الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

الشريحة المستهدفة

ذوو الإعاقة البصرية

كُتَيّب المدرّب

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

الشريحة المُستهدَفة

ذوو الإعاقة البصرية

كُتَيّب المُدَرّب

الموضوع	رقم الصفحـة
تمهيد	6
المبادرة الوطنية للسلامة الرقمية	7
المحور الأول: التهديدات السيبرانية الشائعة	13
التهديدات السيبرانية الشائعة	14
التصيُّد الاحتيالي	15
علامات التصيد الاحتيالي	16
الهندسة الاجتماعية	17
البرمجيات الخبيثة	18
الفيروسات	19
برمجيات الفدية	20
برمجيات التجسُّس	21

الموضوع	رقم الصفحـة
استغلال القارئ الصوتي	22
الروابط المخفية في Text-to-Speech	23
محاكاة الأصوات Voice Cloning	24
السؤال التفاعلي الأول	25
المحور الثاني: آليات الوقاية والسلامة الرقمية	26
مفهوم السلامة الرقمية	27
تأمين الأجهزة	28
التحديثات الأمنية المنتظمة	29
إدارة كلمات المرور	30
المصادقة الثنائية (2FA)	31
حماية الحسابات البنكية	32

الموضوع	رقم الصفحـة
آلية التّعامُل مع حوادث الخَرق	33
إعدادات الخصوصية	34
النسخ الاحتياطي للبيانات	35
شبكات Wi-Fi العامة	36
الوقاية من استغلال القارئ الصوتي	37
فحص الروابط قبل فتحها	38
التعامل مع الرسائل والمكالمات المجهولة	39
السؤال التفاعلي الثاني	40
السؤال التفاعلي الثالث	41
إجابات الأسئلة التفاعلية	42

تمهيد

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

تم تصميم هذا الكُتَيّب بهدف توعية ذوي الإعاقة البصرية بمبادئ السلامة الرقمية، وأفضل الممارسات التي تساعدهم على تفادي المخاطر السيبرانية؛ حيث يهدف هذا الكُتَيِّب إلى تعزيز وعيهم بأبرز هذه التهديدات؛ مثل التصيّد الاحتيالي، واستغلال القارئ الصوتي، والبرمجيات الخبيثة، واستنساخ الصوت، وذلك بطريقة مبسَّطة تتناسب مع احتياجاتهم اليومية واعتمادهم على التقنيات المساعدة.

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

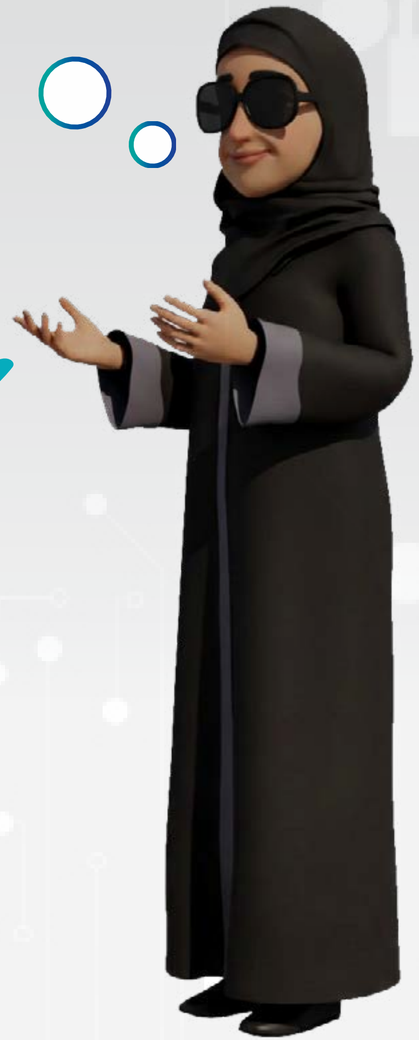
المبادرة الوطنيّة للسلامة الرقميّة

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 المُستهدَفة بالمبادرة

تستهدف المبادرة مختلف شرائح المجتمع، مع تركيزها على الفئات التالية:

01 السنة الأولى

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

02 السنة الثانية

الدبلوماسيون

الإعلاميون

الجمهور العام

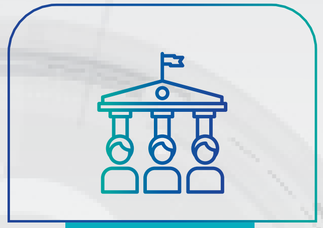
المرأة (العنف الرقمي ضد المرأة)

