الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

حماية الأجهزة والتحقق من مصادر المعلومات

الشريحة المستهدفة
الإعلاميون

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 السـلامة الرقمية

حماية الأجهزة والتحقق من مصادر المعلومات

الشريحة المستهدفة

الإعلاميون

كُتَيّب المُدَرّب


Email or username
****
Remember Me
Forgot Password?
LOGIN
REGISTER

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 - 40466798 - 51045944

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

الفهرس	رقم الصفحـة

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 حماية الأجهزة والتحقّق من مصادر المعلومات، وتزويدهم بأفضل الممارسات التي تُساعدهم على تأمين أجهزتهم وبياناتهم الشخصية والمهنية، وحمايتها من محاولات الاختراق أو الفقدان؛ من خلال التشفير، النسخ الاحتياطي، والمصادقة الثنائية.

كما يُركِّز الكُتَيِّب على تعزيز قدرة الإعلاميين على مُواجهة التضليل الرقمي عبر التحقُّق من الصور والفيديوهات، واكتشاف التزييف العميق، والتعامل مع الأخبار المُضلّلة.

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 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

الفصل الأول

حماية الأجهزة والمعلومات الشخصية والمهنية

حماية الحواسيب والهواتف

الأجهزة هي الأداة الأساسية للصحفي، وأيّ اختراق لها يعني تهديدًا مباشرًا للمعلومات والمصادر. لذلك يجب التعامل معها كخطّ الدفاع الأول.

خطوات الحماية

- قفل الجهاز باستخدام كلمة مرور قوية أو بصمة؛ لتقليل احتمالية الوصول غير المصرَّح به
- الحرص على تحديث نظام التشغيل والبرامج باستمرار؛ لتفادي استغلال الثغرات الأمنية
- تثبيت برنامج حماية (مكافح فيروسات + جدار حماية)، يمنع معظم محاولات الاختراق
- إيقاف البلوتوث وWi-Fi عند عدم الحاجة يُقلّل من فرص التسلل الخفي إلى الجهاز

كيف يُمكن أن يتعرَّض الهاتـف للاختـــراق؟

يحدث الاختراق عندما يتمكَّن شخص غير مصرَّح له من الدخول إلى الهاتف أو الوصول إلى محتوياته دون عِلْم صاحبه.

الطرق الشائعة لاختراق الهواتف

- تحميل تطبيقات مزيَّفة تحتوي على برمجيات خبيثة
- الضغط على روابط احتيالية داخل رسائل أو مواقع
- الاتصال بشبكات Wi-Fi غير آمِنَة
- مشاركة معلومات الدخول أو كلمات المرور مع الغرباء
- فقدان الهاتف بدون كلمة مرور

التحديثات الدورية للبرامج

التحديثات ليست مجرد تحسينات، بل غالبًا ما تحمل حلولًا لثغرات خطيرة قد يَستغلّها المهاجمون.

فوائد التحديثات

- ضَبْط التحديثات التلقائية يَحْمي من التأخير في تثبيت الإصلاحات الأمنية
- التطبيقات مثل برامج التحرير تحتاج تحديثات منتظمة لضمان استقرارها
- التأخُّر في التحديث قد يعني تَرْك باب مفتوح للمخترقين

التشفير وحماية المستندات

التشفير خطوة ضرورية في حماية البيانات فهو يُحافظ على سِرّية الملفات حتى لو سُرِقَت.

