الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

الشريحة المستهدفة
منظمات المجتمع المدني

كُتَيّب المُدَرّب

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

الشريحة المستهدفة

منظمات المجتمع المدني

كُتَيّب المُدَرّب

تمهيد

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

تم تصميم هذا الكُتَيِّب بهدف توعية منظمات المجتمع المدني بمبادئ السلامة الرقمية، وأفضل الممارسات التي تساعدهم على تفادي المخاطر السيبرانية؛ حيث إنّ الأمن السيبراني في هذه المؤسَّسات ليس مُجرَّد ضرورة تقنية، بل هو عامل أساسي لضمان استمرار تقديم الخدمات وتعزيز ثقة المجتمع بها.

وإنّ حِرْص منظمات المجتمع المدني على تعزيز الحماية الرقمية يُسهم في تقليل المخاطر وضمان استدامة العمل في مُواجهة التحديات الحديثة.

وتُعدّ هذه الجهود جزءاً 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

المحور الأول

التهديدات السيبرانية الشَّائعة

مخاطر أمن الأجهزة المحمولة

1. اختراق الجهاز أو سرقة بياناته الحساسة
2. تثبيت تطبيقات خبيثة وسرقة بيانات الدخول
3. أذونات زائدة تَسْمح للتطبيقات بجَمْع البيانات
4. فقدان الجهاز أو سرقته يُؤدّي إلى كَشْف بيانات شخصية ومؤسسية
5. تهديدات Wi-Fi المفتوحة واعتراض الاتصالات

سرقة الهوية عبر الإنترنت

يتعرض ملايين الأشخاص سنويًّا لسرقة معلوماتهم الشخصية، واستخدامها بشكلٍ غير قانوني لأغراض مالية أو احتيالية.

أسباب سرقة الهوية

01 الانتشار الواسع للإنترنت

زيادة الاعتماد على الإنترنت جعلت المعلومات الشخصية أكثر عرضةً للسرقة.

02 الثغرات الأمنية

عدم تأمين المواقع والتطبيقات بشكلٍ كافٍ يمكن أن يُؤدّي إلى تعرُّض البيانات للاختراق.

03 نقص الوعي الأمني

يسهم نقص الوعي بأساليب الحماية الإلكترونية في تسهيل تعرُّض المُستخدِمين للهجمات الإلكترونية.

حقائق ومعلومات

سرقة الهوية عبر الإنترنت تُكلِّف الاقتصاد العالمي أكثر من 50 مليار دولار سنوياً.

مخاطر سرقة الهُويَّة

الاستيلاء على بيانات حكومية أو شخصية، ممّا يُؤدّي إلى خسائر مالية أو مشكلات قانونية

اختراق البريد الإلكتروني والوصول إلى حسابات حسَّاسة مثل البريد الحكومي

انتحال هوية المستخدِم في معاملات مالية أو تنفيذ جرائم رقمية باسم الضحية

استخدام البيانات المسروقة لإنشاء حسابات مُزيَّفة أو تنفيذ عمليات احتيال

أدوات سرقة الهوية

سرقة هوية البريد الإلكتروني

من خلال خرق البريد الإلكتروني للضحية، يمكن للمخترق العثور على معلومات شخصية مهمّة، مثل: أرقام الحسابات المصرفية، وبيانات تسجيل الدخول للمواقع؛ مما يُسهّل عملية سرقة الهوية.

احتيال التسوق عبر الإنترنت

يُقصَد به استغلال مُجرِمي الإنترنت حساب تسوُّقٍ ما لتنفيذ طلبات شرائية دون عِلْم الضحية، ويحدث ذلك إما من خلال خرق البيانات أو التصيد الاحتيالي أو البرمجيات الضّارَّة.

سرقة هوية كبار القَدْر والأطفال

يُعدّ كبار القَدْر والأطفال أكثر عُرضةً لهجمات سرقة الهوية بهدف الحصول على المعلومات الشخصية والوصول إلى الحسابات المصرفية لكبار القَدْر، أو أخذ بيانات الطفل لإنشاء حسابات أخرى للاحتيال على الآخرين أو لابتزاز الطفل.

لنَحْذَر!

من استخدام كلمات مرور ضعيفة، مثل الأسماء أو التواريخ التي يسهل تخمينها، ولْنَخْتَر دائمًا كلمات مرور مُعقَّدة تحتوي على أحرف كبيرة وصغيرة وأرقام ورموز.