العاملون في المجال الصحي

المؤسسات العقابية والنيابة والمؤسسات الإصلاحية

الرياضيون

03 السنة الثالثة



العاملون في وزارتي الدفاع والداخلية

العاملون في قطاع الطاقة

ذوو الاحتياجات الخاصة

العاملون في قطاع التعليم

اليافعون والشباب

الجمهور العام

أدوات التوعية

تعتمد المبادرة على أدوات توعية متنوّعة ومتكاملة، تشمل ما يلي:

دليل السلامة الرقمية

كُتيّبات توعية مطبوعة

شرائح العرض (للمُدرّبين)

فيديوهات التوعية (أنيميشن)

فيديوهات التوعية (تمثيلية)

خَـلّك وَاعي
وَعْيك دِرْعك

الألعاب السيبرانية

أدوات التوعية

بوابة التوعية السيبرانية

الروبوت التفاعلي

وِرَش التوعية

المحور الأول

التهديدات السيبرانية الشائعة

التهديدات السيبرانية الشائعة

هي محاولات لإلحاق الضَّرر بالمستخدِم أو الجهاز أو البيانات، وتُشكِّل خطرًا حقيقيًّا على كلّ مَن يستخدم الإنترنت.

التصيّد الاحتيالي

أسلوب لخداع الضحية ودَفْعه للكشف عن معلومات حساسة، مثل كلمات المرور أو بيانات بطاقات الائتمان

البرمجيات الخبيثة

قد تتسبَّب في تلف الجهاز أو سرقة الملفات المهمة أو تعطيل النظام بالكامل

الهندسة الاجتماعية

تعتمد على استغلال مشاعر الضحايا كالثقة أو الخوف للحصول على بياناتهم دون استخدام أدوات تقنية

هجمات الشبكات

مثل اختراق شبكة Wi-Fi، تُتيح للمهاجمين التجسُّس على المستخدِم

البرامج المُزيَّفة

قد تُقنع المستخدم بتحميلها، لتبدأ بعدها بسرقة بياناته

التصيُّد الاحتيالي

الهجمات القائمة على خداع المستخدِم تعتمد على خَلْق شعور بالثقة للحصول على بيانات حساسة.

Phishing

رسائل بريدية تبدو رسمية، لكنّها تهدف لسرقة كلمات المرور أو البيانات البنكية

Vishing

مكالمات هاتفية احتيالية

Smishing

رسائل نصية أو تطبيقات مراسلة تحتوي على روابط ضارَّة أو برمجيات خبيثة

علامات التصيد الاحتيالي

يمكن التعرُّف على الرسائل المُزيَّفة من خلال ملاحظة بعض العلامات عن طريق القارئ الصوتي.

- وجود أخطاء لغوية أو إملائية في الرسالة
- عنوان البريد الإلكتروني لا يتطابق مع العنوان الرسمي للمؤسسة
- الروابط تبدو غريبة أو غير مألوفة
- الرسالة تطلب معلومات شخصية حساسة بشكل مباشر
- وجود تهديد أو استعجال لاتخاذ إجراء فوري، مثل «سيُغلَق حسابك خلال 24 ساعة»

الهندسة الاجتماعية

الهندسة الاجتماعية تعتمد على استغلال المشاعر البشرية، بدلًا من استخدام أدوات تقنية مُعقَّدة.

يعتمد على جَمْع معلومات عن المستخدِم من مواقع التواصل الاجتماعي

يستغل بعض المشاعر؛ مثل: الخوف، أو التعاطف، أو الحرج

تُعدّ من أخطر الوسائل؛ لأنها لا تحتاج مهارات تقنية، بل تعتمد على سلوك الضحية

يستخدم المهاجم أسلوب الإقناع والتلاعب النفسي للحصول على معلوماتك

قد يتظاهر بأنه مُوظَّف دعم فني، أو صديق، أو مسؤول

البرمجيات الخبيثة

الفيروسات
برمجيات ضارّة تُخرّب نظام التشغيل، أو تسرق البيانات دون عِلْم المستخدم

ديدان الحاسوب
هي برمجيات خبيثة تُشبه الفيروسات، لكنَّها أكثر خطورة بسبب قدرتها على الانتشار التلقائي

البرمجيات الخبيثة هي أخطر أدوات المهاجمين، وتستهدف كلًّا مِن المستخدمين وأنظمة التشغيل.

