الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

التعريف بالهجمات السيبرانية

الشريحة المستهدفة
الإعلاميون

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

التعريف بالهجمات السيبرانية

الشريحة المُستهدَفة

الإعلاميون

كُتيّب المدرّب

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

حقوق الملكية الفكرية

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

16555
00974 404 66 798
00974 510 45 944
academy@ncsa.gov.qa

تمهيد

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

تم تصميم هذا الكُتَيِّب بهدف توعية الإعلاميين بمبادئ السلامة الرقمية، وأفضل الممارسات التي تساعدهم على تفادي المخاطر السيبرانية؛ حيث يهدف هذا الكُتَيِّب إلى تعزيز وعيهم بأبرز التهديدات السيبرانية التي قد يتعرَّضون لها في أثناء عملهم؛ مثل: التصيّد الاحتيالي، برمجيات الفدية، الفيروسات، الهندسة الاجتماعية، التزييف العميق، وسرقة الهوية الرقمية.

كما يُقدِّم الكُتَيّب أفضل الممارسات والإجراءات الوقائية لحماية الأجهزة، وتأمين الحسابات، والتعامل السريع مع مؤشرات الاختراق.

وتُعدّ هذه الجهود جزءًا 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.

وتعمل على نَشْر الوعي بالسلامة الرقمية والاستخدام الآمِن لشبكة الإنترنت والتطبيقات التكنولوجية المختلفة، وتوضيح المخاطر المحتمَلة؛ وذلك بهدف بناء مجتمع آمِن سيبرانيًّا ومُتمكِّن تكنولوجيًّا.

الشرائح المستهدَفة

تستهدف المبادرة مختلف شرائح المجتمع، مع تركيزها في السنة الأولى على الشرائح التالية:

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

الفصل الأول

أساسيات السلامة الرقمية

مفهوم السلامة الرقمية

السلامة الرقمية هي مجموعة الإجراءات والممارسات التي تُمكِّن الإعلاميين من حماية بياناتهم الشخصية والمهنية عند استخدام الأجهزة والإنترنت.

السمات الأساسية للسلامة الرقمية

توفير الحماية للأجهزة من الاختراق والبرمجيات الخبيثة

الحفاظ على سرّية مصادر المعلومات الصحفية

ضمان سلامة المراسلات أثناء التغطيات والتحقيقات

مَنْع الوصول غير المُصرَّح به للبيانات

تعزيز الثقة بين الصحفي والجمهور من خلال بيئة رقمية آمِنَة

التهديدات الرقمية الشائعة

يتعرَّض الإعلاميون لأنواعٍ مختلفةٍ من الهجمات الرقمية التي تَهْدف للسرقة أو التشويه أو التضليل.

أهم التهديدات

- التصيّد الاحتيالي عبر البريد الإلكتروني والرسائل النصية
- البرمجيات الخبيثة وبرامج الفدية
- الهندسة الاجتماعية المبنية على الخداع
- التنصّت على الاتصالات خلال استخدام شبكات عامة
- التزييف العميق لإنتاج فيديوهات أو تسجيلات مُضلّلة

كلمات المرور

كلمات المرور القوية هي خط الدفاع الأول أمام أيّ محاولة اختراق.

خصائص كلمات المرور القوية

أمان البريد الإلكتروني

البريد الإلكتروني أداة أساسية للإعلامي، لكنّه الأكثر استهدافًا.

ممارسات الأمان في البريد

أمان شبكات التواصل الاجتماعي

الحسابات الإعلامية على منصات التواصل الاجتماعي تُعدّ من أهمّ الأهداف للمخترقين.

نصائح لحماية الحسابات

- تحديد مَن يستطيع رؤية المنشورات أو التعليق
- مراجعة التطبيقات المربوطة بالحساب
- تفعيل إشعارات تسجيل الدخول
- الانتباه للرسائل المشبوهة
- استخدام كلمات مرور مختلفة لكل حساب

أمان الشبكات العامة

شبكات Wi-Fi العامة خطيرة على الإعلاميين، خاصةً في أثناء التغطيات.