الميزات

تشفير كامل للقرص الصلب يمنع قراءة البيانات عند فقدان الجهاز

وَضْع كلمة مرور منفصلة على المستندات عالية الحساسية يزيد من مستوى الأمان

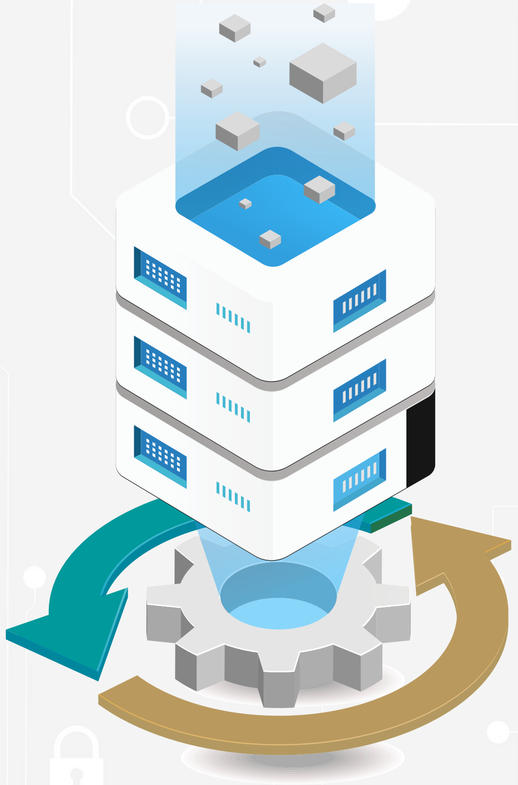
استخدام أدوات مثل BitLocker لتأمين الملفَّات الخاصة بالتحقيقات

النَّسْخ الاحتياطي للبيانات

فقدان الملفات قد يكون نتيجة هجوم أو عطل تقني، والنَّسخ الاحتياطي هو الضمان الوحيد لاستعادتها.

أهم الممارسات

- حفظ نسخة على التخزين السحابي لتسهيل الوصول من أيّ مكان
- الالتزام بجدول دَوري (أسبوعي أو شهري)، يضمن عدم ضياع التحديثات الجديدة للملفات
- إنشاء نسخة إضافية على قرص خارجي غير متَّصل بالإنترنت لتجنُّب التشفير ببرامج الفدية



المصادقة الثنائية (2FA)

إضافة طبقة ثانية من الحماية تجعل عملية الاختراق أكثر صعوبة.

الميزات

تعتمد على إدخال رمز يُرْسَل للهاتف أو يُولد عبر تطبيق خاص بعد إدخال كلمة المرور

تجعل المخترِق بحاجة للوصول إلى جهازك الشخصي، وليس مجرد كلمة المرور

متوافرة على أغلب المنصات والبريد الإلكتروني

أمان شبكات Wi-Fi الخاصة

الإنترنت هو بوابة الأجهزة للعالم الخارجي، وأيّ ضعف فيه قد يكون مدخلًا للهجوم.

خطوات التأمين

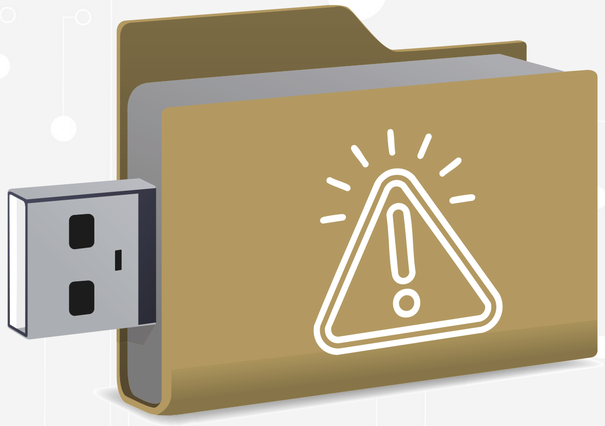
- تغيير كلمة المرور الافتراضية للشبكة يقطع الطريق أمام الاختراقات البسيطة
- تفعيل تشفير WPA2 أو WPA3 يُضيف مستوًى متقدّمًا من الحماية
- مراجعة الأجهزة المتصلة دوريًّا يكشف أيّ دخول غير مشروع

حماية وسائط التخزين

الأقراص الصلبة وذاكرات USB أدوات مُهمَّة، ويجب حماية البيانات المخزَّنة عليها.

طرق الحماية

- تشفير الملفات قبل نقلها على USB أو قرص خارجي يحافظ على سريتها
- فَحْص أيّ وسيط خارجي قبل فَتْحه يمنع انتقال الفيروسات للأجهزة
- عدم استخدام أقراص أو ذواكر مجهولة المصدر يَحُدّ من احتمال الإصابة بالبرمجيات الخبيثة



مؤشرات إصابة الجهاز بالاختراق

التعرُّف المبكّر على علامات الاختراق يُقلّل الخسائر.

