الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ الحماية والخصوصية

الفئة المستهدَفة
الجمهور العام

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 الحماية والخصوصية

الفئة المستهدَفة

الجمهور العام

كُتَيّب المُدَرّب

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 فئات المجتمع بمبادئ السلامة الرقمية وأفضل الممارسات التي تساعد على تجنُّب المخاطر في البيئة الرقمية

يهدف هذا الكتيّب إلى تعزيز وعي المستخدمين بممارسات السلامة الرقمية الأساسية؛ من خلال توضيح كيفية حماية كلمات المرور، تفعيل المصادقة الثنائية، إدارة البصمة الرقمية، الحفاظ على الخصوصية، وضمان الاستخدام الآمِن للأجهزة والإنترنت

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

الشرائح المستهدفة

تستهدف المبادرة مختلف شرائح المجتمع، مع تركيزها على الفئات التالية:

01 السنة الأولى

ذوو الاحتياجات الخاصة

طلبة الجامعات

العمالة الوافدة

مؤسسات المجتمع المدني

القطاع المالي والمصرفي

المرأة والأسرة

كبار القَدْر

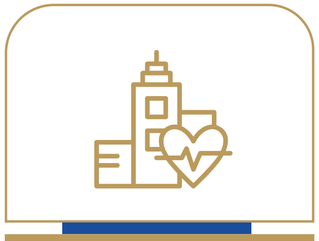
02 السنة الثانية

الدبلوماسيون

الإعلاميون

الرياضيون

المؤسسات العقابية والنيابة والمؤسسات الإصلاحية



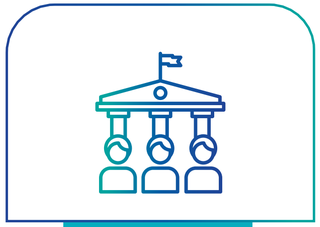
العاملون في المجال الصحي

المرأة (العنف الرقمي ضد المرأة)

الجمهور العام

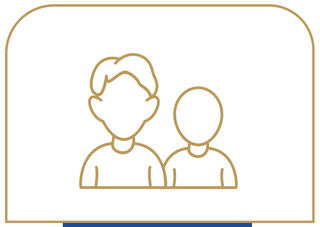
03 السنة الثالثة

العاملون في قطاع الطاقة



العاملون في وزارتي الدفاع والداخلية

الجمهور العام



اليافعون والشباب

ذوو الاحتياجات الخاصة

العاملون في قطاع التعليم

أدوات التوعية

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

دليل السلامة الرقمية

كُتيّبات توعية مطبوعة

شرائح العرض (للمُدرّبين)

فيديوهات التوعية (أنيميشن)

فيديوهات التوعية (تمثيلية)

خَـلّك وَاعـي
وَعْيك دِرْعك

الألعاب السيبرانية

بوابة التوعية السيبرانية

الروبوت التفاعلي

وِرَش التوعية

المحور الأول

كلمات المرور

مفهوم كلمة المرور وأهميتها

كلمة المرور هي رمز سِرّي يُستخدَم للتحقُّق من هوية المستخدِم، وضمان أن الوصول إلى الحسابات يتم مِن قِبَل أصحابها فقط.

أهمية كلمة المرور

- تمنع الوصول غير المصرّح به إلى الحسابات الرقمية
- تحمي البيانات الشخصية والمالية من الاستغلال
- تُسهم في الحفاظ على الخصوصية الرقمية للمستخدِم
- تَحُدّ من مخاطر انتحال الهوية الإلكترونية
- تُعزّز مستوى الأمان العام للخدمات والأنظمة

أخطاء شائعة في إنشاء كلمات المرور

يقع كثير من المستخدِمين في أخطاء تُقلّل من قوة كلمات المرور وتجعلها عُرْضة للتخمين أو الخرق.