ممارسات آمِنَة

- استخدام VPN لتشفير الاتصال
- تجنّب إدخال كلمات مرور أو بيانات مالية
- تعطيل خاصية الاتصال التلقائي بالشبكات
- التحقّق من أن الموقع يبدأ بـ https.

حماية المصادر الصحفية

المصادر الصحفية هي الأكثر حساسية، ويجب التعامل معها بسرية تامة.

طرق الحماية

- تشفير المستندات والملفات المشتركة
- استخدام وسائل تَراسُل آمِنَة
- فَصْل بيانات المصادر عن الملفات الشخصية
- الوعي بمبادئ السلامة الرقمية

مؤشرات تعرُّض الجهاز للاختراق

- بُطْء غير معتاد في الجهاز
- تغييرات مفاجئة في الملفات أو التطبيقات
- ظهور نوافذ أو إعلانات منبثقة
- إشعارات تسجيل دخول من أماكن مجهولة
- إرسال رسائل من البريد دون عِلْمك

الإجراءات الأولية عند الاشتباه بالاختراق

عند ملاحظة أيّ نشاط مشبوه يجب التعامل معه بسرعة.

الخطوات الفورية

فَصْل الجهاز عن الإنترنت مباشرة

تغيير كلمات المرور الأساسية من جهاز آخر آمِن

إبلاغ فريق الدعم التقني أو إدارة المؤسسة الإعلامية

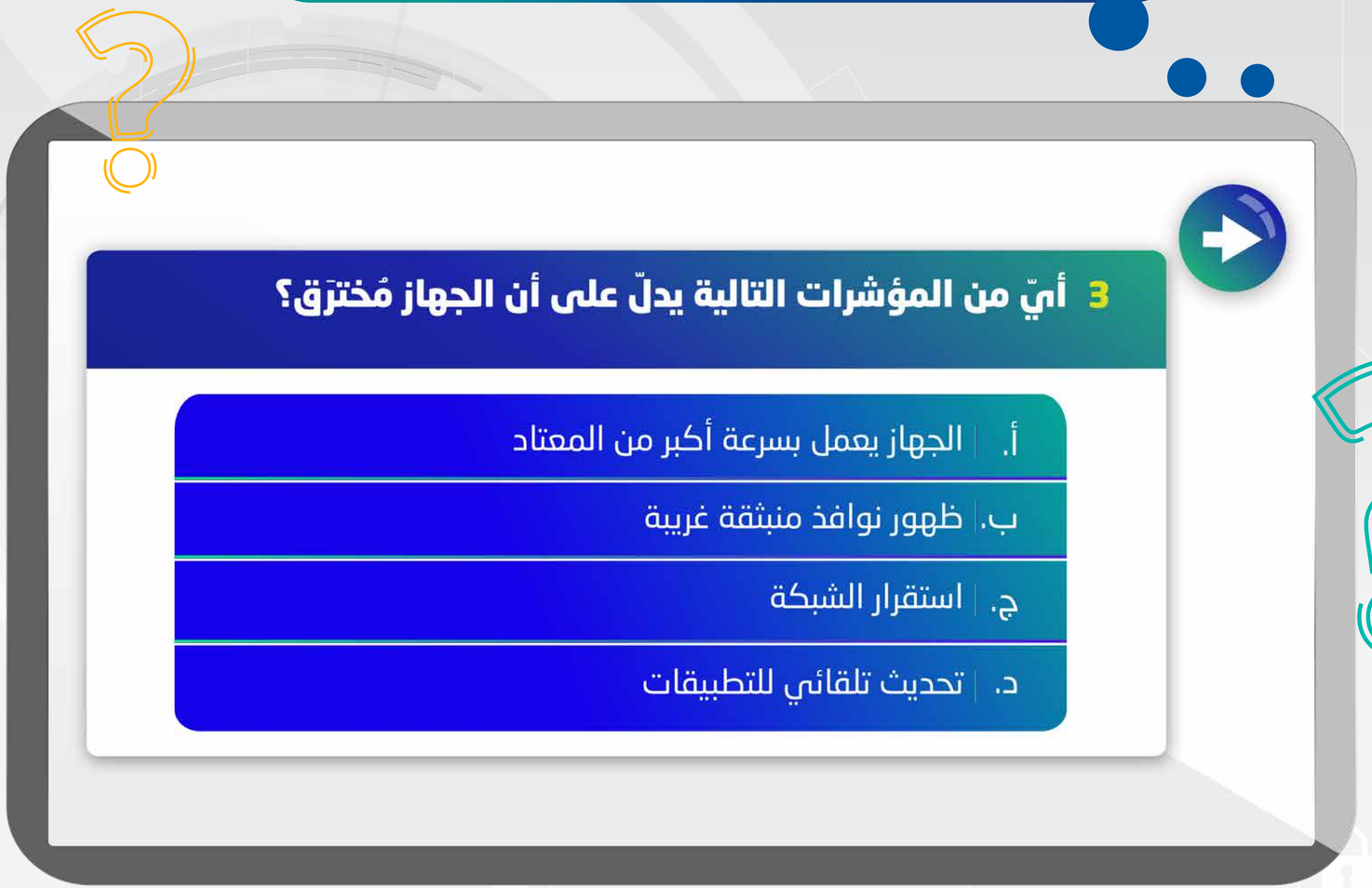
توثيق الحادث (صور، وقت، رسائل)