كيف يمكن تنفيذ سرقة الهوية عبر الإنترنت؟

01

ترتبط سرقة الهوية بشكلٍ وثيقٍ بالتصيد الاحتيالي وتقنيات الهندسة الاجتماعية التي عادةً تُستخدَم لانتزاع معلومات شخصية سرية من الضحايا.

02

بمجرَّد جمع هذه المعلومات يبدأ مُجرِمو الإنترنت في الاستيلاء على حسابات مصرفية عائدة للضحايا أو القيام بإجراءات قانونية باسمهم مثل إصدار التراخيص وإبرام العقود.

علامات سرقة الهوية

رصد نشاط غير طبيعي في الحسابات المصرفية أو تقارير الائتمان بسبب استخدام الهوية المسروقة لإنفاق الأموال أو فتح حسابات جديدة.

01

تلقّي إشعارات من المصرف تُفيد بإنفاق أموال أو تجاوز الحد الائتماني دون عِلْمك.

02

رفض البطاقة الائتمانية عند محاولة الشراء رغم توفُّر الرصيد.

03

علامات سرقة الهوية

التوقُّف عن تلقّي الفواتير عبر البريد الإلكتروني؛ مما يُشير إلى أن المجرم قام بتغيير بيانات الاتصال.

04

عدم القدرة على تسجيل الدخول إلى الحسابات المصرفية أو حسابات التواصل الاجتماعي.

05

حقائق ومعلومات

تحدث محاولة اختراق سيبراني على الإنترنت كل 39 ثانية؛ مما يُوضّح حجم الخطر المستمر الذي يتعرّض له المُستخدِمون.

أنواع برمجيات الفدية (Ransomware)

Crypto Ransomware

يقوم هذا النوع بتشفير ملفات المُستخدِم وطلب فدية لفَكّ التشفير.

Locker Ransomware

يمنع هذا النوع الوصول إلى الجهاز بالكامل، وليس الملفات فقط، ويطلب فديةً لإعادة الوصول.

Scareware

يعتمد على التخويف بإرسال إشعارات كاذبة تدَّعي اكتشاف البرمجيات الخبيثة، ويطلب دفع فدية لإصلاح المشكلة.

Doxware

يُهدّد بنشر المعلومات الحسَّاسة المسروقة من الضحية إذا لم يتم دفع الفدية.

مخاطر برمجيات الفدية (Ransomware)

1
تشفير البيانات بالكامل أو إغلاق الأجهزة مما يمنع الوصول إليها

2
حَجْب الأنظمة الحيوية والملفات التشغيلية الضرورية للعمل

3
تهديد بنشر بيانات حساسة (Doxware) للحصول على فدية إضافية

4
انتشار سريع عبر مرفقات البريد الإلكتروني، والتطبيقات المقرصنة، والثغرات الأمنية

5
خسائر تشغيلية، وتوقُّف الخدمات، ودفع فدية محتملة

التهديدات السيبرانية الخاصة بالمجتمع المدني

1. سرقة البيانات الحسَّاسة: منظمات المجتمع المدني تُخزّن بعض البيانات الشخصية والحسَّاسة مثل الهُويات الوطنية، السجلات الصحية، والبيانات المالية التي يمكن أن تُستغَلّ في الهجمات.
2. تعطيل الخدمات العامة: الهجمات السيبرانية مثل هجمات الحرمان من الخدمة (DDoS) قد تُعطِّل البِنْيَة التَّحتيَّة الأساسية، مثل المياه والكهرباء والخدمات الصحية.
3. الهجمات على شبكات الاتصال: استهداف شبكات الاتصالات يمكن أن يُؤدِّي إلى تعطيل أنظمة الإبلاغ الطارئ والتواصل الداخلي.
4. الهندسة الاجتماعية: تَستهدف الموظفين عبر رسائل خادعة للحصول على بيانات تسجيل الدخول أو الوصول إلى الأنظمة الحسَّاسة.
5. الاعتماد على التكنولوجيا غير المُحدَّثة: يُؤدّي استخدام البرمجيات القديمة إلى زيادة مخاطر الثغرات الأمنية.

الجرائم السيبرانية الشائعة

1

التَّصيُّد الاحتيالي

يَستخدم المهاجمون رسائل بريد إلكتروني مُزيَّفة لخداع الموظفين للكشف عن معلومات حساسة.