أبرز الأخطاء الشائعة

- استخدام كلمات مرور بسيطة يَسْهل توقّعها أو تخمينها
- الاعتماد على معلومات شخصية معروفة أو متاحة للآخرين
- اختيار كلمات مرور قصيرة لا تُوفّر حماية كافية
- إعادة استخدام كلمة المرور نفسها في أكثر من حساب
- مشاركة كلمة المرور مع أشخاص آخرين بدافع الثقة

خصائص كلمة المرور القوية

تعتمد قوة كلمة المرور على مجموعة من الخصائص التي تزيد من صعوبة خرقها باستخدام الأساليب التقليدية أو الآلية.

خصائص كلمة المرور القوية

- تكـون بطـول كافٍ يجعـل تخمينهـا أمرًا بالـغ الصعوبـة
- تحتـوي علـى مزيج مـن الـحروف الكبيـرة والصغيـرة
- تتضمـن أرقامًـا ورمـوزًا خاصـة؛ لزيـادة التعقيـد
- غير مرتبطة بمعلومات شخصية أو متوقّعة
- فريـدة وغيـر مسـتخدَمة فـي حسـابات أخـرى

إدارة كلمات المرور

لا تقل إدارة كلمات المرور أهمية عن إنشائها؛ إذ تؤدي الإدارة غير الصحيحة إلى إضعاف مستوى الحماية.

ممارسات الإدارة الآمنة

- تجنُّب كتابة كلمات المرور في أماكن يسهل الوصول إليها
- عدم حفظ كلمات المرور على الأجهزة دون حماية
- استخدام وسائل تخزين رقمية مُشفَّرة وآمِنَة
- الامتناع عن إرسال كلمات المرور عبر وسائل غير آمِنَة
- مراجعة كلمات المرور وتحديثها عند الحاجة

مخاطر إعادة استخدام كلمات المرور

يؤدي استخدام كلمة مرور واحدة لعدة حسابات إلى توسيع نطاق الضرر في حال تعرُّض أحد الحسابات للخرق

أبرز المخاطر

01 انتقال الخرق بسرعة إلى حسابات أخرى

02 فُقدان السيطرة على أكثر من خدمة رقمية

03 تعريض البيانات الشخصية والمهنية للخطر

04 استغلال الحسابات في أنشطة احتيالية

05 صعوبة احتواء آثار الخرق لاحقًا

أدوات إدارة كلمات المرور

توفّر أدوات إدارة كلمات المرور حلولًا عملية لتخزين وإنشاء كلمات مرور قوية بطريقة آمِنَة.

فوائد هذه الأدوات

- إنشاء كلمات مرور قوية تلقائيًّا
- تخزين كلمات المرور بشكلٍ مشفَّر
- تقليل الاعتماد على التذكُّر اليدوي
- منع تكرار استخدام كلمات المرور
- رفع مستوى الأمان العام للحسابات

تغيير كلمات المرور الدورية

يُعدّ تغيير كلمة المرور إجراءً وقائيًّا مُهمًّا في حالات مُحدَّدة ترتفع فيها احتمالية الخطر.

الحالات التي تستدعي التغيير

- الاشتباه في محاولة خَرْق للحساب
- استخدام أجهزة أو شبكات غير موثوقة
- مشاركة كلمة المرور مع طرف آخر سابقًا
- مرور فترة طويلة دون تحديثها

التعامل مع تسريب كلمات المرور

يتطلّب تسريب كلمات المرور تصرّفًا سريعًا لتقليل الأضرار المحتملة وحماية الحسابات المرتبطة.

الإجراءات الواجب اتباعها

- تغيير كلمة المرور فورًا
- تحديث كلمات المرور المرتبطة بها
- تفعيل المصادقة الثنائية للحساب
- مراجعة سِجِل النشاطات المشبوهة
- إبلاغ الجهة المختصة عند الحاجة

حماية كلمات المرور في الأجهزة المشتركة

يزداد خطر كشف كلمات المرور عند استخدام أجهزة مشتركة في العمل أو الدراسة أو الأماكن العامة.

إجراءات الحماية

- تجنُّب حفظ كلمات المرور على الجهاز
- تسجيل الخروج بعد انتهاء الاستخدام مباشرة
- استخدام وَضْع التَّصفُّح الخاص عند الإمكان
- رفض خيار حفظ بيانات الدخول تلقائيًّا
- التأكُّد من خلو الجهاز من برمجيات ضارة

أمان كلمات المرور في بيئات العمل والتعليم

تتطلب البيئات المؤسسية والتعليمية التزامًا أعلى بسياسات الحماية؛ نظرًا لحساسية البيانات.

أفضل الممارسات

- الالتزام بسياسات كلمات المرور المعتمَدة
- عدم مشاركة الحسابات بين المستخدمين
- استخدام المصادقة الثنائية كلما أمكن
- تغيير كلمات المرور وفق جدول محدَّد
- رفع الوعي الأمني بين الموظفين والطلبة

المحور الثاني

المصادقة الثنائية

مفهوم المصادقة الثنائية وأهميتها

المصادقة الثنائية هي آلية تحقُّق تعتمد على استخدام وسيلتين مختلفتين لإثبات هوية المستخدِم قبل السماح بالدخول.

أهمية المصادقة الثنائية

01 تُقلّل بشكل كبير من احتمالية خرق الحسابات

02 تحمي المستخدِم حتى عند تسريب كلمة المرور

03 تضيف طبقة أمان مستقلة عن كلمة المرور

04 تَحُدّ من مخاطر انتحال الهوية الرقمية

05 تُعزّز الثقة في الخدمات الرقمية المستخدَمة

الفرق بين المصادقة الأحادية والثنائية

تعتمد المصادقة الأُحادية على عنصر واحد فقط، بينما تعتمد المصادقة الثنائية على عنصرين مختلفين للتحقق.

الفروق الأساسية بين النوعين

- المصادقة الأحادية تعتمد على كلمة المرور فقط
- المصادقة الثنائية تجمع بين كلمة المرور ووسيلة تحقُّق إضافية
- المصادقة الأحادية أكثر عُرضة للخرق
- المصادقة الثنائية تُوفّر مستوى أمان أعلى
- المصادقة الثنائية تُقلّل أثر تسريب بيانات الدخول

مخاطر الاعتماد على كلمة المرور فقط

يؤدي الاعتماد على كلمة المرور وحدها إلى زيادة احتمالية تعرّض الحسابات للخرق.

أبرز المخاطر

- سهولة تخمين كلمات المرور الضعيفة
- استغلال كلمات المرور المسرّبة
- تعرُّض الحسابات لهجمات آلية
- فقدان السيطرة على الحساب بسرعة
- اتساع نطاق الضرر عند الخرق

أنواع المصادقة الثنائية

تتنوَّع وسائل المصادقة الثنائية بحسب طريقة إرسال أو توليد رمز التحقق.

أبرز أنواع المصادَقة الثنائية

- إرسال رمز تحقّق عبر الرسائل النصية إلى هاتف المستخدِم
- توليد رموز مؤقّتة عبر تطبيقات المصادقة المخصّصة
- إرسال رمز تحقّق عبر البريد الإلكتروني المرتبط بالحساب
- استخدام مفاتيح أمان مادية مخصّصة
- التحقّق عبر الإشعارات الفورية داخل التطبيقات

تطبيقات المصادقة الثنائية

تُستخدَم تطبيقات المصادقة الثنائية لتوليد رموز تحقّق مُؤقَّتة بشكلٍ آمِن ومستقل عن الشبكة.

أهمية استخدام هذه التطبيقات

- توليد رموز تحقُّق آمِنَة
- العمل دون الحاجة إلى اتصال دائم بالإنترنت
- تقليل الاعتماد على الرسائل النصية
- تعزيز أمان الحسابات الحساسة
- سهولة إدارة عدة حسابات في مكان واحد

المصادقة الثنائية البيومترية

تعتمد المصادقة البيومترية على الخصائص الجسدية الفريدة للمستخدِم كوسيلة تحقُّق إضافية.

مزايا المصادقة البيومترية

01 صعوبة تقليد الخصائص الجسدية للمستخدِم

02 سهولة وسرعة في إتمام عملية التحقُّق

03 تقليل الاعتماد على الحفظ والتذكُّر

04 تعزيز الأمان في الأجهزة الذكية

05 رفع مستوى الحماية للحسابات الحساسة

تفعيل المصادقة الثنائية للحسابات الشخصية

يُعدّ تفعيل المصادقة الثنائية إجراءً بسيطًا، لكنّه فعّال في رفع مستوى الأمان.

الخطوات العامة للتفعيل

1. الدخول إلى إعدادات الأمان في الحساب
2. اختيار خيار المصادقة الثنائية أو التحقُّق بخطوتين
3. تحديد وسيلة التحقُّق المناسبة للمستخدِم
4. ربط الحساب برقم هاتف أو تطبيق مصادقة
5. حفظ رموز الاسترداد في مكان آمِن.

التعامل مع فقدان وسيلة المصادقة

قد يتعرّض المستخدِم لفقدان الهاتف أو وسيلة التحقُّق، ما يتطلب إجراءات بديلة لاستعادة الوصول.

الإجراءات الواجب اتباعها

- استخدام رموز الاسترداد المحفوظة مسبقًا
- التحقُّق من الهوية عبر القنوات الرسمية
- تحديث وسيلة المصادقة فور استعادة الحساب
- إلغاء ربط الوسيلة المفقودة بالحساب
- مراجعة إعدادات الأمان بالكامل

أفضل الممارسات لاستخدام المصادقة الثنائية

- تفعيل المصادقة الثنائية لجميع الحسابات المهمة
- استخدام تطبيقات المصادقة بدل الرسائل النصية متى أمكن
- عدم مشاركة رموز التحقُّق مع أيّ جهة
- الاحتفاظ بنُسَخ آمِنَة من رموز الاسترداد
- مراجعة إعدادات الأمان بشكلٍ دوري

المحور الثالث

البصمة الرقمية

مفهوم البصمة الرقمية

01 البصمة الرقمية هي مجموع البيانات التي يتم إنشاؤها أو تسجيلها نتيجة استخدام الفرد للإنترنت والتقنيات.

02 توضّح حجم البيانات المتداولة عن المستخدِم دون إدراكه

03 تُظهر كيفية تكوين صورة رقمية عن الفرد

04 تُسهم في تعزيز الوعي بالخصوصية الرقمية

05 تساعد على اتخاذ قرارات رقمية أكثر وعيًا

06 تدعم حماية الهوية الرقمية للمستخدِم

أنواع البصمة الرقمية

تنقسم البصمة الرقمية إلى نوعين رئيسيين يختلفان في طريقة تكوُّنها ومستوى تحكُّم المستخدم بها.

أنواع البصمة الرقمية

- البصمة الرقمية النَّشطة التي يُنتجها المستخدِم عند النشر أو التفاعل المباشر
- البصمة الرقمية الخاملة التي تتكوَّن دون تدخُّل مباشر من المستخدِم
- البصمة النشطة تكون غالبًا تحت سيطرة المستخدِم
- البصمة الخاملة تُجْمَع تلقائيًّا عبر الأنظمة والتطبيقات
- كلا النوعين يُسهمان في تشكيل الهوية الرقمية

كيف تتكوَّن البصمة الرقمية للمستخدِم؟

تتكوّن البصمة الرقمية من خلال سلسلة من الأنشطة اليومية التي يقوم بها المستخدِم في أثناء استخدامه للتقنيات الرقمية.

آليات تكوُّن البصمة الرقمية

- تسجيل الدخول إلى المواقع والتطبيقات المختلفة
- النشر والتعليق والمشاركة عبر المنصات الرقمية
- عمليات البحث والتصفح عبر محركات البحث
- استخدام التطبيقات والخدمات الرقمية المتنوعة
- الموافقة على ملفات تعريف الارتباط (Cookies)

مخاطر البصمة الرقمية

يـؤدي إهمـال إدارة البصمـة الرقميـة إلـى تعـرُّض المسـتخدِم لمخاطـر متعـدّدة علـى المسـتويين الشـخصي والمهنـي.

أبرز المخاطر المحتملة

- استغلال البيانات الشخصية دون عِلْم المستخدم
- انتهاك الخصوصية الرقمية على المدى الطويل
- استخدام المعلومات لأغراض احتيالية أو تسويقية
- تكوين صورة غير دقيقة عن المستخدِم
- صعوبة حذف الآثار الرقمية بعد انتشارها

علاقة البصمة الرقمية بالخصوصية

01 ترتبط البصمة الرقمية ارتباطًا مباشرًا بمستوى الخصوصية الذي يتمتع به المستخدِم في البيئة الرقمية

02 كلما زادت البصمة الرقمية قلّت الخصوصية

03 إعدادات الخصوصية تَحُدّ من جمع البيانات

04 مشاركة المعلومات تُؤثّر مباشرة على الخصوصية

05 التحكُّم في البصمة يُعزّز الخصوصية الرقمية

06 الوعي الرقمي أساس لحماية الخصوصية

تأثير وسائل التواصل الاجتماعي

تُعدّ منصات التواصل الاجتماعي من أكثر العوامل تأثيرًا في تضخيم البصمة الرقمية للمستخدِم.

أبرز مظاهر التأثير

- تراكم المحتوى المنشور بمرور الوقت
- سهولة إعادة نشر المحتوى دون تحكُّم
- ربط الحسابات الشخصية بمنصات متعددة
- تحليل التفاعلات والسلوكيات الرقمية
- صعوبة التحكُّم الكامل في المحتوى القديم

تتبّع السلوك الرقمي عبر المواقع والتطبيقات

تعتمد العديد من المواقع والتطبيقات على أدوات لتتبُّع نشاط المستخدِم لأغراض مختلفة.

آليات التتبُّع الشائعة

- استخدام ملفات تعريف الارتباط (Cookies)
- تتبُّع سجل التصفُّح وعمليات البحث
- جَمْع بيانات الموقع الجغرافي
- تحليل نَمَط الاستخدام داخل التطبيقات
- مشاركة البيانات مع أطراف أخرى

إدارة البصمة الرقمية

يمكن للمستخدِم إدارة بصمته الرقمية؛ من خلال اتباع ممارسات واعية في أثناء استخدامه للتقنيات.

ممارسات إدارة البصمة الرقمية

- مراجعة إعدادات الخصوصية بشكل دوري
- تقليل مشاركة المعلومات الشخصية
- حذف الحسابات غير المستخدَمة
- التحكُّم في أذونات التطبيقات
- استخدام أدوات حماية الخصوصية

أمثلة على البصمة الرقمية

01 التعليق على منشورات في منصات التواصل الاجتماعي

02 إنشاء حسابات في مواقع التسوق الإلكتروني

03 البحث المتكرّر عن موضوعات مُحدَّدة عبر الإنترنت

04 تحميل التطبيقات والموافقة على أذوناتها

05 الاشتراك في النشرات البريدية والخدمات الرقمية

المحور الرابع

الخصوصية والبيانات الشخصية

مفهوم الخصوصية الرقمية

الخصوصية الرقمية هي حقّ المستخدِم في التحكُّم ببياناته الشخصية وكيفية جمعها واستخدامها في البيئة الرقمية.