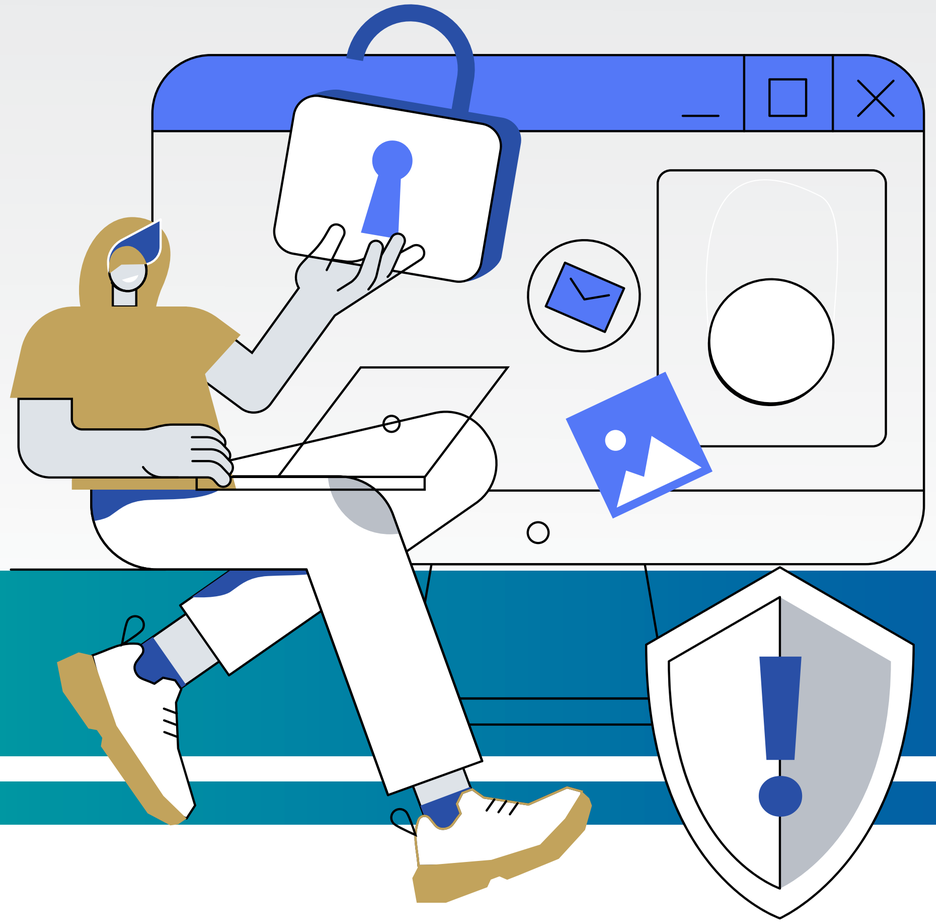
إجراء فحص شامل للجهاز

السؤال التفاعلي الأول

السؤال التفاعلي الثاني

السؤال التفاعلي الثالث





الفصل الثاني

التهديدات والهجمات السيبرانية

البرمجيات الخبيثة (Malware)

يقوم المهاجمون بإرسال البرمجيات الخبيثة إلى الأجهزة بهدف إلحاق الضرر، أو سرقة البيانات، أو التحكُّم في المحتويات.