2

برمجيات الفدية (Ransomware)

تشفير البيانات الأساسية للمؤسسة، والمطالبة بفدية لفكّ تشفيرها.

3

البرمجيَّات الضَّارَّة (Malware)

برامج تستهدف تعطيل الأنظمة أو سرقة المعلومات.

4

هجمات الحرمان من الخدمة (DDoS)

إغراق الشبكات بطلبات وهمية لإيقاف الخدمات.

5

استهداف سلاسل التوريد

مُهاجمة الشركات المُورّدة للحصول على وصول غير مباشر إلى الأنظمة الأساسية.

تأثير الهجمات السيبرانية

1. **الخسائر المالية:** التكاليف المرتبطة بإصلاح الأنظمة، ودفع الفدية، والتعويضات القانونية.

2. **فقدان الثقة:** تعرُّض بيانات العملاء أو المواطنين للخرق يُؤدّي إلى تراجع الثقة بالمؤسسة.

3. **توقُّف الخدمات:** الهجمات قد تؤدي إلى شلل مُؤقّت أو طويل الأمد في تقديم الخدمات العامَّة.

تأثير الهجمات السيبرانية

4

الأضرار القانونية والتنظيمية: الهجمات قد تُعرّض المؤسسة للمساءَلة القانونية وغرامات تتعلق بعدم الامتثال لمعايير الأمن السيبراني.

5

التأثير على السُّمعة: تُؤثّر الهجمات سلباً على سُمعة المؤسَّسة المدنية بين الجمهور.

السؤال التفاعلي الأول

1 ما هو التصرُّف الصحيح عند تلقِّي بريد إلكتروني يبدو رسميًّا به مرفقات مجهولة؟

- أ. فتحها فورًا
- ب. الضغط على المرفقات للتحقُّق
- ج. حذف الرسالة
- د. التواصل مع الجهة الرسمية من خلال موقعها أو الاتصال المباشر

السؤال التفاعلي الثاني

السؤال التفاعلي الثالث

المحور الثاني

آليات الوقاية والسلامة الرقمية

كلمات المرور لحماية الهواتف المحمولة

كلمات المرور تُعدّ خط الدفاع الأول للهواتف المحمولة، ولا بدَّ من مراعاة الآتي عند كتابة كلمات المرور:

- اختيار مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز.
- تجنُّب استخدام كلمة المرور نفسها لعدَّة حسابات أو أجهزة مختلفة.
- تغيير كلمات المرور بشكلٍ دَوري.

حقائق ومعلومات

85% من خروقات الأمن السيبراني ناتجة عن أخطاء يرتكبها مُستخدِمو الإنترنت، منها فتح روابط مجهولة، أو تقديم بيانات شخصية للغُرَباء، أو عدم اتباع تعليمات التصفُّح الآمِن للإنترنت.

القياسات الحيوية لحماية الهواتف المحمولة

القياسات الحيوية تُعدّ طبقة حماية إضافية لأجهزة الهواتف المحمولة، وتشمل:

- بصمة الإصبع.
- التعرُّف على الوجه.
- لزيادة مستوى الأمان يُنصَح بتمكين كلمة المرور الاحتياطية أو رقم التعريف الشخصي (PIN) في حالة فشل المصادقة البيومترية أو تَعرُّضها للخطر.

المصادقة مُتعدّدة العوامل

01

المصادقة متعددة العوامل تُعدّ طبقة أمان إضافية تهدف إلى التحقُّق من هُويّة المُستخدِم قبل السماح له بالوصول إلى البيانات.

02

الهدف من المصادقة مَنْع المُستخدِمين غير المصرَّح لهم من الوصول إلى الشبكة أو البيانات.

03

يُفضَّل اعتماد أساليب مصادقة قوية؛ مثل: المزج بين كلمات المرور، أو القياسات الحيوية كبصمة الإصبع والوجه، أو أرقام التعريف الشخصية.

04

المصادقة من التقنيات الفعالة التي تُوفّر الحماية للهواتف المحمولة من التهديدات السيبرانية.

حقائق ومعلومات

البصمة الرقمية هي مسارات عبر الإنترنت نتركها وراءنا، تنشأ من استخدامنا لمواقع الويب ومنصات التواصل الاجتماعي، وعمليات الشراء عبر الإنترنت.

تشفير بيانات الهواتف المحمولة

التشفير هو عملية تحويل البيانات إلى رموز لا يمكن الوصول إليها إلا للأطراف المصرَّح لها باستخدام مفتاح التشفير.