أهمية الخصوصية الرقمية

- تَمنح المستخدِم السيطرة على معلوماته الشخصية
- تَحُدّ من الاستغلال غير المشروع للبيانات
- تحمي الهوية الرقمية
- تُعزّز الثقة في الخدمات الرقمية
- تدعم الاستخدام الآمِن للتقنيات

أنواع البيانات الشخصية

تختلف البيانات التي يتم جمعها عن المستخدِم من حيث طبيعتها ومستوى حساسيتها.

أنواع البيانات الشخصية

- البيانات التعريفية مثل الاسم ورقم الهوية
- بيانات الاتصال مثل رقم الهاتف والبريد الإلكتروني
- البيانات المالية والمصرفية
- البيانات الصحية والبيومترية
- بيانات الموقع الجغرافي والسلوك الرقمي

مخاطر مشاركة المعلومات الشخصية

تؤدي مشاركة البيانات الشخصية دون وعي إلى تعرُّض المستخدِم لمخاطر متعددة.

أبرز المخاطر

- انتحال الهوية الرقمية
- الاحتيال المالي والإلكتروني
- انتهاك الخصوصية الشخصية
- استغلال البيانات لأغراض تسويقية
- فقدان السيطرة على المعلومات المنشورة

إعدادات الخصوصية

توفّر التطبيقات ومنصات التواصل أدوات للتحكُّم في مستوى الخصوصية عند الاستخدام.

أهمية ضبط إعدادات الخصوصية

- التحكُّم فيمن يمكنه رؤية المحتوى
- تقليل جَمْع البيانات غير الضرورية
- تحديد صلاحيات الوصول للمعلومات
- منع التتبُّع غير المرغوب فيه
- تعزيز أمان الحسابات الشخصية

الأذونات الممنوحة للتطبيقات

تطلب التطبيقات أذونات للوصول إلى بعض بيانات الجهاز، وقد يُشكِّل ذلك خطرًا عند سوء الاستخدام.

التعامل مع الأذونات

- منح الأذونات الضرورية فقط
- رَفْض الأذونات غير المرتبطة بوظيفة التطبيق
- مراجعة الأذونات بشكل دوري
- إلغاء الأذونات للتطبيقات غير المستخدَمة
- التحقُّق من سياسات الخصوصية قبل التثبيت

التعامل مع طلبات جمع البيانات

تقوم بعض الخدمات بطلب بيانات تفوق الحاجة الفعلية لتقديم الخدمة.

إرشادات التعامل مع هذه الطلبات

- قراءة سبب طلب البيانات قبل الموافقة
- رفض مشاركة البيانات غير الضرورية
- التأكُّد من مصداقية الجهة الطالبة
- مراجعة شروط الاستخدام وسياسة الخصوصية
- إلغاء الموافقة عند عدم الحاجة للخدمة

ممارسات تعزيز الخصوصية الرقمية

يساعد الالتزام بعادات رقمية واعية على حماية الخصوصية على المدى الطويل.

أبرز الممارسات

- تقليل مشاركة المعلومات الشخصية عبر الإنترنت
- استخدام كلمات مرور قوية وفريدة
- تفعيل المصادقة الثنائية للحسابات المهمة
- مراجعة إعدادات الخصوصية بانتظام
- التحقّق من مصادر التطبيقات والمواقع

المحور الخامس

الاستخدام الآمِن للأجهزة والإنترنت

تحديث الأنظمة والتطبيقات

تُسهم التحديثات الدورية في معالجة الثغرات الأمنية وتحسين مستوى الحماية العامة للأجهزة

