الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية
حمايــة البيانـــات والخصوصيــة

الشريحة المستهدفة
المرأة

كُتَيّب المُدَرّب

مبادئ عامة في السلامة الرقمية

حمايـــة البيـانـــات والخصوصيـة

الشريحة المستهدفة

المرأة

كُتَيّب المُدَرّب

تمهيد

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

تم تصميم هذا الكُتَيِّب بهدف توعية المرأة بمبادئ السلامة الرقمية وأفضل الممارسات التي تساعدها على تجنّب المخاطر في البيئة الرقمية.

يهدف هذا الكُتَيّب إلى تعزيز وعي النساء والفتيات بأهمية الأمن الرقمي ودوره في حماية الخصوصية والحياة الرقمية، من خلال التعريف بأبرز المخاطر التي قد تواجههن في بيئة الإنترنت، مثل العنف الإلكتروني، والتحرّش الرقمي، والملاحقة عبر الإنترنت، والتصيّد الاحتيالي، وسرقة الهوية الرقمية، والتزييف العميق.

كما يقدّم الكُتَيّب إرشادات عملية وإجراءات وقائية تساعد المرأة على تأمين أجهزتها الشخصية وحساباتها الإلكترونية، والتصرُّف السليم عند مواجهة أيّ تهديد أو إساءة رقمية، إلى جانب نشر ثقافة الاستخدام الآمِن والمسؤول للتقنية.

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 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

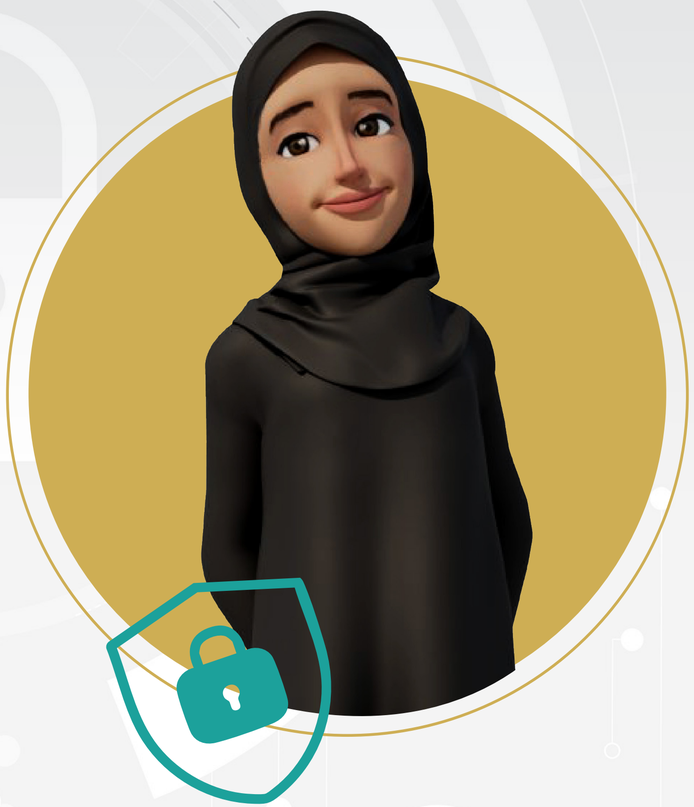
تستهدف المبادرة مختلف شرائح المجتمع، مع تركيزها في السنة الأولى على الشرائح التالية:

- 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

مبـــادئ الأمـــن الرقمـــي

مفهوم الأمن الرقمي

الأمن الرقمي هو القدرة على استخدام التقنيات الحديثة والإنترنت بشكلٍ آمِن ومسؤول يحمي خصوصية المرأة ويصون بياناتها من أيّ تهديد أو إساءة.

يهدف إلى تمكين النساء من التفاعل مع العالم الرقمي بثقة ودون خوف من الاستغلال أو التتبُّع.

- يشمل حماية الأجهزة والبيانات الشخصية
- يُعزّز الثقة في التعامل مع المنصات الإلكترونية
- يَحُدّ من المخاطر قبل وقوعها من خلال الوعي والممارسات الوقائية

أهمية الخصوصية الرقمية

الخصوصية الرقمية تعني الحفاظ على المعلومات الشخصية من الوصول غير المُصرَّح به، سواء من أفراد أو جهات خارجية.

بالنسبة للمرأة، تُعدّ الخصوصية الرقمية أساس الأمان النفسي والاجتماعي.