حصان طروادة
برمجيات تبدو طبيعية، لكنَّها تُؤدّي لاختراق الجهاز أو تعطيل وظائفه

برمجيات الفدية
برمجيَّات تقوم بتشفير الملفات، والمُطالَبة بفدية مقابل فكّ التشفير

برمجيات التجسُّس
مراقبة نشاط المستخدِم وسرقة المعلومات الشخصية

الفيروسات

الفيروس هو بَرْمجية ضارَّة تدخل إلى جهازك وتُغيِّر طريقة عمله، أو تُتْلِف البيانات الموجودة عليه.

يُرفَق الفيروس غالبًا مع ملفات تبدو طبيعية مثل الصور أو المستندات

يبدأ الفيروس بالانتشار عند فتح الملف أو تشغيله

بعض الفيروسات تتسبَّب في حذف الملفات أو تعطيل نظام التشغيل بالكامل

ينتقل الفيروس من جهاز إلى آخر عبر الإنترنت أو وسائط مثل USB

تفعيل برامج مكافحة الفيروسات المُحدّثة باستمرار يُسهم في الحماية من الفيروسات

برمجيات الفدية

برمجيات الفدية هي أحد أخطر أنواع الهجمات؛ حيث يتم تشفير الملفات، ثم يُطلَب دَفْع مبلغ مالي لفكّ التشفير.

تُرسَل عادةً عبر رسائل بريد إلكتروني تحتوي على مرفقات مُزيَّفة

المُهاجِم يطلب فدية مالية مقابل استعادة الملفات

بعد الإصابة، تُغلَق الملفات أو النظام بالكامل

الحل الأفضل: النَّسخ الاحتياطي المنتظم، وعدم فتح المرفقات المشبوهة

حتى عند الدفع، لا يوجد ضمان لاسترجاع الملفات

برمجيات التجسُّس

تعمل هذه البرامج في الخفاء وتقوم بتسجيل كل ما تفعله على الجهاز، بما في ذلك ضغطات لوحة المفاتيح.

تُرسِل معلوماتك للمهاجم، بما في ذلك كلمات المرور ورسائل البريد

قد تراقِب الكاميرا أو الميكروفون دون إذنك

يمكن أن تُبطِّئ الجهاز وتجعله يتصرّف بغرابة

من الصعب ملاحظتها دون برنامج متخصّص

استخدم جدار حماية (Firewall) ومضاد فيروسات قوي يساعد على الحماية منها

استغلال القارئ الصوتي

اعتماد أيّ مُستخدِم على أدوات الصوت للتفاعل مع الأجهزة يمكن أن يُستغَلّ مِن قِبَل المهاجمين:

- رسائل أو صفحات يَصْعُب تمييزها صوتيًّا عن المحتوى الرسمي
- إشعارات صوتية مُزيَّفة تُقرَأ على أنها حقيقية
- روابط خبيثة تظهر آمِنَة عند القراءة الصوتية
- تطبيقات مُزيَّفة تتظاهر بأنها أدوات مساعدة

الروابط المخفية في Text-to-Speech

تقنيات تحويل النص إلى كلام قد تُستخدَم لإخفاء روابط ضارة:

- نصوص تُقرَأ على أنها آمِنَة، لكنّها تحتوي روابط خبيثة
- رسائل بريدية أو نصية يمكن أن تُستغَلّ بهذه الطريقة
- التحقُّق الصوتي وحده قد لا يكشف المخاطر

محاكاة الأصوات Voice Cloning

التقنيات الحديثة تُتيح تقليد الأصوات لإقناع المستخدِم بتنفيذ إجراءات ضارة:

- محاكاة صوت شخص موثوق مثل زميل أو موظف بنك
- خداع المستخدِم لإجراء تحويلات مالية أو مشاركة بيانات سرية
- صعوبة اكتشاف الاحتيال صوتيًّا

السؤال التفاعلي الأول

ما أهم إجراء عند التعامل مع رسائل البريد الإلكتروني البنكي الصوتية؟

أ. التحقُّق من المصدر، استخدام أدوات قراءة آمِنَة، ومتابعة النشاط المالي

ب. قراءة الرسائل فورًا، والرد عليها بسرعة

ج. تجاهل كل الرسائل الصوتية

د. مشاركة رمز التحقق مع أيّ شخص للتأكيد

المحور الثاني

آليات الوقاية والسلامة الرقمية

مفهوم السلامة الرقمية

هي ممارسات تساعد على استخدام الإنترنت والتكنولوجيا بطريقة آمِنَة.