يمكن تشفير مساحة تخزين جهاز الهاتف وبيانات التطبيقات.

يُعدّ تشفير بيانات الهاتف المحمول أداةً فعّالةً لحماية البيانات المهمّة من السرقة في حالة اختراق الجهاز أو سرقته أو فقدانه.

عملية التشفير تقوم بتحويل البيانات إلى رموز غير مقروءة وغير مفهومة؛ ممّا يمنع المهاجمين من الاستفادة منها.

حقائق ومعلومات

تتصاعد الخسائر الناجمة عن الهجمات السيبرانية بشكلٍ كبيرٍ، فمِن المتوقَّع أن تصل إلى أكثر من 10 تريليونات دولار في عام 2025.

طُرق تشفير بيانات الهواتف المحمولة

يمكن تفعيل التشفير على أجهزة IOS من قائمة الإعدادات عبر الضغط على (Face ID & Passcode)، والذي سيُطالب المُستخدِم بإدخال رمز قفل الشاشة الخاص به، ثمّ التمرير إلى أسفل الصفحة؛ حيث تظهر عبارة "تمَّ تمكين حماية البيانات".

يتم تشفير أجهزة الأندرويد من خلال تحديد حقل "الأمان" من الإعدادات، ثمّ تحديد خيار "التشفير"، ومنه اختيار "تشفير الهاتف".

في حالة عدم شحن الهاتف أو مقاطعة عملية التشفير عندها سيتم فَقْد جميع البيانات، فعملية التشفير تستغرق نحو ساعة وأكثر؛ لهذا يجب الاستعداد جيداً قبل البدء بها.

تحديث برامج وتطبيقات الهاتف المحمول

01 التحديثات هي عملية تثبيت إصدارات حديثة لبرامج أو أنظمة الهواتف المحمولة؛ بهدف تعزيز أمانها، وإصلاح الأخطاء أو نقاط الضعف أو مشكلات التوافق.

02 يُفضَّل التحديث بشكلٍ منتظم، أو تمكين التحديث التلقائي.

03 تطبيقات وأنظمة الهواتف المحمولة المُحدَّثة تُوفّر أماناً للهاتف المحمول، وتحميه من الخروقات.

إدارة أذونات الهاتف المحمول

الأذونات هي عملية التحكُّم في الوصول إلى ميزات أو وظائف معيَّنة على الهواتف أو التطبيقات.

تسهم الأذونات في تعزيز خصوصية وأمان الجهاز.

بالاعتماد على الأذونات يمكن تحديد البيانات التي يمكن الوصول إليها أو استخدامها أو مشاركتها.

لا بدَّ من الحذر عند إدارة الأذونات، ومنح الحد الأدنى من الوصول اللازم لأداء المهام فقط، ومراجعة الأذونات وإلغائها بانتظام، وتجنُّب مَنْحها لمصادر مجهولة.

احذر!

لا تُشارِك معلوماتك الشخصية، مثل رقم الهوية أو العنوان أو رقم الهاتف، على مواقع أو منصَّات لا تتأكّد من أمانها.

الهُويَّة الرقمية وأمن الاتصالات

حماية الهوية الرقمية من السرقة تعتمد على تأمين اتصال آمِن بالإنترنت، من خلال:

01

التأكد عند إدخال المعلومات الشخصية عبر الإنترنت أن الاتصال آمِن. لذا يُنصَح دوماً باستخدام شبكة المنزل أو البيانات الخلوية، وتجنُّب شبكة Wi-Fi العامة، والتي تكون بدون حماية.

02

استخدام VPN في حال الاضطرار لاستخدام الشبكة العامة؛ بهدف حماية البيانات والاتصالات من القرصنة الإلكترونية ولتشفير جميع الاتصالات.

لنَحْذَر!

النقر على أيّ روابط مشبوهة تصل عبر البريد الإلكتروني، حتى لو بدا أن المُرسِل شخص نعرفه، فمن الممكن أن تكون محاولة تصيُّد احتيالي.

الهُويَّة الرقمية وكلمات المرور

إنشاء كلمات مرور قوية يصعب تخمينها، ولحمايتها من السرقة يمكن استخدام مدير كلمات المرور لتخزينها بشكلٍ آمِن.

اختيار كلمات مرور مؤلَّفة من مزيجٍ من الأحرف والأرقام والرموز.

في حال الرغبة في إضافة طبقة أمان أخرى، فالمصادقة الثنائية تُحقّق ذلك.