من وسائل المحافظة على الخصوصية الرقمية

- تجنّب مشاركة الصور والمعلومات الحساسة على المنصات العامة
- عدم قبول طلبات الصداقة من أشخاص مجهولين
- مراجعة إعدادات الخصوصية بانتظام في كلّ تطبيق
- التفكير قبل النشر، فالمحتوى الرقمي لا يختفي بسهولة

الاستخدام الآمِن للأجهزة

الأجهزة الذكية أصبحت جزءًا لا يتجزّأ من حياة المرأة اليومية، لذلك فإنّ تأمينها يُعدّ أولوية.

- قفل الجهاز ببصمة أو كلمة مرور قوية
- تحديث نظام التشغيل والتطبيقات باستمرار
- تفعيل خاصية "العثور على الجهاز" عند الفقدان أو السرقة
- تجنّب تثبيت التطبيقات من مصادر مجهولة

إدارة كلمات المرور

كلمات المرور هي المفتاح الأول لحماية البيانات.

- يجب أن تكون طويلة ومُعقَّدة، وتختلف بين الحسابات
- استخدام برامج إدارة كلمات المرور الآمِنَة
- عدم استخدام المعلومات الشخصية مثل الاسم أو تاريخ الميلاد
- تغيير كلمات المرور بانتظام، خاصةً بعد ملاحظة أيّ نشاط مريب

إعدادات الخصوصية

وسائل التواصل تُمثِّل مساحة للتعبير، لكنّها أيضًا بيئة مفتوحة قد تُعرِّض المرأة للمخاطر إذا لم يتم إدارتها بوَعْي.

- تفعيل المصادقة الثنائية لحماية الحسابات
- تحديد مَن يمكنه رؤية المنشورات والتفاعل معها
- إلغاء أذونات التطبيقات غير الموثوقة المرتبطة بالحساب
- تجنّب مشاركة الموقع الجغرافي في أثناء التنقل أو السفر
- مراجعة إعدادات الحسابات الاجتماعية، وتحديد مَن يمكنه رؤية المنشورات
- حَصْر قبول طلبات الصداقة بالأشخاص المعروفين
- عدم مشاركة تفاصيل الحياة اليومية بشكلٍ متكرّر

حماية البيانات

تُعدّ الصور والمحادثات العائلية من أكثر أنواع البيانات حساسية.

- استخدام تطبيقات مراسلة آمِنَة بتقنية التشفير الطرفي
- حَذْف الرسائل القديمة، أو التي تتضمَّن بيانات شخصية
- تجنّب إرسال الصور أو المستندات الحساسة عبر البريد أو الرسائل العامة
- الاحتفاظ بنُسَخ احتياطية مُشفَّرة للبيانات الهامة
- عدم تخزين الصور الحساسة على الأجهزة المتصلة بالإنترنت
- استخدام تطبيقات تشفير لحِفْظ الصور الخاصة
- حَذْف الصور المُكرَّرة أو غير الضرورية بانتظام

تعزيز الثقافة الرقمية

نَشْر الوعي الرقمي داخل الأسرة يخلق بيئة آمِنَة للجيل الجديد من الفتيات.

- تعليم البنات أساسيات الخصوصية والأمان عند استخدام الإنترنت
- متابعة التطبيقات والألعاب التي تَستخدمها الفتيات الصغيرات
- تشجيع الحوار المفتوح حول التحديات الرقمية
- المشاركة في وِرَش التوعية الرقمية النسائية

السؤال التفاعلي الأول

1 ما أفضل ممارسة لحماية حساباتك الرقمية؟

أ. استخدام كلمة مرور واحدة لكل الحسابات

ب. تفعيل المصادقة الثنائية، وتغيير كلمة المرور دوريًّا

ج. مشاركة كلمة المرور مع صديقة موثوقة

د. ترك الحسابات مفتوحة على الأجهزة العامة

المحور الثاني

التحرُّش الرقمي والمُلاحَقة

العنف الإلكتروني وأشكاله

العنف الإلكتروني هو أيّ سلوك عدائي أو تهديدي يُمارَس عبر الإنترنت أو المنصات الرقمية ضد النساء.

يهدف إلى إيذائهن نفسيًّا أو اجتماعيًّا أو حتى ماديًّا؛ من خلال استخدام التكنولوجيا كسلاح.