تساعد على حماية المعلومات الشخصية من السرقة أو الاستخدام غير المصرَّح به

تُمكِّن المستخدِم من التفاعل الآمِن مع الإنترنت والتطبيقات التكنولوجية

تشمل استخدام أدوات الأمان؛ مثل: كلمات المرور والمصادقة الثنائية

تُعزِّز ثقة المستخدِم في استخدام الأدوات والخدمات الإلكترونية المختلفة

تضمن بيئة رقمية أكثر أمانًا لذوي الإعاقة البصرية؛ خصوصًا عند الاعتماد على قارئات الشاشة

تأمين الأجهزة

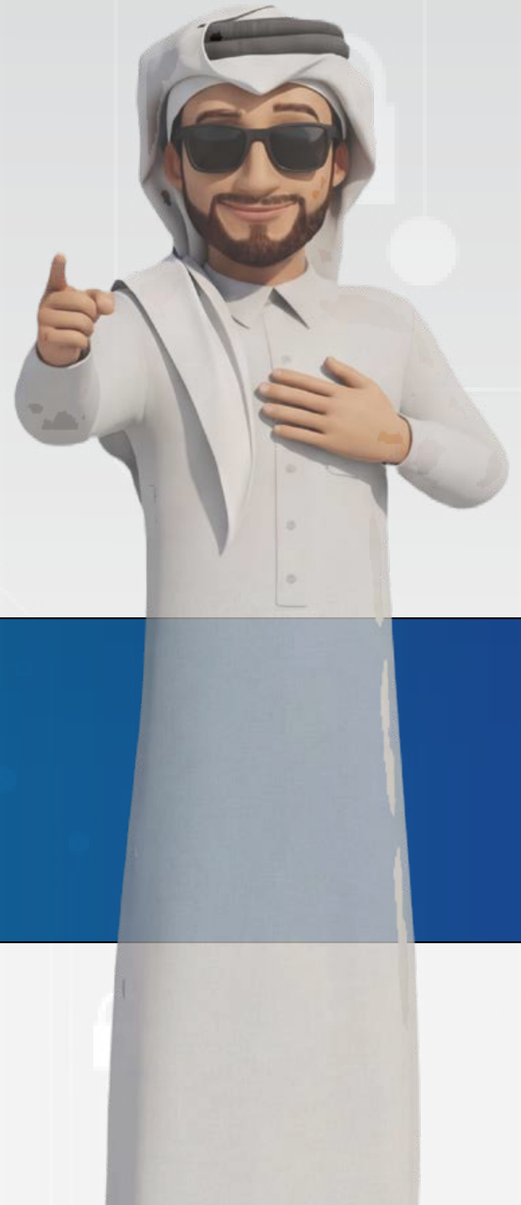
تأمين الأجهزة الذكية يُقلِّل مخاطر الوصول غير المصرَّح به، خصوصًا عند الاعتماد على الصوت:

- تفعيل قَفْل الشاشة بالصوت
- التحقُّق البيومتري (بصمة أو التعرُّف على الوجه) متوافق مع أدوات الصوت
- تحديث النظام والتطبيقات بانتظام
- تعطيل الميزات غير الضرورية التي قد تكشف البيانات

التحديثات المنتظمة

الحفاظ على تحديث النظام والتطبيقات يُقلّل من استغلال الثغرات:

- تفعيل التحديث التلقائي للنظام والتطبيقات
- تحديث قارئات الشاشة لضمان توافق الميزات الجديدة
- إزالة التطبيقات غير المستخدَمة أو القديمة
- مراجعة إعدادات الأمان بعد كلّ تحديث
- متابعة تنبيهات الأمان بشكل دوري



إدارة كلمات المرور

استخدام جمل طويلة تحتوي على كلمات وأرقام ورموز يمكن نُطْقها بسهولة

عدم استخدام الكلمات الشائعة أو المعلومات الشخصية القابلة للتخمين

تغيير كلمة المرور بشكلٍ دوريّ لضمان الأمان

استخدام كلمات مرور مختلفة لكلّ حساب

الاعتماد على القارئ الصوتي يتطلَّب كلمات مرور يمكن تذكُّرها بسهولة صوتيًّا، ولكن يَصْعُب تخمينها:

دَمْج كلمات المرور مع مدير كلمات مرور صوتي لتسهيل الإدخال

المصادقة الثنائية (2FA)

هي وسيلة أمان تُضيف خطوة ثانية لحماية الحسابات بعد إدخال كلمة المرور.

