المبكر لأي خطر

الرسائل الاحتيالية عبر الهاتف

هي شَكْل من أشكال التصيُّد يَستخدم الرسائل النصية القصيرة كوسيلة للخداع.

تحتوي على روابط تدّعي تقديم جوائز أو تحديثات بنكية

النقر عليها قد يؤدي إلى سرقة البيانات أو تثبيت برمجيات ضارَّة

يُنْصَح بعدم فتح أيّ رابط من مُرسِل غير معروف

التواصل مباشرة مع الجهة الرسمية؛ للتأكد من مصداقية الرسالة

مخاطر التطبيقات المجانية

تُقدِّم بعض التطبيقات خدمات جذّابة، لكنها تجمع بيانات المستخدِمين دون تصريح واضح.

- تطلب أذونات كثيرة تتجاوز حاجتها الفعلية
- قد تتابع الموقع أو تسجّل الأنشطة في الخلفية
- قراءة سياسة الخصوصية قبل التثبيت خطوة أساسية
- حذف التطبيقات غير الضرورية أو المشبوهة بشكل دوري

البرمجيات المزيّفة لتحديث النظام

يلجأ المهاجمون إلى إرسال إشعارات مُزيَّفة تُوهِم المستخدِم بأنّ جهازه يحتاج إلى تحديث فَوري.

بمجرد الضغط على الرابط، تُنزَّل برمجيات ضارَّة

يجب اعتماد التحديثات الرسمية فقط من إعدادات الجهاز

عدم تحميل أيّ ملف تنفيذي من بريد إلكتروني أو موقع مجهول

تحديث النظام بانتظام يُغْلِق الثغرات الأمنية

التخزين السحابي

يُعدّ التخزين السحابي وسيلةً مريحةً، لكنَّه قد يصبح خطرًا إذا أُسِيء استخدامه.

- رفع الملفات الحساسة دون تشفير يُعرِّضها للسرقة
- مشاركة روابط عامة قد تَمْنح الآخرين صلاحية الوصول غير المقصود
- يُنصَح باستخدام خدمات سحابية موثوقة، وتفعيل المصادقة الثنائية
- حَذْف الملفات القديمة من الحسابات السحابية بانتظام

الإعلانات المُضلّلة

تُستخدم بعض الإعلانات المموّلة على الإنترنت وسيلة لنشر الروابط الخبيثة.

تَدَّعي بعض الإعلانات تقديم خصومات أو فرص ربح فورية

النقر عليها يؤدّي إلى صفحات تُحمِّل برمجيات غير آمِنَة

تجنّب الضغط على الإعلانات غير الموثوقة أو المثيرة للفضول

استخدام إضافات حجب الإعلانات على المتصفّح يُعزّز الأمان

إعدادات الخصوصية

عـدم تفعيـل إعـدادات الخصوصيـة يمنـح الغربـاء إمكانيـة الوصـول إلـى البيانـات الشـخصية.

- مراجعة إعدادات الحسابات الاجتماعية، وتحديد مَن يمكنه رؤية المنشورات
- حَصْر قبول طلبات الصداقة بالأشخاص المعروفين
- عدم مشاركة تفاصيل الحياة اليومية بشكل متكرّر
- ضَبْط إعدادات الموقع لتجنُّب تتبُّع الموقع الجغرافي تلقائيًّا

التحديثات الأمنية

تُعدّ التحديثات الدورية خطّ الدفاع الأخير ضدّ التهديدات الجديدة.

تأجيل التحديثات يَجْعل الجهاز عُرْضة للبرمجيات الخبيثة

تفعيل خاصية التحديث التلقائي لجميع التطبيقات والأنظمة

تحتوي التحديثات على تصحيحات لثغرات تُستغَل في الاختراقات

إعادة تشغيل الجهاز بعد التحديث لضمان تثبيت الحماية بالكامل

السؤال التفاعلي الخامس

5 أيّ من العبارات التالية يُعبِّر عن أسلوب "الهندسة الاجتماعية"؟

أ. استخدام برامج لتشفير الملفات

ب. إقناع المستخدم بمشاركة معلوماته طوعًا عبر الخداع

ج. اختراق النظام عبر ثغرة تقنية

السؤال التفاعلي السادس

6 ما الإجراء الأفضل لتجنُّب الإصابة ببرمجيات الفدية؟

أ. إجراء نَسْخ احتياطي منتظم، وتجنُّب المرفقات المشبوهة

ب. فتح المرفقات من أيّ بريد وارد

ج. تجاهل النَّسْخ الاحتياطي للملفات

د. تثبيت أيّ برنامج مجاني متاح على الإنترنت

إجابات الأسئلة التفاعلية

01 **إجابة السؤال التفاعلي الأول**

ب. تغيير كلمة المرور فورًا من جهاز آمِن

02 **إجابة السؤال التفاعلي الثاني**

ب. استخدام VPN وتجنّب إدخال بيانات حساسة

03 **إجابة السؤال التفاعلي الثالث**

ج. التحقُّق من هوية المرسِل قبل فتح المرفق، أو حذفه عند الشك

04 **إجابة السؤال التفاعلي الرابع**

د. استخدام بطاقات ذات حدود مالية منخفضة، والتأكد من أمان الموقع قبل الدفع

05 **إجابة السؤال التفاعلي الخامس**

ب. إقناع المستخدم بمشاركة معلوماته طوعًا عبر الخداع

05 **إجابة السؤال التفاعلي السادس**

أ. إجراء نسخ احتياطي منتظم، وتجنّب المرفقات المشبوهة

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

16555 - 40466798 - 51045944

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