السمـــات الرئيسيـــة

- تنتقل عبر المرفقات أو الروابط المشبوهة
- قد تُخْفِي نفسها داخل برامج أو تطبيقات ظاهرها سليم
- تتنوّع بين فيروسات، ديدان، برمجيات فدية، أو برمجيات تجسُّس

- تؤدي إلى فقدان السيطرة على الأجهزة أو البيانات
- تُستخدم أحيانًا للتجسُّس على عمل الصحفيين

طرق الوقاية

- تثبيت برامج مكافحة الفيروسات، وتحديثها بانتظام
- تجنُّب تحميل البرامج من مواقع غير موثوقة
- عدم الضغط على الروابط أو المرفقات المجهولة
- تشغيل جدار الحماية لصدّ الهجمات
- إجراء فَحْص دوري للجهاز للتأكُّد من خلوّه من البرمجيات الضارَّة

الفيروسات

الفيروس هو برمجيَّة ضارَّة تَدخل إلى الجهاز وتُغيِّر طريقة عمله، أو تُتْلِف البيانات الموجودة عليه.

السمات الرئيسية

- يُرفَق غالبًا مع ملفات تبدو طبيعية مثل الصور أو المستندات
- يبدأ الفيروس بالانتشار عند فَتْح الملف أو تشغيله
- بعض الفيروسات تتسبَّب في حذف الملفات أو تعطيل النظام بالكامل
- ينتقل من جهاز إلى آخر عبر الإنترنت أو وسائط مثل USB

طرق الوقاية

- استخدام برامج مكافحة الفيروسات المُحدّثة باستمرار
- عدم فَتْح الملفات مجهولة المصدر
- فحص وسائط التخزين (USB) قبل تشغيلها
- تحديث أنظمة التشغيل والبرامج لإغلاق الثغرات الأمنية

برمجيات الفدية (Ransomware)

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

السمـــات الرئيسيـــة

- تُرسَل عادة عبر رسائل بريد إلكتروني تحتوي على مرفقات مزيَّفة
- المهاجم يطلب فدية غالبًا بعُمْلة رقمية مثل البيتكوين
- بعد الإصابة، تُغْلِق الملفات أو النظام بالكامل
- حتى عند الدفع، لا يُوجَد ضمان لاسترجاع الملفات

طرق الوقاية

النَّسخ الاحتياطي المنتظِم للملفات المهمة

استخدام برامج أمنية متخصّصة في منع هجمات الفدية

تجنّب فتح المرفقات من مصادر مجهولة

تحديث النظام والتطبيقات باستمرار لسدّ الثغرات

أحصنة طروادة (Trojans)

هو نوع من الفيروسات التي تُصيب الحواسيب وأجهزة الهواتف المحمولة، ويكون على شكل ملف يُرفِق نفسه مع أحد البرامج الموجودة على الإنترنت.

السمات الرئيسية

- تفتح بابًا خلفيًّا يُتيح للمهاجم التحكم بالجهاز
- تُقدَّم كأداة لتحرير الفيديو أو إدارة البريد
- قد تُستخدَم لسرقة كلمات مرور الحسابات

طرق الوقاية

استخدام برامج كشف التسلل ومكافحة الفيروسات

تحميل البرامج من المواقع الرسمية فقط

عدم تثبيت أيّ برنامج غير معروف أو مشكوك فيه

مراقبة نشاط الجهاز والبرامج المثبّتة بانتظام

التصيد الاحتيالي

التصيّد الاحتيالي هو محاولة خداع من خلال رسائل أو مواقع تبدو كأنها حقيقية، لكنَّها مُصمَّمة لسرقة المعلومات.