يشمل التهديد، العنف، التشهير، أو المُلاحَقة الإلكترونية

ينتشر في وسائل التواصل والمراسلات الخاصة

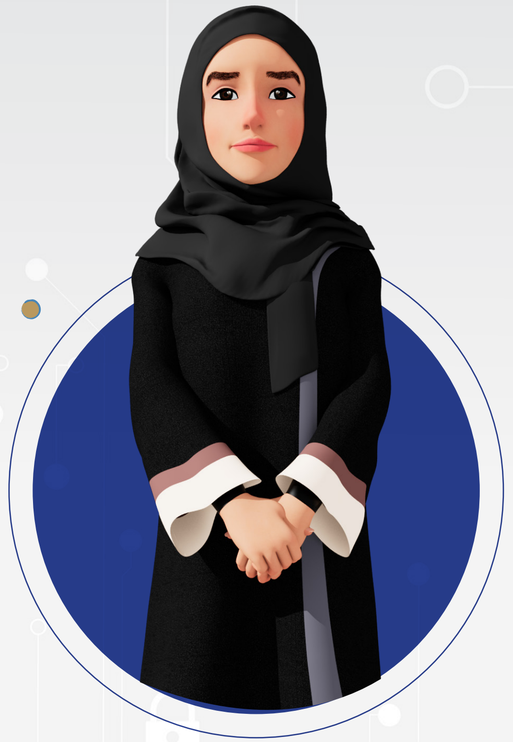
يترك آثارًا عميقة على الضحايا نفسيًّا واجتماعيًّا

التحرُّش الرقمي

يُعدّ التحرُّش الرقمي أحد أكثر أشكال العنف انتشارًا ضد النساء في الفضاء السيبراني

قد يكون عبر رسائل غير مرغوبة، صور مسيئة، أو تعليقات جارحة

أحيانًا يَتخفَّى المُتحرِّش خلف حسابات وهمية



تجاهل الرسائل المسيئة، وحظر المُرسِل خطوة أُولى مُهمة

يمكن الإبلاغ عن المتحرشين عبر أدوات الإبلاغ داخل المنصات

المُلاحَقة الإلكترونية

هي مُراقَبة شخص بشكلٍ مُتكرّر عبر الإنترنت دون إذنه.
قد تبدأ برسائل أو تعليقات بسيطة، ثم تتطوَّر إلى تهديد أو تتبُّع دائم.

راقبي مَن يتفاعل مع منشوراتك بشكل غير طبيعي

تجنّبي مشاركة موقعك الجغرافي بشكلٍ عام

احتفظي بالأدلة الرقمية لتوثيق الحالة

أبْلِغي الجهات المختصة إذا شعرتِ بأنكِ مُلاحَقة

المؤشرات التحذيرية للمُلاحَقة

التعرُّف المُبكّر على العلامات التحذيرية يساعد في الحدّ من الضرر.

- رسائل متكررة وغير مرغوبة من الشخص نفسه
- محاولات للوصول إلى معلوماتك الشخصية أو صورك
- تهديدات مباشرة أو ضمنية
- تعليقات تسيء إلى سُمعتك أو تحاول ترهيبك

آليَّات التعامل مع التهديدات

المعرفة المسبقة بخطوات التصرُّف تُمكِّن المرأة من السيطرة على الموقف.

التبليغ الفوري عن الحساب أو الرسائل المسيئة

حَظْر المستخدم المسيء، وعدم الردّ عليه إطلاقًا

التواصل مع الدعم الفني للمنصة

إبلاغ الجهات الأمنية إذا تطوَّر التهديد إلى عنف أو مُلاحَقة

توثيق الأدلة الرقمية

توثيق الأدلة يُعدّ أهمّ خطوة قانونية في التعامل مع العنف الإلكتروني.

- تصوير الشاشة مع حفظ التاريخ والوقت
- حفظ روابط الصفحات والمحادثات الأصلية
- عدم حذف الرسائل أو الحساب المسيء
- التواصل مع الجهات المختصة في الدولة

السؤال التفاعلي الثاني

2 أيٌّ من التصرُّفات التالية يُعتَبر تصرُّفًا صحيحًا عند التعرُّض للتحرش الإلكتروني؟