سد الثغرات الأمنية المكتشفة حديثًا

تعزيز خصائص الحماية في النظام

تحسين استقرار وأداء الجهاز

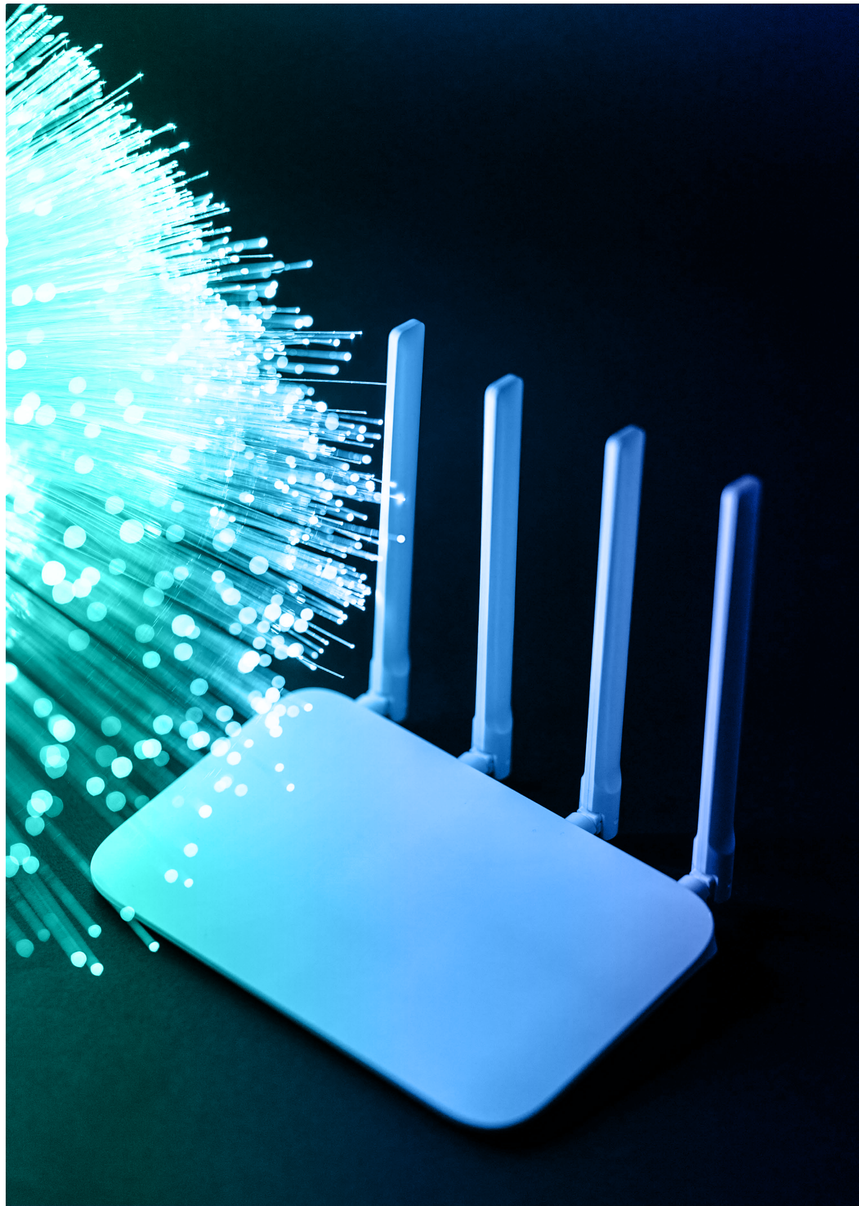
رفع مستوى التوافق مع تقنيات الأمان الحديثة

مخاطر الشبكات اللاسلكية العامة

تُعدّ الشبكات اللاسلكية العامة من أكثر البيئات عُرْضة لانتهاك الخصوصية وسرقة البيانات.

أبرز المخاطر المرتبطة بها

- اعتراض البيانات المُرسَلة والمُستقبَلة
- انتحال الشبكات مِن قِبَل جهات غير موثوقة
- تتبُّع نشاط المستخدِم دون عِلْمه
- سرقة بيانات تسجيل الدخول
- نَشْر برمجيات ضارة عبر الشبكة



الحماية من البرمجيات الخبيثة

تشمل البرمجيات الخبيثة برامج تُصمَّم لإلحاق الضرر بالأجهزة أو سرقة المعلومات.