تطلب من المستخدِم إدخال رمز تحقُّق يتم إرساله إلى الهاتف أو البريد بعد إدخال كلمة المرور

تمنع المخترق من الدخول حتى لو كان يَعْرف كلمة المرور؛ لأنه لا يملك رمز التحقُّق الثاني

متاحة في معظم التطبيقات، مثل Gmail Facebook Xg

تساعد بشكل خاص في حماية الحسابات البنكية والبريدية من الهجمات السيبرانية

حماية الحسابات البنكية

تفعيل المصادقة الثنائية لجميع الحسابات البنكية

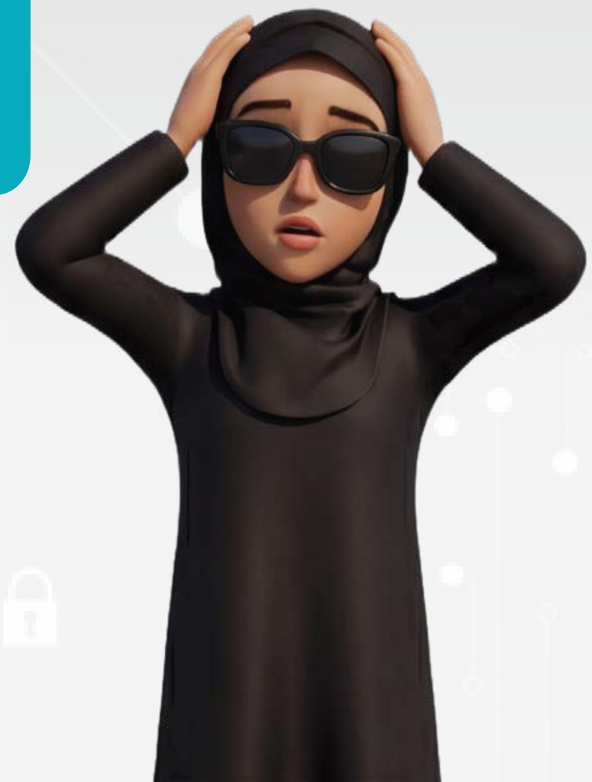
تجنُّب مشاركة بيانات الحساب عبر المكالمات أو الرسائل

التحقُّق الصوتي وحده لا يكفي، ويجب اعتماد إجراءات إضافية:

مُتابعة العمليات المالية بانتظام عبر تطبيقات آمِنَة

التواصل مباشرة مع البنك عند وجود نشاط مريب

استخدام أدوات قراءة رسائل البريد البنكي الصوتية للتحقُّق من صحة المحتوى



آلية التّعامُل مع حوادث الخَرق

توجد خطوات مُهمَّة للتَّعامُل مع حالات الخرق:

تغيير كلمات المرور

تغيير جميع كلمات المرور لحساباتك المُختَرقة وغير المُختَرقة فورًا

إبلاغ الجهات المعنية

الاتصال بالبنك أو المنصة المُختَرَقة، والإبلاغ عن الحادث

تحديث الأنظمة والبرامج

التأكُّد من أن نظام التشغيل وبرامج الحماية مُحدَّثة؛ لتجنُّب الثغرات الأمنية

استخدام برامج مُكافَحة الفيروسات

فَحْص الأجهزة باستخدام برامج موثوقة لإزالة أيّ برمجيات خبيثة

مُراقَبة الحسابات المالية بشكلٍ دوريّ، لملاحظة أيّ تغيير

هذه الخطوات تُساعد في تقليل الضَّرر، واستعادة الأمان بَعْد الخرق.

إعدادات الخصوصية

تقييد الوصول للبيانات يُقلِّل خطر التجسُّس أو الاستغلال.

- ضبط الأذونات للموقع، الميكروفون، والكاميرا للتطبيقات الموثوقة فقط
- مراجعة إعدادات الخصوصية بشكل دوري
- تعطيل الخدمات غير الضرورية التي تجمع بيانات حساسة
- مراقبة نشاط التطبيقات الصوتية بشكلٍ منتظم
- الاعتماد على إعدادات الخصوصية المدمجة في النظام

النسخ الاحتياطي للبيانات

النَّسْخ الاحتياطي يحمي البيانات من الضياع أو الهجمات.