أبرز المؤشرات

- بُطْء الجهاز المفاجئ رغم قلة البرامج قد يُشِير لوجود برمجية خبيثة تعمل بالخلفية
- ظهور ملفات غريبة أو اختفاء أخرى مُؤشّر واضح على نشاط غير طبيعي
- فتح التطبيقات أو الرسائل دون تدخُّل المستخدِم قد يدلّ على سيطرة خارجية

استعادة البيانات بعد الاختراق

في حال نجح الهجوم، هناك إجراءات تساعد على تقليل الأضرار.

الخطوات

- فصل الجهاز عن الإنترنت مباشرة لوقف تسرُّب البيانات
- استخدام النُّسَخ الاحتياطية لاستعادة الملفات بسرعة
- اللجوء لإعادة التهيئة(Format) ؛ إذا لم تنجح حلول الحماية

السؤال التفاعلي الأول

1- ما الطريقة الأكثر أمانًا للاحتفاظ بنُسْخة احتياطية من الملفات؟

أ. حفظها على القرص الخارجي غير المتصل بالإنترنت

ب. تركها على سطح المكتب

ج. تخزينها في ذاكرة USB دائمة التوصيل

د. إرسالها بالبريد الإلكتروني

السؤال التفاعلي الثاني

2- ما أبرز مؤشر على إصابة الجهاز ببرمجية خبيثة؟

- أ. ارتفاع حرارة الجهاز وبطؤه رغم قلة البرامج
- ب. زيادة سرعة الإنترنت فجأة
- ج. إغلاق التطبيقات بعد الانتهاء منها
- د. تثبيت تحديثات النظام تلقائيًّا

السؤال التفاعلي الثاني

3- ما الهدف الأساسي من المصادقة الثنائية؟

أ. تسريع تسجيل الدخول

ب. جعل الحساب يحتاج لخطوتين مختلفتين لتأكيد الدخول

ج. تخزين البيانات في السحابة

د. إلغاء كلمات المرور نهائيًّا

الفصل الثاني

التحقق من مصادر المعلومات ومكافحة الأخبار المُضلّلة

مفهوم الأخبار المُضلّلة

الأخبار المُضلّلة هي محتويات إعلامية يجري إنتاجها أو نَشْرها بقَصْد الخداع أو إثارة البلبلة أو التأثير على الجمهور. وقد تكون مكتوبة أو مصورة أو مسموعة.

السمات الرئيسية للأخبار المُضلّلة

- قد تكون مُلفَّقة بالكامل، ولا صلة لها بالواقع
- قد تُبنَى على وقائع حقيقية أُخرجت من سياقها
- كثيرًا ما تلجأ إلى المبالغة في الأرقام أو الأحداث
- غالبًا ما تُرْفَق بمصادر غامضة أو مجهولة

التحقُّق من الصور والفيديوهات

الصور والفيديوهات تُعتبَر الأكثر استغلالًا في التضليل، خصوصًا مع تقنيات التعديل الحديثة.

طرق التحقُّق

- استخدام البحث العكسي عن الصور لتحديد أصلها وتاريخها
- استخدام أدوات موثوقة لتحليل الفيديوهات والكشف عن الإطارات والتفاصيل
- التدقيق في الظلال أو ملامح المكان لمطابقتها مع الحدث
- مقارنة المحتوى مع أكثر من مصدر موثوق

التزييف العميق والفيديوهات المُفَبْرَكَة

التزييف العميق أصبح أحد أخطر وسائل التضليل؛ نظرًا لصعوبة اكتشافه.

مؤشرات الكشف

- عدم تطابق حركة الفم مع الصوت في الفيديو
- تفاصيل بصرية غير طبيعية مثل الألوان أو الظلال
- غياب مصادر أصلية للمقطع أو نشره أولًا عبر قنوات مجهولة
- اقتصار الفيديو على نسخة واحدة رغم أهميته المُفتَرضَة

دور وسائل التواصل الاجتماعي في نشر التضليل

وسائل التواصل ساعدت على تسريع انتشار الأخبار الكاذبة بشكلٍ غير مسبوق.

أبرز سمات النشر عبر وسائل التواصل

- الاعتماد على العناوين المثيرة لجَذْب التفاعل دون التأكُّد من المضمون
- إعادة نشر الأخبار بسرعة من دون تحقُّق مسبق
- استخدام الصور المُعدَّلة والهاشتاغات لنشر الشائعة
- الاعتماد على "الترند" كدليل كاذب على المصداقية

خطوات الوقاية من الوقوع في التضليل

لتقليل الخطر من الوقوع في التضليل، هناك مجموعة من الإجراءات الوقائية الأساسية.

خطوات الوقاية

- بناء شبكة من المصادر الموثوقة لتأكيد الأخبار
- عدم التسرُّع في نَشْر أيّ خبر قبل التحقُّق من صحته
- توعية الجمهور بخطورة الأخبار المُضلّلة وآليات كشفها
- الاعتماد على مصادر متعدّدة ومتنوّعة قبل اعتماد المعلومة

الإشارات التحذيرية في النصوص المُضلّلة

الأخبار المُضلّلة غالبًا ما تحمل أنماطًا لغويةً متكرّرة يمكن ملاحظتها.

السمات التحذيرية

- استخدام لغة عاطفية مُبالَغ فيها؛ لإثارة الخوف أو الغضب
- الاعتماد على عبارات مثل "مصادر مطلعة"، أو "خبير لم يُصرّح باسمه"
- غياب التفاصيل الدقيقة مثل المكان والزمان
- المُبالَغة في الأرقام والإحصائيات من دون مصدر موثق

الهجمات السيبرانية المرتبطة بنَشْر الأخبار المُضلّلة

غالبًا ما تبدأ الحملات المُضلّلة بمحاولات اختراق حسابات الصحفيين أو المؤسسات الإعلامية.

مظاهر هذه الهجمات

- اختراق البريد الإلكتروني لنشر أخبار مُزيَّفة باسم الصحفي
- السيطرة على حسابات وسائل التواصل الاجتماعي لبثّ الشائعات
- استهداف المواقع الإعلامية بهجمات حَجْب الخدمة لتعطيلها
- استخدام البرمجيات الخبيثة للتجسس على الأجهزة وسرقة المعلومات

حماية الحسابات من الاختراق

الحسابات الرقمية للصحفيين تُعدّ بوابة أساسية للهجمات المُضلّلة.

خطوات الحماية

- استخدام كلمات مرور قوية وفريدة لكل حساب
- تفعيل المصادقة الثنائية لحماية إضافية
- مراجعة النشاطات الأخيرة في الحسابات؛ للكشف عن أيّ دخول غير مشروع
- الحذر من رسائل البريد أو الروابط المشبوهة

السؤال التفاعلي الرابع

السؤال التفاعلي الخامس

5- ما أبرز مؤشر على أن الفيديو مُفَبْرَك بتقنية التزييف العميق؟

- **أ.** وضوح عالٍ في الصورة
- **ب.** تثبيت تحديثات النظام تلقائيًّا
- **ج.** ظهور تفاصيل غير طبيعية في الوجوه أو الألوان أو الظلال
- **د.** وجود أكثر من نسخة للمقطع في مصادر مختلفة

السؤال التفاعلي السادس

6- ما نتائج الضغط على رابط مجهول المصدر في رسالة بريد إلكتروني؟

أ. تحسين سرعة الاتصال بالإنترنت

ب. تثبيت تحديثات النظام تلقائيًّا

ج. إعادة توجيه المستخدِم إلى صفحات مُزيَّفة، أو تحميل برمجيات خبيثة

د. زيادة مساحة التخزين في الجهاز

إجابات الأسئلة التفاعلية

01 **إجابة السؤال التفاعلي الأول**

أ. حفظها على القرص الخارجي غير المتصل بالإنترنت

02 **إجابة السؤال التفاعلي الثاني**

أ. ارتفاع حرارة الجهاز وبطؤه رغم قلة البرامج

03 **إجابة السؤال التفاعلي الثالث**

ب. جعل الحساب يحتاج لخطوتين مختلفتين لتأكيد الدخول

04 **إجابة السؤال التفاعلي الرابع**

1. ب. تضليل الجمهور أو التأثير على الرأي العام

05 **إجابة السؤال التفاعلي الخامس**

ج. ظهور تفاصيل غير طبيعية في الوجوه أو الألوان أو الظلال

06 **إجابة السؤال التفاعلي السادس**

ج. إعادة توجيه المستخدم إلى صفحات مُزيَّفة، أو تحميل برمجيات خبيثة

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