سمات رسائل التصيد الاحتيالي

غالبًا ما تأتي على شَكْل رسائل بريد إلكتروني أو رسائل نصية مُزيَّفة

تَطلب من المستخدم إدخال بيانات حسَّاسة مثل كلمات المرور أو أرقام البطاقات البنكية

تَستخدم لغةً مستعجلة مثل "حسابك موقوف، تصرَّف الآن!"؛ لتحفيزك على التفاعل دون تفكير

تُقلّد تصميم وشعارات مؤسسات معروفة لتبدو كأنها شرعية

الهدف الرئيسي هو سرقة المعلومات لاستغلالها ماليًّا أو للابتزاز

طرق الوقاية

التأكـد مـن عناويـن البريـد والروابـط قبـل النقـر عليهـا

عـدم مشـاركة البيانـات الشـخصية عبـر الرسـائل المشـبوهة

استخدام خاصية التحقق بخطوتين للحسابات

الهندسة الاجتماعية

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

السمات الرئيسية

- يَستخدم المهاجم أسلوب الإقناع والتلاعُب النفسي للحصول على المعلومات
- قد يتظاهر بأنه مُوظَّف دعم فني، أو صديق، أو مسؤول
- يستغلّ مشاعر مثل الخوف، أو التعاطف، أو الحَرَج لدَفْعك للتجاوب
- يعتمد على جَمْع معلومات من مواقع التواصل لجَعْل المستخدِم يثق به
- تُعدّ من أخطر الوسائل؛ لأنها لا تحتاج مهارات تقنية، بل تعتمد على سلوك الضحية

طرق الوقاية

- التحقُّق من هوية المتصل أو المُرسِل قبل مشاركة أيّ معلومة
- تجنّب مشاركة تفاصيل حساسة مع أشخاص غير موثوقين
- توعية الفريق الصحفي بخطورة هذا الأسلوب
- اعتماد بروتوكولات واضحة للتحقُّق قبل الاستجابة لأيّ طلب

التزييف العميق (Deepfake)

التزييف العميق هو استخدام الذكاء الاصطناعي لإنتاج محتوى مزيَّف بشكل قريب للواقع.

السمات الرئيسية

- إنشاء فيديوهات أو تسجيلات صوتية تُقلِّد شخصيات عامة
- صعوبة التمييز بين الحقيقي والمزيَّف
- تهديد مباشر لسُمعة الصحفي أو المؤسسة الإعلامية
- يُستخدَم لنَشْر أخبار مُضلّلة تَستهدف الرأي العام

طرق كشف المحتوى المزيف

ملاحظة العلامات غير الطبيعية في الحركات أو الأصوات

استخدام أدوات كشف التزييف العميق

التحقّق من البيانات الوصفية (Metadata) للملفات الرقمية

الاعتماد على مصادر متعدّدة قبل نَشْر أي محتوى مرئي أو صوتي

سرقة الهوية الرقمية

تحدث سرقة الهُويَّة الرقمية عندما يقوم شخص غير مصرَّح له بالوصول إلى معلومات هُويَّة شخص آخر على الإنترنت، واستخدامها بشكلٍ غير قانوني؛ لتحقيق مكاسب شخصية أو مالية.

أمثلة على البيانات المسروقة

طرق الوقاية

- تغيير كلمات المرور الأساسية بشكل دوري
- تجنّب مشاركة تفاصيل حساسة على الإنترنت
- التأكد من عناوين البريد والروابط قبل النقر عليها
- استخدام برامج كشف التسلل
- استخدام برامج مكافحة الفيروسات وتحديثها باستمرار
- عدم مشاركة كلمة المرور مع أيّ شخص

السؤال التفاعلي الرابع

السؤال التفاعلي الخامس

السؤال التفاعلي السادس

إجابات الأسئلة التفاعلية

01	**إجابة السؤال التفاعلي الأول** ب. تغيير كلمة المرور فورًا
02	**إجابة السؤال التفاعلي الثاني** ج. استخدام VPN
03	**إجابة السؤال التفاعلي الثالث** ب. ظهور نوافذ منبثقة غريبة
04	**إجابة السؤال التفاعلي الرابع** ب. تشفير البيانات وطلب المال لفك التشفير
05	**إجابة السؤال التفاعلي الخامس** أ. الهندسة الاجتماعية
06	**إجابة السؤال التفاعلي السادس** د. النسخ الاحتياطي

قبل أن نختم يُرجَى التفضل بإدراج بياناتكم وتقييم الورشة، وعليه، يُرجَى مسح الرابط الآتي:

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency