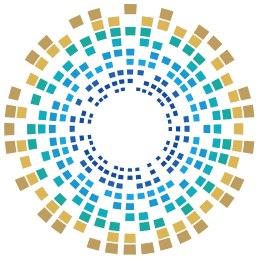
مبادئ عامة في السلامة الرقمية

هي السيبرانية

الشريحة المستهدفة
المرأة

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مبـــادئ عامـــة فـي السلامـــة الرقميـة هي السيبرانية

الشريحة المستهدفة

المرأة

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

حقوق الملكية الفكرية

المادة مملوكة للوكالة الوطنية للأمن السيبراني في دولة قطر، وكافة حقوق الملكية الفكرية التي تشمل حق المؤلف وحقوق التأليف والنشر والطباعة، كُلّها مكفولة للوكالة الوطنية للأمن السيبراني في دولة قطر.

وعليه فجميع الحقوق محفوظة للوكالة، ولا يجوز إعادة نشر أي أجزاء من هذا الكُتَيّب، أو الاقتباس منه، أو نَسْخ أيّ جزء منه، أو نقله كليًّا أو جزئيًّا في أيّ شكلٍ وبأيّ وسيلة، سواء بطُرق إلكترونية أو آلية، بما في ذلك التصوير الفوتوغرافي، أو التسجيل، أو استخدام أي نظام من نُظُم تخزين المعلومات واسترجاعها، سواء من الأنظمة الحالية أو المُبتكَرة في المستقبل؛ إلا بعد الرجوع إلى الوكالة، والحصول على إذنٍ خَطّي منها.

ومَن يُخالِف ذلك يُعرّض نفسه للمُساءَلة القانونية.

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

00974 404 663 62

00974 404 663 79

academy@ncsa.gov.qa

www.ncsa.gov.qa

تمهيـــد

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 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.

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

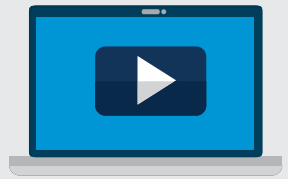
أدوات التوعية

تعتمد المبادرة على أدوات توعية متنوّعة ومتكاملة، تشمل ما يلي:

دليل السلامة الرقمية

كتيبات توعية

ألعاب سيبرانية



فيديوهات توعية

ألعاب تعليمية مبتكَرة

ورش توعية

01 المحور الأول

أساسيات السلامة الرقمية

مفهوم السلامة الرقمية

السلامة الرقمية هي مجموعة من الممارسات والإجراءات التي تهدف إلى حماية المعلومات الشخصية، وضمان الاستخدام الآمِن للتقنيات الحديثة.

يُسهم هذا المفهوم في تمكين النساء من التفاعُل مع العالم الرقمي بثقة ودون خوف من الاستغلال أو التتبُّع.

أبرز أهداف السلامة الرقمية

1. حماية البيانات من الوصول أو الاستخدام غير المصرّح به
2. تمكين المستخدمين من التفاعل مع الإنترنت بثقة ومسؤولية
3. الوقاية من الجرائم الإلكترونية كالتصيّد والاختراق والتحرُّش
4. نَشْر ثقافة الوعي بالأمن السيبراني في المجتمع
5. تقوية القُدرة على التمييز بين المحتوى الموثوق والمُضلّل
6. دعم الممارسات الوقائية قبل وقوع المخاطر الرقمية

الوعي بالأمن السيبراني

يُعدّ الوعي الذاتي أساس الحماية الرقمية؛ إذ يساعد على اتخاذ قرارات سليمة في أثناء استخدام الإنترنت.
كلّ سلوك واعٍ يُسهم في خَفْض احتمالية التعرُّض للمخاطر السيبرانية.

التفكير المسبق قبل نشر أو مشاركة أيّ محتوى

الابتعاد عن الروابط أو المرفقات مجهولة المصدر

تجنّب استخدام شبكات Wi-Fi العامة في المعاملات المالية

الاطلاع على المستجدّات الأمنية بشكلٍ دوريّ لفَهْم التهديدات الحديثة

تفادي إدخال البيانات الشخصية في مواقع غير موثوقة

قراءة التحذيرات الأمنية وعدم تجاوزها دون انتباه

الحرص على تحميل البرامج والتطبيقات من المصادر الرسمية فقط

حماية الخصوصية الرقمية

تُمثّل الخصوصية الرقمية صمام الأمان في عالم مترابط تُتداول فيه البيانات بسرعة.
وتعني السيطرة على المعلومات الشخصية، وتحديد مَن يمكنه الوصول إليها أو استخدامها.
بالنسبة للمرأة، تُعدّ الخصوصية الرقمية أساس الأمان النفسي والاجتماعي.

إجراءات الحفاظ على الخصوصية

- مراجعة إعدادات الخصوصية في جميع التطبيقات بانتظام
- حذف الصور والمنشورات القديمة أو غير الضرورية
- تقييد إمكانية مشاهدة المنشورات أو التعليقات على الحسابات الاجتماعية
- عدم مشاركة تفاصيل الحياة اليومية باستمرار
- الامتناع عن مشاركة الموقع الجغرافي في أثناء التنقل أو السفر
- قبول طلبات الصداقة فقط من الحسابات المعروفة والمحقّقة
- استخدام أسماء حسابات لا تتضمَّن معلومات شخصية واضحة
- تجنُّب التسجيل في المواقع التي تطلب بيانات غير ضرورية

تأمين الأجهزة

تُمثّل الأجهزة الذكية البوابة الرئيسة للدخول إلى العالم الرقمي، ما يجعل حمايتها أمرًا بالغ الأهمية.

أبرز خطوات تأمين الأجهزة

- استخدام قفل آمِن يعتمد على كلمة مرور قوية أو بصمة حيوية
- تحديث نظام التشغيل والتطبيقات بشكلٍ دوري لسدّ الثغرات الأمنية
- تفعيل خاصية "العثور على الجهاز"؛ لتحديد الموقع في حال الفقدان
- حذف التطبيقات غير الموثوقة، أو التي تطلب صلاحيات مُبَالغًا فيها
- تعطيل الاتصال التلقائي بالشبكات اللاسلكية العامة
- تثبيت برامج الحماية من الفيروسات وتحديثها باستمرار
- حِفْظ الملفات الحساسة في مساحات تخزين مشفَّرة
- استخدام جدار الحماية لتقليل احتمالات الاختراق

إدارة كلمات المرور

تُمثّل كلمة المرور خط الدفاع الأول ضد أيّ محاولة للوصول غير المُصرَّح به.

وتعتمد قوة الحماية الرقمية على مدى صلابة كلمات المرور وسلامة إدارتها.

طرق إنشاء وإدارة كلمات المرور

1. الاعتماد على كلمات طويلة؛ تحتوي على رموز وأرقام وحروف متنوعة
2. استخدام كلمة مرور مختلفة لكل حساب أو خدمة رقمية
3. تجنُّب استخدام المعلومات الشخصية أو الكلمات الشائعة
4. تغيير كلمات المرور بشكل دوري، خاصةً بعد أيّ نشاط مشبوه
5. الاستعانة ببرامج موثوقة لإدارة كلمات المرور وحفظها بأمان
6. تجنُّب حفظ كلمات المرور في المتصفحات أو الأجهزة العامة
7. تسجيل الخروج من الحسابات بعد الانتهاء من الاستخدام

حماية البيانات والمحتوى

البيانات الشخصية تُمثِّل ثروة رقمية ينبغي التعامل معها بحذر، فالتهاون في تخزينها أو مشاركتها يفتح الباب أمام الاستغلال والاختراق.

إرشادات لضمان سلامة البيانات

1. استخدام تطبيقات تراسل تدعم التشفير من طرف إلى طرف
2. عدم إرسال الصور أو المستندات الحساسة عبر البريد أو المحادثات العامة
3. إنشاء نُسَخ احتياطية مُشفَّرة للملفات المُهمَّة بشكلٍ منتظم
4. حذف الرسائل القديمة أو التي تحتوي على بيانات شخصية
5. تخزين الملفات الخاصة في وسائط غير متصلة بالإنترنت
6. استخدام برامج تشفير متقدمة لحماية الصور والمستندات
7. التأكُّد من مَسْح البيانات نهائيًّا قبل بيع أو إعادة تهيئة الأجهزة

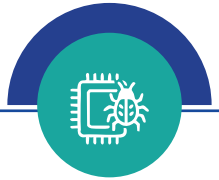
التعامل مع التهديدات الرقمية

التعامل الهادئ والمنهجي مع أيّ خطر رقمي يُقلّل من آثاره المحتملة، فردّ الفعل الصحيح هو الخطوة الأولى نحو الحل.

إجراءات التصرف عند مواجهة تهديد رقمي

توثيق الرسائل أو المحتوى المسيء عبر لقطات الشاشة

عدم الرد على الرسائل العدائية أو مجهولة المصدر



حظر الحسابات المشبوهة فورًا

تغيير كلمات المرور، وتأمين الحسابات المتأثرة

التواصل مع الجهات المختصة أو فِرَق الدعم الفني للمنصات

الاحتفاظ بالأدلة الرقمية تحسبًا لأيّ متابعة قانونية

الممارسات المستدامة للأمان الرقمي

تحقيق الأمان الرقمي ليس عملية مؤقّتة، بل إجراءات تُمارَس باستمرار.
الاستمرارية في تطبيق الإجراءات الوقائية تضمن استقرار البيئة الرقمية على المدى الطويل.

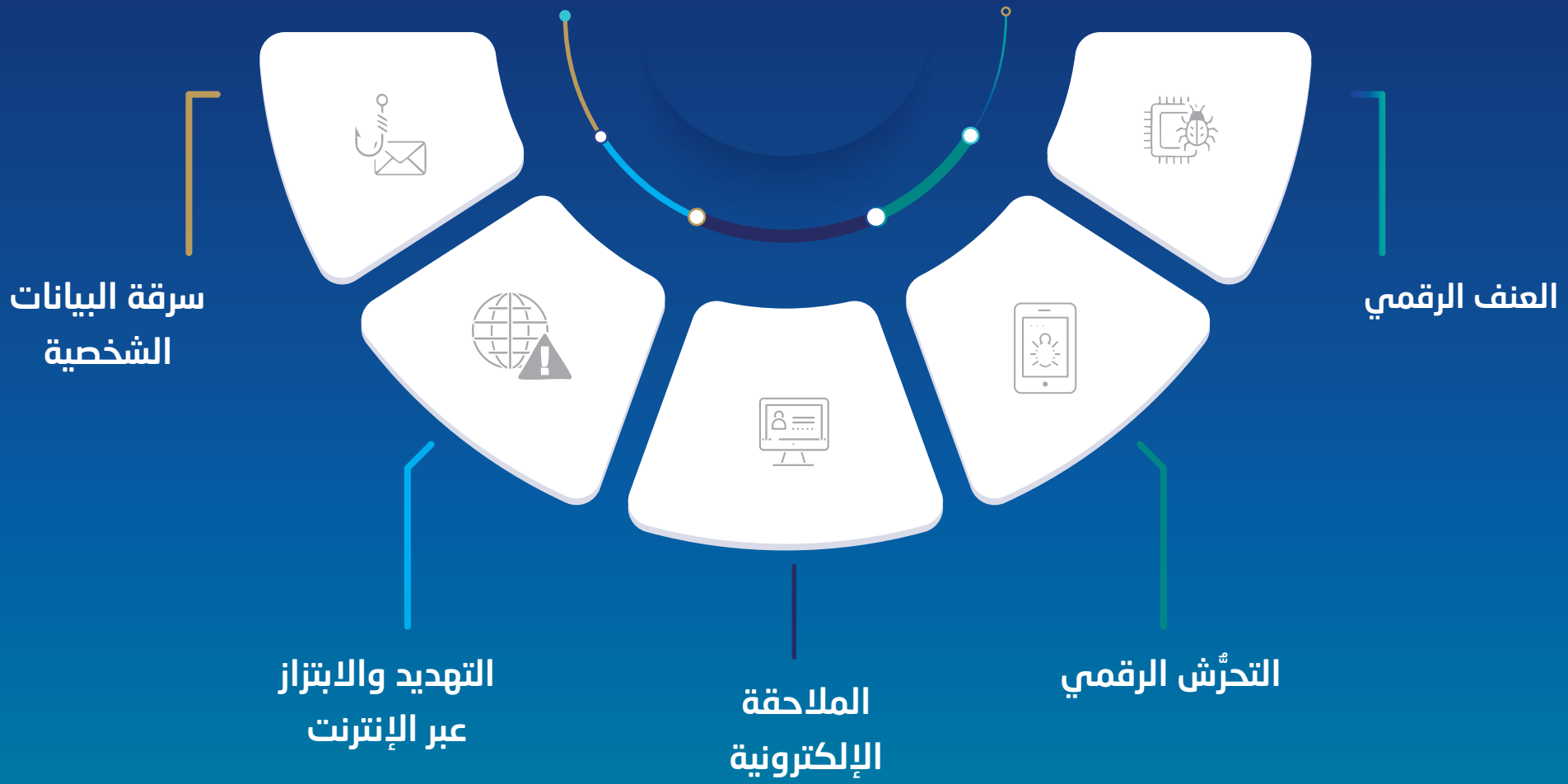
ممارسات وقائية دائمة

- تحديث الأنظمة والتطبيقات فور صدور النُّسَخ الجديدة
- مراجعة إعدادات الأمان شهريًّا
- استخدام المصادقة الثنائية في جميع الحسابات الحساسة
- مراقبة الأنشطة غير المألوفة في الحسابات أو الأجهزة
- نشر الوعي بين الأصدقاء والزملاء حول أهمية الحماية الرقمية
- تبنّي ثقافة «التفكير قبل النقر» في جميع التفاعلات الإلكترونية

02 المحور الثاني

السلوك الآمِن في الفضاء السيبراني

التهديدات الرقمية التي تُواجِه النسـاء والفتيات



مفهوم السلوك الرقمي الآمِن

السلوك الآمِن في الفضاء الإلكتروني هو مجموعة من الممارسات الواعية التي تهدف إلى استخدام التكنولوجيا والإنترنت بطريقة مسؤولة تُقلّل من المخاطر، وتحافظ على الخصوصية والسلامة الرقمية للنساء والفتيات.

يشمل التصرُّف الواعي عند التعامل مع المعلومات أو المحتوى المنشور على المنصات

يرتكز على الوعي بالحقوق والواجبات داخل الفضاء السيبراني

يُعدّ أساسًا لبناء بيئة رقمية آمِنَة تسودها الثقة والاحترام المتبادل

يُسْهِم في الحدّ من الجرائم السيبرانية التي تنشأ من السلوك غير المسؤول

إدارة المعلومات الشخصية

المعلومات الشخصية تُعدّ أثمن ما يُمْلَك في البيئة الرقمية، وحمايتها مسؤولية مستمرة.

1. عدم الإفصاح عن البيانات الحساسة في المحادثات أو التعليقات العامة
2. استخدام البريد الإلكتروني الرسمي في التعاملات المهنية فقط
3. التحقُّق من سياسات الخصوصية قبل تقديم أيّ معلومات عبر الإنترنت
4. تخزين البيانات المهمة في أماكن آمِنَة ومشفَّرة
5. حذف المعلومات القديمة أو غير الضرورية بانتظام

الاستخدام الآمِن للأجهزة والتطبيقات

الاستخدام الذكي للأجهزة يَحُدّ من فُرَص التعرُّض للاختراق أو فقدان البيانات.

- تثبيت برامج موثوقة فقط من المتاجر الرسمية
- تفعيل القفل التلقائي وكلمات المرور المُعقَّدة
- عدم مشاركة الأجهزة أو الحسابات مع الآخرين دون حاجة
- تجنُّب الاتصال بشبكات الإنترنت العامة غير الآمِنَة
- مراقبة أذونات التطبيقات، والتأكُّد من توافقها مع طبيعة عملها

العنف الإلكتروني

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.

1 يشمل التهديد، الابتزاز، التشهير، ونشر محتوى مسيء

2 يمكن أن يكون مُوجَّهًا بشكل مباشر أو غير مباشر من خلال الرسائل أو التعليقات

3 يترك آثارًا نفسية عميقة؛ مثل: القلق والاكتئاب، وانخفاض الثقة بالنفس

4 يزيد العنف الإلكتروني من الشعور بالعزلة والانفصال عن المجتمع الرقمي

5 يتطلب وعيًا مجتمعيًّا للتعرُّف عليه، والحد من انتشاره

التحرُّش الرقمي

التحرُّش الرقمي أحد أكثر أشكال العنف الإلكتروني انتشارًا، ويَستهدف غالبًا النساء والفتيات.

01 يتمثّل في الرسائل غير المرغوبة، الصور أو الفيديوهات المسيئة، والتعليقات الجارحة

02 قد يَستخدم المتحرّشون حسابات وهمية لإخفاء هويتهم الحقيقية

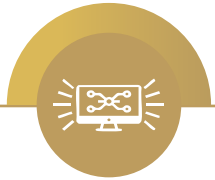
03 يمكن أن يكون التحرش عبر البريد الإلكتروني، وسائل التواصل الاجتماعي، أو تطبيقات المراسلة

04 يُسبّب التحرش الرقمي تراجعًا في الحرية الرقمية والثقة في استخدام الإنترنت

05 تجاهل الرسائل المسيئة، أو حظر المُرسِل؛ يُشكّل خطوة أولية مُهمَّة للحدّ من الأذى

الملاحقة الإلكترونية

الملاحقة الإلكترونية تعني مُتابَعة شخص بشكلٍ مُتكرّر عبر الإنترنت دون إذنه. وقد تتطوَّر من تفاعلات بسيطة إلى تهديد دائم.

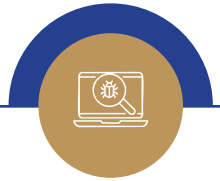


تشمل مراقبة المنشورات، التعليقات، أو المواقع التي يزورها المستخدِم

قد تبدأ بمحاولات جَمْع معلومات شخصية، ثم تتصاعد إلى تهديدات مباشرة

تسبّب الملاحقة الإلكترونية شعورًا دائمًا بالخوف وفقدان الأمان الرقمي

تُشكِّل تهديدًا للخصوصية الشخصية والاجتماعية، وتَحُدّ من حرية الحركة الرقمية



حفظ الأدلة الرقمية والإبلاغ عن الجهات المختصة يُقلِّل من آثار الملاحقة

الوقاية من العنف والتحرُّش

التعامل الواعي مع العنف والتحرش الإلكتروني يُقلِّل من مخاطرهما ويَحُدّ من انتشارهما.

1. استخدام أدوات الحظر والتقارير داخل المنصات الرقمية عند التعرُّض لأيّ تهديد
2. حماية المعلومات الشخصية، وتجنُّب مشاركة الموقع الجغرافي أو البيانات الحساسة
3. مراجعة إعدادات الخصوصية بشكلٍ دوري لتقليل المخاطر
4. الاحتفاظ بالأدلة الرقمية؛ مثل: الرسائل، أو لقطات الشاشة؛ لتسهيل التوثيق القانوني
5. اللجوء إلى الجهات المختصة أو الدعم النفسي عند تفاقم الموقف
6. نَشْر الوعي بين المجتمع حول مخاطر العنف والتحرش الرقمي وأساليب الوقاية

03 المحور الثالث

التهديدات الرقمية وأساليب الوقاية

مفهوم التهديدات الرقمية

التهديدات الرقمية هي مجموعة من المخاطر التي تَستهدف الأجهزة أو البيانات أو الهوية الإلكترونية، وتتنوع في أساليبها ودرجات خطورتها.

تشمل البرمجيات الخبيثة، الاختراقات، الاحتيال، وانتحال الهوية

تتطور باستمرار مع تطور التقنية وأساليب الذكاء الاصطناعي

تُصيب الأفراد والمؤسسات على حدّ سواء، وغالبًا تبدأ بخطأ بسيط من المستخدِم

تهدف إلى سرقة المعلومات، تعطيل الأنظمة، أو ابتزاز الضحايا

الوعي والوقاية يُمثّلان الركيزة الأساسية لمواجهتها

التصيّد والاحتيال السيبراني

التصيّد الاحتيالي من أكثر الهجمات انتشارًا، ويعتمد على الخداع لإقناع المستخدِم بتقديم بياناته طوعًا.

01 يظهر عادة عبر البريد الإلكتروني أو الرسائل النصية أو الإعلانات الزائفة

02 يستخدم المهاجمون عبارات طارئة مثل «تحديث الحساب» أو «إغلاق البطاقة البنكية»

03 تتضمَّن الرسائل روابط مُزيَّفة تؤدي إلى مواقع تحاكي الأصلية

04 يتم جمع كلمات المرور أو المعلومات البنكية بمجرد التفاعل مع الرابط

05 الوقاية تتم بتجاهل الرسائل المشبوهة، والتحقُّق من هوية المرسل رسميًّا

06 استخدام المصادقة الثنائية يُقلِّل من فُرَص نجاح الهجمات الاحتيالية

البرمجيات الخبيثة

البرمجيات الخبيثة هي أدوات رقمية ضارَّة تُزْرَع داخل الأجهزة بهدف التخريب أو السرقة. وتُعدّ برمجيات الفدية أخطر أنواعها.

01

تنتقل عبر المرفقات، التطبيقات المقرصنة، أو مواقع غير آمِنَة

02

برمجيات الفدية تقوم بتشفير الملفات والمطالبة بمبلغ مالي لفك التشفير

03

تُظهر الأجهزة المصابة بُطْئًا أو سلوكًا غريبًا عند التشغيل

04

حتى بعد دَفْع الفدية، لا يوجد ضمان لاستعادة البيانات

05

الحماية تتطلب نُسَخًا احتياطية مُشفَّرة، وتحديث برامج الحماية باستمرار

06

تجنّب تثبيت أيّ ملف أو تطبيق من مصادر مجهولة

انتحال الهوية

انتحال الهوية يحدث عندما يتم استخدام معلومات شخص ما دون إذنه.

1. تتضمّن البيانات المستهدَفة: الصور، أرقام البطاقات، أو الحسابات الاجتماعية
2. تُستخدَم المعلومات المسروقة في الاحتيال المالي أو التشهير أو الابتزاز
3. الانتشار الكبير للمحتوى الشخصي يُسهِّل عمليات الانتحال
4. يمكن اكتشاف بعض الحالات من خلال إشعارات الدخول أو محاولات التحقُّق غير المعتادة
5. تقليل مشاركة البيانات الحساسة وإدارة كلمات المرور بوَعْي يَمْنع الانتحال
6. متابعة النشاطات الإلكترونية للحسابات بشكلٍ دوريّ تكشف التهديدات مبكرًا

التزييف العميق

التزييف العميق تقنية تعتمد على الذكاء الاصطناعي لإنشاء صور أو مقاطع فيديو مُزيَّفة يَصْعُب تمييزها عن الأصلية.

1. تُستخدَم أحيانًا لتشويه السُّمعة أو ابتزاز الأفراد
2. تنتشر بسرعة عبر وسائل التواصل بسبب طابعها الصادم
3. يمكن أن تُؤثِّر على الرأي العام، وتخلق أزمات اجتماعية أو سياسية
4. الوقاية تتطلب التحقُّق من المصدر قبل إعادة النشر أو المشاركة
5. استخدام أدوات كشف التزييف وتحليل الصور يُعزِّز الوعي بالمحتوى الرقمي
6. التعليم الإعلامي الرقمي من أفضل وسائل الحدّ من انتشار المعلومات المزيفة

الهندسة الاجتماعية

الهندسة الاجتماعية تقوم على استغلال الثقة أو الفضول للحصول على المعلومات دون اختراق تقني مباشر.

يتظاهر المُهاجِم بأنه موظّف رسمي أو جهة معروفة لطلب بيانات حساسة

قد يُرسِل رسائل وُدّية أو يُقدِّم عروضًا مُغْرية لبناء علاقة ثقة

يَستخدم المُهاجِم العواطف مثل الخوف أو التعاطف لدفع الضحية إلى التفاعل

غالبًا ما تكون البداية بسؤال بسيط يتبعه طلب معلومات دقيقة

الوعي بأساليب الخداع هذه يُعدّ خط الدفاع الأول

يُنْصَح بعدم مشاركة أيّ معلومة إلا بعد التحقُّق من هوية الجهة الطالبة

التطبيقات والروابط المُضلّلة

تُعدّ التطبيقات والروابط غير الموثوقة من أكثر الوسائل التي تُستخدَم لاختراق الأجهزة وسرقة البيانات.

بعض التطبيقات تطلب أذونات تتجاوز وظيفتها الأساسية

تحميل البرامج من مصادر مجهولة يؤدي إلى تثبيت برمجيات خبيثة

الروابط القصيرة أو غير المألوفة تُستخدَم كثيرًا في حملات الاحتيال

يُفضَّل تحميل التطبيقات فقط من المتاجر الرسمية المعتمدة

مراجعة أذونات الوصول للتطبيقات بشكلٍ دوريّ خطوة ضرورية للأمان

تجاهل أيّ رابط يُرْسَل من جهة مجهولة حتى وإن بدا مألوفًا في ظاهره

التخزين السحابي

التخزين السحابي يُعدّ وسيلة عملية لحفظ الملفات، لكنّه يحتاج إلى إدارة واعية لتجنُّب التسريب أو الاختراق.

01 رفع الملفات الحساسة دون تشفير يجعلها عُرْضة للوصول غير المصرّح به

02 بعض الخدمات المجانية لا تَضمن مستوى أمان مرتفعًا

03 الروابط العامة قد تَمنح الآخرين حق الوصول الكامل إلى الملفات

04 يُنصَح باستخدام خدمات سحابية موثوقة، وتفعيل المصادقة الثنائية

05 حذف الملفات القديمة، وتقليل مشاركة الروابط المفتوحة يُعزّز الحماية

06 النَّسخ الاحتياطي المشفّر للبيانات الحساسة يحافظ على استمرارية الأمان

التحديثات الدورية

التحديثات الأمنية والتثقيف التقني ركيزتان أساسيتان لحماية المستخدمين من التهديدات المستجدَّة.

1. تُصْدِر الشركات التقنية تحديثات لمعالجة الثغرات المكتَشَفة
2. تأجيل التحديثات يجعل الأنظمة عُرْضة للهجمات والاختراق
3. تفعيل التحديث التلقائي يضمن الحماية الفورية دون تدخُّل يدوي
4. إعادة تشغيل الأجهزة بعد التحديث ضروري لتطبيق الإصلاحات بالكامل
5. التثقيف المستمر حول أساليب الاحتيال والتصيد يرفع من مستوى الوعي العام
6. المشاركة في ورش التوعية الرقمية تُسْهم في بناء مجتمع أكثر أمانًا ومسؤولية

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/2023743341//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