عدم استخدام أيّ كلمة مرور لحسابات أو خدمات متعدّدة.

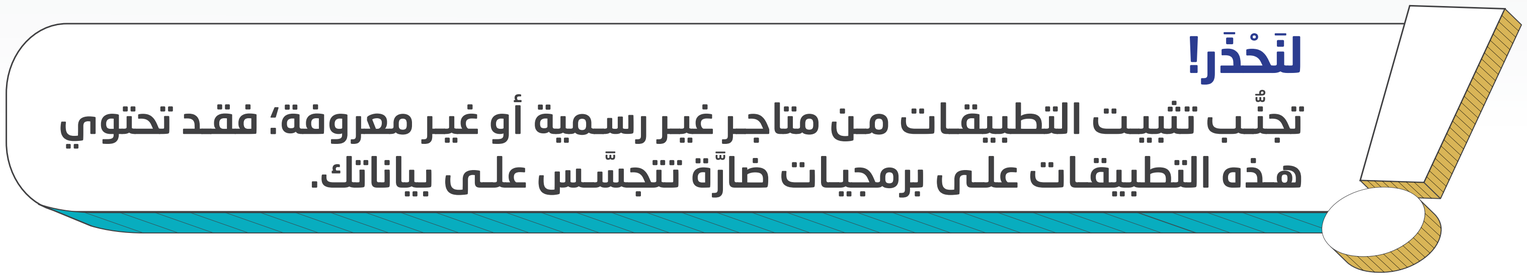
تغيير كلمات المرور بشكلٍ دَوريّ.

حقائق ومعلومات

التصيد الاحتيالي أحد أكثر أساليب الهجمات شيوعًا؛ وذلك من خلال إغراء المُستخدِمين لتقديم معلوماتهم الشخصية عبر رسائل مزيَّفة.

البصمة الرقمية وحماية الهوية

الإفراط في مشاركة البيانات الشخصية عبر وسائل التواصل الاجتماعي، يمكن أن يساعد المجرمين على سرقة الهوية الرقمية.



لنَحْذَر!

تجنُّب تثبيت التطبيقات من متاجر غير رسمية أو غير معروفة؛ فقد تحتوي هذه التطبيقات على برمجيات ضارَّة تتجسَّس على بياناتك.

حماية الهوية عبر الإنترنت

01 التأكد من بدء عنوان الويب بـ https وليس http؛ إذ يُشير حرف «s» إلى الأمان، مع وجود رمز القفل بجوار الرابط.

02 الاتصال بالمرسل عند الشَّك في هويّة المُرسِل على البريد الإلكتروني.

03 تفعيل التحديث التلقائي لجميع البرامج والتطبيقات ومُتصفّح الويب.

04 تثبيت برامج مكافحة الفيروسات، وبرامج مكافحة البرمجيات الضّارَّة.

05 عدم منح الغرباء حق الوصول إلى جهاز الحاسوب أو الهاتف عن بُعد.

لنَحْذَر!

تجاهُل تحديثات البرامج والتطبيقات؛ فالتحديثات غالباً ما تحتوي على إصلاحات أمنية مُهمّة للحماية من الثغرات الجديدة.

حماية البيانات الرقمية

مراقبة الحسابات المصرفية

يُعدّ التحقُّق من الحساب المصرفي عبر الإنترنت بانتظام أمراً ضرورياً؛ لرصد أيّ نشاط مشبوه واتخاذ الإجراء المناسب لمنع وقوع أضرار جسيمة للأموال أو السُّمعة.

الحذر عند التخلص من البيانات المهمَّة

عند التخلُّص من أوراق أو مستندات تحتوي على معلومات شخصية أو مهمَّة، ينبغي التخلص منها بشكل آمِن؛ منعاً من وصولها إلى أيدي المحتالين.

ينطبق الأمر كذلك على الحواسيب والهواتف، ففي حالة الرغبة في بيعها يجب التأكد من مسح جميع البيانات الشخصية المخزَّنة عليها.

الحماية من برمجيات الفدية (Ransomware)

- تثبيت برامج حديثة وفعَّالة لمكافحة الفيروسات.
- تحديث نظام تشغيل الجهاز.
- فحص وسائط التخزين الخارجية قبل توصيلها بالجهاز.
- استخدام كلمات مرور قوية، وتغييرها بين الحين والآخر.

