الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

أمن البيانات والسلامة الرقمية

الشريحة المستهدفة

الإعلاميون

كُتَيّب المُدَرّب

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مبادئ عامة في السلامة الرقمية

أمن البيانات والسلامة الرقمية

الشريحة المستهدفة

الإعلاميون

كُتيّب المُدَرّب

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

1655

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 وحماية أجهزتهم وبياناتهم في أثناء التغطيات الميدانية، والتعامل الآمِن مع الشبكات العامة، وحماية الصور والمصادر الصحفية.

إضافةً إلى إستراتيجيات حماية السُّمعة الإلكترونية وإدارة الهوية الرقمية، ممّا يجعل السلامة الرقمية أولويةً مهنيةً يومية للإعلاميين.

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

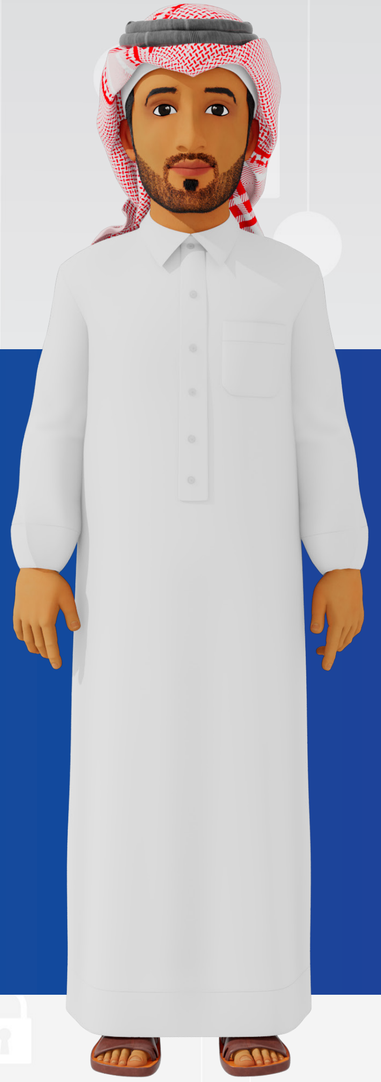
مجموعة من فعاليات التوعية في مجال السلامة الرقمية والأمن السيبراني؛ تَستهدف المجتمع المحلي على اختلاف الشرائح العُمرية والاجتماعية والقطاعات المهنية.

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

أمن البيانات في أثناء التغطيات الميدانية

حماية الأجهزة خلال التنقل

الأجهزة المحمولة هي الأداة الأهم في العمل الميداني، لكنّها أيضًا الأكثر عُرضة للضياع أو السرقة.

خطوات الحماية

- استخدام كلمات مرور قوية، وتشفير كامل للأجهزة المحمولة
- حمل الحواسيب والهواتف في حقائب آمِنَة مُزوّدة بأقفال
- تعطيل الاتصال التلقائي بشبكات Wi-Fi أو Bluetooth في أثناء التنقل
- تفعيل ميزة "العثور على الجهاز"؛ لإمكانية قفله عن بُعْد عند فقدانه

إدارة البيانات الحساسة في التحقيقات الصحفية

التحقيقات الصحفية غالبًا ما تتضمَّن معلومات بالغة الأهمية يجب حمايتها بعناية.

خطوات الإدارة الآمِنَة

تصنيف البيانات وفق مستوى حساسيتها (عادي - سري - سري للغاية)

استخدام كلمات مرور منفصلة للملفات عالية الأهمية

تخزين الملفات الحساسة في أقراص أو وحدات تخزين مشفّرة

عدم نَسْخ البيانات إلى وسائط خارجية غير محمية

إجراءات السلامة عند استخدام الشبكات العامة

شبكات الإنترنت العامة أكثر عُرْضَة للهجمات السيبرانية.

خطوات الحماية

- تجنُّب الوصول إلى الحسابات أو البيانات الحساسة عبر شبكة إنترنت عامة
- استخدام VPN لحماية حركة البيانات
- تفعيل جدار الحماية الشخصي عند الاتصال بالشبكات العامة
- تسجيل الخروج من جميع الحسابات بعد الاستخدام مباشرة

أدوات VPN للصحفيين

شبكات VPN تُعدّ مِن أهمّ الوسائل لتأمين الاتصال بالإنترنت.

فوائد استخدامها

- تشفير حركة البيانات، ومنع اعتراضها
- تغيير عنوان الجهاز على الإنترنت؛ لإخفاء موقع المُستخدِم
- تقليل مخاطر الاختراق عند استخدام شبكات عامة

حماية البيانات

حماية البيانات من أولويات الأمن السيبراني؛ لذلك يجب اتباع خطوات ضرورية لحمايتها ومنع تسربها أو إتلافها.

إجراءات الحماية

- أرشفة المواد النهائية في خوادم مُؤمَّنة
- حَذْف الملفات غير الضرورية لمنع تسريبها
- نقل الملفات الحساسة إلى وسائط تخزين غير متصلة بالإنترنت
- مراجعة دورية لضمان بقاء البيانات بأمان على المدى الطويل

التعامل مع مصادر مجهولة عبر الإنترنت

المصادر المجهولة قد تكون فرصة للحصول على معلومة مهمة، لكنّها في المقابل قد تُستغَل كأداة لتضليل الصحفي.

الوقايـــــة

التأكُّد من الهوية الرقمية

استخدام أدوات تتبُّع البريد أو الحسابات؛ للتأكد من أصالة الجهة المرسِلة

التعامل عبر قنوات آمِنَة

الاعتماد على تطبيقات تَراسُل مُشفّرة عند الحاجة للتواصل

التحقّق المتقاطع

مقارنة ما يُقدّمه المصدر مع بيانات من مصادر أخرى موثوقة

حماية الصور والفيديوهات

الصور والفيديوهات التي يجمعها الصحفي قد تحتوي على أدلة حساسة أو تفاصيل ميدانية يمكن استغلالها ضدّه أو ضدّ مصادره.

الحماية

استخدام وسائط تخزين مُؤمَّنة

مثل الأقراص المشفَّرة أو التخزين السحابي

مَنْح حَقّ الوصول المحدود

مشاركة الموادّ فقط مع الأطراف الموثوقة

الاعتماد على علامات مائية

لحماية الحقوق ولإثبات المصدر عند إعادة النشر

السؤال التفاعلي الأول

1 ما الخطر الأساسي من استخدام الإنترنت العام دون أدوات حماية؟

أ. بُطْء سرعة الاتصال

ب. إمكانية اعتراض البيانات والوصول إلى الحسابات

ج. تقليل حجم الملفات المرسلة

د. صعوبة تسجيل الدخول إلى الحسابات

السؤال التفاعلي الثاني

2 ما الهدف الأساسي من استخدام VPN في أثناء التغطيات الميدانية؟

أ. زيادة سرعة الإنترنت

ب. تحسين جودة الفيديو

ج. تشفير الاتصال وإخفاء الموقع الحقيقي

د. تخزين الملفات الكبيرة على الخادم

السؤال التفاعلي الثالث

3 لماذا يُنْصَح بحذف الملفات غير الضرورية بعد انتهاء التحقيق؟

أ. لتسريع عمل الجهاز فقط

ب. لتوفير مساحة تخزين أكبر

ج. لتقليل احتمالية تسريب البيانات أو استغلالها

د. لزيادة سرعة الإنترنت

الفصل الثاني

السلامة الرقمية للصحفيين والإعلاميين

إدارة الهوية الرقمية

الهوية الرقمية تُمثّل الانعكاس الافتراضي لشخصية الصحفي ومصداقيته.

خطوات الإدارة الآمِنَة

- الفصل بين الحسابات الشخصية والمهنية بشكل واضح
- مراجعة الإعدادات الأمنية لحسابات التواصل الاجتماعي بانتظام
- استخدام صور وأسماء رسمية فقط في الحسابات المهنية
- مراقبة أيّ انتحال أو تزوير للهوية الرقمية والإبلاغ عنه فورًا

حماية السمعة الإلكترونية

تشويه السمعة عبر الإنترنت قد يُستخدم كسلاح ضد الصحفيين.

إجـــراءات الحمـــاية

تفعيـل التنبيهـات لمراقبـة ذِكْـر الاسـم أو المؤسسـة عبـر الإنترنـت

التواصـل مـع المنصـات لإزالـة المحتـوى المسـيء بسـرعة

الـرد بحـذر وتجنُّـب الدخـول فـي جـدالات مفتوحـة تزيد مـن الانتشـار السـلبي

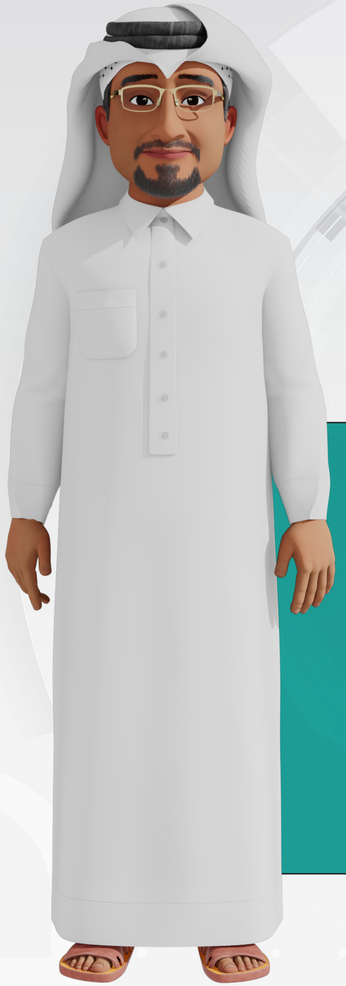
إستراتيجيات التعامل مع محاولات الاختراق

الهجمات الرقمية قد تَستهدف الأجهزة، الحسابات، أو حتى المؤسسات الصحفية بأكملها.

خطوات الاستجابة

- عَزْل الجهاز أو الحساب المتضرّر فورًا عن الشبكة
- تحديد نوع الهجـــوم (تصيُّد، اختراق، برمجيات خبيثة...)
- تغيير كلمات المرور لجميع الحســـابات المرتبطة
- إبلاغ الفريق التقني أو المؤسسة لاتخاذ الإجراءات العاجلة.

استخدام أدوات الأمن السيبراني



بعض الأدوات تُمكِّن الصحفيين من تعزيز دفاعاتهم الرقمية بشكل ملحوظ.

أبرز الأدوات

- برامج مكافحة الفيروسات المتقدّمة مع خاصية التحديث التلقائي
- جدران حماية شخصية لمنع التسلل والاختراق
- أدوات تشفير الملفات وحمايتها بكلمات مرور قوية
- برامج إدارة كلمات المرور

الخصوصية على شبكات التواصل

الخصوصية الرقمية تُمثِّل خطّ الدفاع الأول للصحفي؛ إذ تساعد على تقليل فرص استهدافه أو جمع معلومات عنه.

خطوات مهمة لحماية الخصوصية

مراجعة صلاحيات التطبيقات بانتظام

تعطيل أيّ صلاحيات غير ضرورية؛ مثل الوصول إلى الكاميرا أو جهات الاتصال

ضبط قوائم الأصدقاء والمتابعين

قبول الطلبات من أشخاص موثوقين فقط، ومراجعة الحسابات المشبوهة بشكل دوري

تقييد عرض المنشورات

استخدام إعدادات الخصوصية لتحديد مَن يُمكنه رؤية المحتوى

مراقبة الحسابات المُزيَّفة

البحث المستمر عن حسابات تنتحل شخصية الصحفي والإبلاغ عنها

الهندسة الاجتماعية

الهندسة الاجتماعية من أخطر أساليب الاختراق؛ لأنها تستهدف الصحفي نفسيًّا وسلوكيًّا أكثر من استهداف جهازه.

خطوات الحماية

عدم مشاركة كلمات المرور

كلمات المرور شخصية، ولا يُفْصح عنها لأيّ شخص مهما كانت درجة الثقة

التأكُّد من هوية المتواصل

التحقّق من أرقام الهواتف والبريد قبل الرد على أيّ طلب حساس

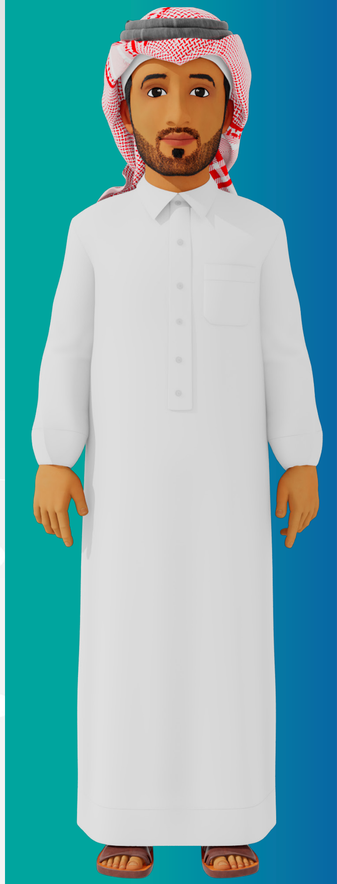
الحذر من مكالمات أو رسائل تدّعي أنها من جهات رسمية

التحقُّق من القنوات الرسمية وعدم الاستجابة الفورية

اتّباع مبدأ الشك المهني

أيّ تواصل غير متوقَّع يُعامَل بحذرٍ، حتى يثبت العكس.

السؤال التفاعلي الرابع



4 ما الهدف الأساسي من إدارة الهوية الرقمية للصحفي؟

أ. زيادة عدد المتابعين

ب. تعزيز المصداقية وحماية الحسابات من الانتحال

ج. تحسين سرعة الإنترنت

د. تقليل استهلاك البطارية

السؤال التفاعلي الخامس

5 ما أول خطوة يجب القيام بها عند اكتشاف اختراق في جهاز؟

أ. الاستمرار في استخدام الجهاز

ب. إعادة تشغيل الجهاز فقط

ج. عزل الجهاز أو الحساب عن الشبكة فورًا

د. حذف جميع الملفات

إجابات الأسئلة التفاعلية

01 **إجابة السؤال التفاعلي الأول**

ب. إمكانية اعتراض البيانات والوصول إلى الحسابات

02 **إجابة السؤال التفاعلي الثاني**

ج. تشفير الاتصال وإخفاء الموقع الحقيقي

03 **إجابة السؤال التفاعلي الثالث**

ج. لتقليل احتمالية تسريب البيانات أو استغلالها

04 **إجابة السؤال التفاعلي الرابع**

ب. تعزيز المصداقية وحماية الحسابات من الانتحال

05 **إجابة السؤال التفاعلي الخامس**

ج. عزل الجهاز أو الحساب عن الشبكة فورًا

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