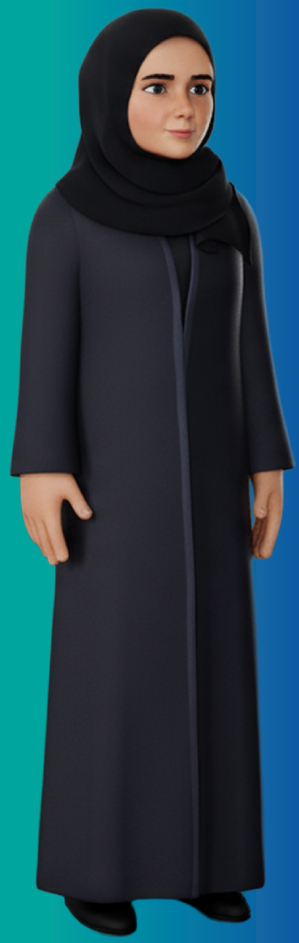
أ. حذف الرسائل فورًا

ب. الرد، ومحاولة التفاوض

ج. حفظ الأدلة، والإبلاغ عن الحادثة للجهات المختصة

د. تجاهل الرسائل، وعدم إخبار أحد

السؤال التفاعلي الثالث



3 ما أفضل إجراء عند ملاحظة وجود شخص يُراقب نشاطك باستمرار على الإنترنت؟

أ. مَنْحه فرصة لتوضيح موقفه

ب. حَظْره فورًا، وتفعيل إعدادات الخصوصية والإبلاغ عنه

ج. الرد عليه لتخويفه

د. تجاهله ومُواصلة النشر كالمعتاد

المحور الثالث

التهديدات الرقمية وأساليب الوقاية

التصيّد الاحتيالي

يُعدّ التصيّد الاحتيالي من أكثر أساليب الخداع شيوعًا، ويَعتمد على إرسال رسائل أو روابط تبدو حقيقية، لكنّها تهدف إلى سرقة المعلومات.

تأتي الرسائل الاحتيالية عادة عبر البريد الإلكتروني أو الرسائل النصية أو مواقع مزيَّفة

تطلب الرسائل الاحتيالية إدخال بيانات مثل كلمات المرور أو أرقام البطاقات

تعتمد على أسلوب الإقناع باستخدام عبارات مستعجلة أو تهديدية

يجب تجاهل الرسائل المشبوهة، والتحقُّق من مصدرها قبل أيّ تفاعل

الروابط والمواقع المُزيَّفة

تنتشر المواقع المزيَّفة التي تُحاكي واجهات المتاجر أو المؤسسات الرسمية لخداع المستخدمين.

قد تحمل أسماء نطاق شبيهة بالمواقع الأصلية مع تغييرات طفيفة

تُستخدم لجمع بيانات تسجيل الدخول أو معلومات الدفع

يمكن التحقق من موثوقية الموقع عبر عنوانه (URL) أو الشهادة الأمنية (https)

يُفضَّل الوصول للمواقع مباشرة من مُحرّك البحث وليس من روابط مرسلة

برمجيات الفدية

هي برمجيات خبيثة تقوم بتشفير الملفات، وتطلب فدية مالية مقابل فكّ التشفير.

تصل غالبًا عبر مُرفقات البريد أو روابط مشبوهة

بعد الإصابة، يُمنَع المستخدِم من الوصول إلى ملفاته

حتى بعد الدفع، لا يُوجد ضمان لاسترجاع البيانات

الوقاية تكون من خلال النَّسخ الاحتياطي المنتظم، وتجنّب المرفقات المجهولة

البرمجيات الخبيثة

تشمل مجموعة من البرمجيات التي تُزْرَع داخل الأجهزة بغرض التخريب أو سرقة البيانات.

تتسبَّب في بُطْء النظام أو سرقة كلمات المرور أو مراقبة الأنشطة

قد تَختبئ في تطبيقات أو ملفات تبدو طبيعية

تجنّب تحميل البرامج من مواقع غير موثوقة

يمكن الوقاية منها عبر تثبيت برامج مكافحة الفيروسات وتحديثها باستمرار

الهندسة الاجتماعية

يستهدف المهاجمون من خلالها سلوك الإنسان بدل الثغرات التقنية، عبر الخداع والتلاعُب النفسي.

- قد يتظاهر المهاجِم بأنّه موظف دعم، أو ينتمي إلى جهة رسمية
- يجمع المعلومات من حسابات التواصل لبناء الثقة، ومِن ثَمَّ الخداع
- يستخدم أساليب عاطفية؛ مثل: الاستعجال أو الإلحاح، للحصول على معلومات مُهِمَّة
- يُنصَح بعدم مشاركة أيّ بيانات دون تحقُّق من هوية الطرف المقابل

التزييف العميق

تقنية قائمة على الذكاء الاصطناعي تُستخدَم لتوليد صور أو فيديوهات مُزيَّفة تُشْبِه الحقيقية بشكل كبير.

يمكن أن تُستخدَم لانتحال الهوية أو نَشْر محتوى مُضلّل

يصعب على المستخدِم العادي اكتشافها دون أدوات تحليل

يُنصَح بعدم إعادة نشر أيّ محتوى قبل التحقُّق من مصدره

استخدام أدوات كشف التزييف، وبرامج تحليل الوسائط الرقمية

سرقة الهوية الرقمية

تحدث عندما يتمكَّن أحدهم من الحصول على معلومات شخصية واستخدامها باسم الضحية.

تشمل سرقة الحسابات، أرقام البطاقات، أو البريد الإلكتروني

قد تُستخدَم البيانات في عمليات احتيال مالي أو اجتماعي

تقليل مشاركة البيانات الشخصية يُقلِّل من احتمالية التعرض لسرقة الهوية

المراقبة الدورية للنشاطات المالية تساعد في الاكتشاف المبكّر

الرسائل الاحتيالية عبر الهاتف

هي شكل من أشكال التصيّد يَستخدم الرسائل النصية القصيرة وسيلةً للخداع.

تحتوي على روابط تدّعي تقديم جوائز أو تحديث البيانات البنكية

النقر عليها قد يؤدي إلى سرقة البيانات، أو تثبيت برمجيات ضارّة

يُنصَح بعدم فتح أيّ رابط من مُرسِل غير معروف

التواصل مباشرة مع الجهة الرسمية؛ للتأكد من مصداقية الرسالة

مخاطر التطبيقات المجانية

تُقدّم بعض التطبيقات خدمات جذّابة، لكنّها تجمع بيانات المستخدِمين دون تصريح واضح.

تطلب أذونات كثيرة تتجاوز حاجتها الفِعْلية

قراءة سياسة الخصوصية قبل التثبيت خطوة أساسية

قد تتابع الموقع أو تسجّل الأنشطة في الخلفية

حذف التطبيقات غير الضرورية أو المشبوهة بشكل دوري

البرمجيات المزيّفة لتحديث النظام

يلجأ المهاجمون إلى إرسال إشعارات مُزيَّفة تُوهِم المستخدِم بأنّ جهازه يحتاج إلى تحديث فوري.

- بمجرد الضغط على الرابط، تُنزَّل برمجيات ضارَّة
- يجب اعتماد التحديثات الرسمية فقط من إعدادات الجهاز
- عدم تحميل أيّ ملف تنفيذي من بريد إلكتروني أو موقع مجهول
- تحديث النظام بانتظام يُغْلِق الثغرات الأمنية

التخزين السحابي

يُعدّ التخزين السحابي وسيلة مريحة، لكنّه قد يصبح خطرًا إذا أُسيء استخدامه.

- رفع الملفات الحساسة دون تشفير يُعرِّضها للسرقة
- مشاركة روابط عامة قد تمنح الآخرين صلاحية الوصول غير المقصود
- يُنصَح باستخدام خدمات سحابية موثوقة، وتفعيل المصادقة الثنائية
- حذف الملفات القديمة من الحسابات السحابية بانتظام

الإعلانات المُضلّلة

تُستخدَم بعض الإعلانات المُموَّلة على الإنترنت وسيلةً لنشر الروابط الخبيثة.

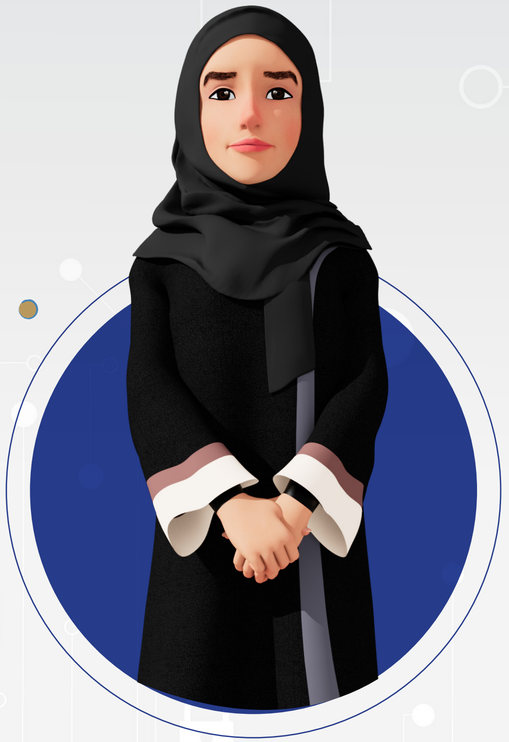
- قد تَدَّعي تقديم خصومات أو فُرَص ربح فورية
- النقر عليها يؤدّي إلى صفحات تحمّل برمجيات غير آمِنَة
- تجنّب الضغط على الإعلانات غير الموثوقة أو المثيرة للفضول
- استخدام إضافات حَجْب الإعلانات على المتصفّح يُعزّز الأمان

التحديثات الأمنية

تُعدّ التحديثات الدورية خطّ الدفاع الأخير ضدّ التهديدات الجديدة.

تحتوي التحديثات على تصحيحات لثغرات تُستغَل في الاختراقات

تأجيل التحديثات يجعل الجهاز عُرْضَة للبرمجيات الحديثة



تفعيل خاصية التحديث التلقائي لجميع التطبيقات والأنظمة

إعادة تشغيل الجهاز بعد التحديث؛ لضمان تثبيت الحماية بالكامل

السؤال التفاعلي الرابع

4 أيّ مِن العبارات التالية يُعبِّر عن أسلوب "الهندسة الاجتماعية"؟

أ. استخدام برامج لتشفير الملفات

ب. إقناع المستخدم بمشاركة معلوماته طوعًا عبر الخداع

ج. اختراق النظام عبر ثغرة تقنية

السؤال التفاعلي الخامس

5 ما الإجراء الأفضل لتجنُّب الإصابة ببرمجيات الفدية؟

أ. إجراء نَسْخ احتياطي منتظم، وتجنّب المرفقات المشبوهة

ب. فتح المرفقات من أيّ بريد وارد

ج. تجاهل النسخ الاحتياطي للملفات

د. تثبيت أيّ برنامج مجاني متاح على الإنترنت

إجابات الأسئلة التفاعلية

01 **إجابة السؤال التفاعلي الأول**

ب. تفعيل المصادقة الثنائية، وتغيير كلمة المرور دوريًّا

02 **إجابة السؤال التفاعلي الثاني**

ج. حفظ الأدلة، والإبلاغ عن الحادثة للجهات المختصة

03 **إجابة السؤال التفاعلي الثالث**

ب. حظره فورًا، وتفعيل إعدادات الخصوصية والإبلاغ عنه

04 **إجابة السؤال التفاعلي الرابع**

ب. إقناع المستخدِم بمشاركة معلوماته طوعًا عبر الخداع

05 **إجابة السؤال التفاعلي الخامس**

أ. إجراء نَسْخ احتياطي منتظم، وتجنّب المرفقات المشبوهة

المراجع

1. ernest, nonum et al. SOCIAL ENGINEERING: UNDERSTANDING HUMAN FACTORS IN CYBER SECURITY. International Journal of Convergent and Informatics Science Research. May 2025, on site: https://harvardpublications.com/hijcisr/article/view/326
2. eSafety Commissioner (Australia). Staying safe: Cyberstalking, on site: https://www.esafety.gov.au/key-topics/staying-safe/cyberstalking
3. European Institute for Gender Equality. Cyber violence against women, on site: https://www.eige.europa.eu/gender-based-violence/cyber-violence-against-women
4. European Parliament. (2023). IPOL_STU(2023)743341_EN [PDF]. on site: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/743341/IPOL_STU(2023)743341_EN.pdf
5. IBM. What is malware?, on site: https://www.ibm.com/think/topics/malware
6. Karnouskos, Stamatis. Artificial Intelligence in Digital Media: The Era of Deepfakes, IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY, June 2020, on site: https://ieeexplore.ieee.org/document/9123958
7. Kosinski, Matthew. IBM. What is phishing?, on site: https://www.ibm.com/think/topics/phishing
8. Kosinski, Matthew. IBM. What is ransomware? Retrieved, on site: https://www.ibm.com/think/topics/ransomware
9. National Cyber Security Centre. Password policy: updating your approach. November 2018, on site: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
10. Startup Defense. Fake software update prompts. on site: https://www.startupdefense.io/cyberattacks/fake-software-update-prompts
11. UN Women. FAQs: Digital abuse, trolling, stalking and other forms of technology-facilitated violence against women. February 2025, on site: https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women
12. United Nations Office on Drugs and Crime. Handling of digital evidence (Module 6), on site: https://www.unodc.org/e4j/ar/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

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