الحماية من برمجيات الفدية (Ransomware)

عدم فتح مرفقات البريد الإلكتروني الوارد من أشخاص مجهولين.

عدم فتح الإعلانات المنبثقة على مواقع الإنترنت.

النَّسخ الاحتياطي للبيانات بشكلٍ دَوريّ.

حقائق ومعلومات

الشركات التي تعتمد على إنترنت الأشياء في الصناعة تزيد من كفاءتها الإنتاجية بنسبة 25% عن طريق تحسين مراقبة المعدات.

أفضل الممارسات لتقليل المخاطر

01 **إدارة الوصول**

التَّأكُّد مِن مَنْح الصلاحيات فقط للمُوظّفين الذين يحتاجونها لأداء عملهم.

02 **تحديث الأنظمة**

المحافظة على تحديث أنظمة التشغيل والبرامج لسدّ الثغرات الأمنية.

03 **التدريب المستمر**

توعية الموظفين حول التهديدات السيبرانية، وكيفية التعامل معها.

04 **التشفير**

استخدام التشفير لحماية البيانات الحسَّاسة أثناء نقلها وتخزينها.

05 **المراقبة المستمرة**

استخدام أدوات لرَصْد النشاط غير المعتاد داخل الأنظمة.

إجراءات الحماية المخصَّصة

اختبارات الاختراق

إجراء اختبارات دَورية لتحديد نقاط الضعف في الأنظمة.

1

خطة استجابة للحوادث

إعداد خطة واضحة للتعامل مع الهجمات السيبرانية وتقليل آثارها.

2

النَّسخ الاحتياطي للبيانات

الاحتفاظ بنُسَخ احتياطية دَوْرية للبيانات في مواقع آمِنَة.

3

المصادقة مُتعدّدة العوامل (MFA)

إضافة طبقات أمان إضافية لتسجيل الدخول.

4

عَقْد شَراكات مع جهات الأمن السيبراني

التَّعاون مع شركات مُتخصّصة لتحسين الدفاعات الأمنية ومُواجَهة التهديدات المتطورة.

5

السؤال التفاعلي الرابع

السؤال التفاعلي الخامس

السؤال التفاعلي السادس

6 حماية الهُويَّة الرقمية تعتمد على تأمين الاتصال بالإنترنت عبر .....

أ. استخدام شبكة المنزل أو البيانات الخلوية

ب. استخدام شبكة Wi-Fi عامة

ج. عدم استخدام VPN حال الاتصال بشبكة عامة

إجابات الأسئلة التفاعلية

01	**إجابة السؤال التفاعلي الأول** د. التواصل مع الجهة الرسمية من خلال موقعها أو الاتصال المباشر
02	**إجابة السؤال التفاعلي الثاني** ب. تُطلَب فيها معلومات حسَّاسة
03	**إجابة السؤال التفاعلي الثالث** ج. التأثير النفسي وبناء الثقة
04	**إجابة السؤال التفاعلي الرابع** د. كل ما سبق
05	**إجابة السؤال التفاعلي الخامس** ج. النَّسخ الاحتياطي للبيانات بشكلٍ دَوريّ
06	**إجابة السؤال التفاعلي السادس** أ. استخدام شبكة المنزل أو البيانات الخلوية

المراجع

1. A Sysmon Incremental Learning System for Ransomware Analysis and Detection, on site: https://arxiv.org/abs/2501.01089
2. Composite Behavioral Modeling for Identity Theft Detection in Online Social Networks, on site: https://arxiv.org/abs/1801.06825
3. Data Encryption Battlefield: A Deep Dive into the Dynamic Confrontations in Ransomware Attacks, on site: https://arxiv.org/abs/2504.20681
4. Identity Theft and Societal Acceptability of Electronic Identity in Europe and the United States, on site: https://arxiv.org/abs/2412.07445
5. NIST SP 800-63-3: Digital Identity Guidelines, on site: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
6. NIST SP 800-63-4: Digital Identity Guidelines, on site: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.pdf
7. NIST SP 800-63A: Enrollment and Identity Proofing Requirements, on site: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63a.pdf
8. NIST SP 800-63B: Authentication and Lifecycle Management, on site: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf
9. Ransomware Analysis Using Feature Engineering and Deep Neural Networks, on site: https://arxiv.org/abs/1910.00286
10. Ransomware Detection and Classification Strategies, on site: https://arxiv.org/abs/2304.04398

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

16555 - 6379 - 51045944

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