- حفظ نُسْخة مُشفَّرة من البيانات المهمة
- التحقُّق من إمكانية الوصول إلى النّسخ الاحتياطية عند الحاجة
- تحديث النُّسَخ الاحتياطية بانتظام
- استخدام النَّسْخ الاحتياطي السحابي الموثوق
- تخزين كلمات المرور وبيانات الحسابات بشكل آمِن

شبكات Wi-Fi العامة

استخدام الشبكات المفتوحة قد يُعرِّض البيانات للسرقة.

يمكن للمخترق المتصل بنفس الشبكة التنصّت على البيانات المرسَلة

غالبًا ما تكون هذه الشبكات غير مُشفَّرة، مما يسمح برؤية كل البيانات

يُفضَّل استخدام VPN عند الاضطرار لاستخدام شبكة عامة؛ لحماية الاتصال

بعض المهاجمين يستخدمون شبكات باسم يشبه أسماء الفنادق أو المقاهي لجَذْب الضحايا

لا يُنْصَح بإجراء معاملات مالية أو إدخال كلمات مرور في أثناء الاتصال بالشبكات العامة المفتوحة

الوقاية من استغلال القارئ الصوتي

الاعتماد على القارئ الصوتي يتطلب اتخاذ إجراءات إضافية لتجنُّب استغلال المهاجمين لهذه الخاصية.

التأكُّد من مصدر الرسائل والمواقع قبل التعامل معها

استخدام أدوات تحقُّق إضافية قبل النقر على أيّ رابط أو فتح أيّ محتوى جديد

تحديث برامج القارئ الصوتي بانتظام لضمان قراءة المحتوى بشكلٍ آمِن

الاعتماد على تطبيقات أمان متوافقة مع قارئ الصوت لفَحْص الروابط والملفات

فحص الروابط قبل فتحها

ذوو الإعاقة البصرية أكثر عُرْضَة لروابط خبيثة بسبب اعتمادهم على القارئ الصوتي.

- استخدام أدوات قراءة URL صوتيًّا للتأكُّد من الوجهة
- تجنُّب النقر على روابط مشبوهة أو مختصرة
- المقارنة مع النطاق الرسمي للموقع قبل أيّ إدخال بيانات
- التحقُّق عبر تطبيقات أمان متوافقة مع القارئ الصوتي
- تحديث أدوات الفحص بانتظام لضمان اكتشاف الروابط الجديدة

التعامل مع الرسائل والمكالمات المجهولة

الاعتماد على الصوت يجعل التحقُّق من المرسِل أصعب، لذلك يجب الحذر.

- تجاهل الرسائل والمكالمات غير الموثوقة
- التحقُّق دائمًا من هوية المرسِل عبر قنوات رسمية
- عدم فتح أيّ روابط أو ملفات من مُرسِل مجهول
- استخدام أدوات فَحْص الروابط والملفات صوتيًّا
- توثيق أيّ محاولة احتيال للإبلاغ عنها

السؤال التفاعلي الثاني

كيف تساهم التحديثات الأمنية المنتظمة في حماية الأجهزة؟

أ. لتحسين واجهة التطبيقات

ب. لتسهيل تحميل التطبيقات الجديدة

ج. لإغلاق الثغرات المعروفة، ومنع استغلالها من قبل المخترقين

د. لتخزين كلمات المرور على الهاتف

السؤال التفاعلي الثالث

ما أهم نقطة عند التعامل مع رسائل البريد الإلكتروني البنكي الصوتية؟

أ. التحقُّق من المصدر، استخدام أدوات قراءة آمِنَة، ومتابعة النشاط المالي

ب. قراءة الرسائل فورًا والرد عليها بسرعة

ج. تجاهل كل الرسائل الصوتية

د. مشاركة رمز التحقُّق مع أيّ شخص للتأكيد

إجابات الأسئلة التفاعلية

01

إجابة السؤال التفاعلي الأول

ب. لإضافة طبقة حماية إضافية تمنع الوصول غير المصرَّح به حتى إذا تم كشف كلمة المرور

02

إجابة السؤال التفاعلي الثاني

ج. لإغلاق الثغرات المعروفة، ومنع استغلالها مِن قِبَل المخترقين

03

إجابة السؤال التفاعلي الثالث

أ. التحقق من المصدر، استخدام أدوات قراءة آمِنَة، ومتابعة النشاط المالي

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