وسائل الحماية الأساسية

- تجنُّب تحميل الملفات من مصادر غير موثوقة
- عدم تثبيت البرامج المقرصنة أو المجهولة
- تحديث النظام وبرامج الحماية بانتظام
- فَحْص الملفات قبل فتحها أو تشغيلها
- الحذر من الروابط والمرفقات المشبوهة

برامج الحماية والجدران النارية

تساعد برامج الحماية والجدران النارية في منع التهديدات قبل وصولها إلى الجهاز.

أهمية استخدامها

- كشف البرمجيات الخبيثة في وقتٍ مُبكّر
- منع الاتصالات غير المصرّح بها
- مراقبة حركة البيانات الداخلة والخارجة
- تقليل مخاطر خرق الشبكات
- تعزيز الأمان العام للنظام

الاستخدام الآمِن للتطبيقات

تُشكِّل التطبيقات والألعاب مصدرًا محتملًا للمخاطر عند تحميلها أو استخدامها دون ضوابط.

ممارسات الاستخدام الآمِن

- تحميل التطبيقات من المتاجر الرسمية فقط
- قراءة تقييمات المستخدِمين قبل التثبيت
- مراجعة الأذونات المطلوبة بعناية
- تجنُّب الألعاب التي تطلب بيانات غير مُبرَّرة
- حذف التطبيقات غير المستخدَمة

التعامل مع الروابط المشبوهة

تُستخدم الروابط المشبوهة كوسيلة شائعة لنشر البرمجيات الخبيثة أو تنفيذ عمليات احتيالية.

إرشادات التعامل الآمِن

01 عدم النقر على روابط من مصادر غير معروفة

02 التحقُّق من عنوان الرابط قبل فتحه

03 الحذر من الروابط المصحوبة برسائل عاجلة

04 تجنُّب إدخال البيانات عبر روابط غير موثوقة

أمان الأجهزة المحمولة

تحتوي الأجهزة المحمولة على بيانات شخصية حساسة، وتتطلب حماية خاصة.

إجراءات تعزيز الأمان

- تفعيل قفل الشاشة بوسيلة آمِنَة
- تحديث نظام التشغيل والتطبيقات باستمرار
- تجنُّب تثبيت التطبيقات من مصادر غير موثوقة
- تفعيل ميزة تحديد الموقع والمسح عن بُعْد
- عدم ترك الجهاز دون رقابة في الأماكن العامة

النَّسخ الاحتياطي للبيانات

يُعدّ النَّسخ الاحتياطي وسيلة فعّالة لحماية البيانات من الفقدان أو التلف.

فوائد النسخ الاحتياطي

- استعادة البيانات عند حدوث أعطال تقنية
- تقليل آثار هجمات الفدية
- حماية الملفات الشخصية والمهنية
- تقليل الخسائر الناتجة عن فقدان البيانات

ممارسات الاستخدام الآمِن للإنترنت

يسهم الالتزام بعادات رقمية صحيحة في رفع مستوى الأمان العام في أثناء استخدام الإنترنت.

أبرز الممارسات

- تسجيل الخروج من الحسابات بعد الانتهاء من استخدامها
- عدم مشاركة البيانات الشخصية دون ضرورة
- استخدام كلمات مرور قوية وفريدة
- تحديث الأجهزة والبرامج بانتظام
- التحقّق من مصداقية المواقع والخدمات

المراجع

1. Baltezarević, Radoslav & Baltezarevic, Ivana Social Media Impersonation as a Cybersecurity Threat International Topkapi Congress IV, October 2024, on site: https://wwwresearchgatenet/publication/384657784_SOCIAL_MEDIA_IMPERSONATION_AS_A_CYBERSECURITY_THREAT

2. 2. Cybersecurity and Infrastructure Security Agency (CISA) Use Strong Passwords, on site: https://wwwcisagov/secure-our-world/use-strong-passwords

3. 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://harvardpublicationscom/hijcisr/article/view/326

4. IBM What is malware?, on site: https://wwwibmcom/think/topics/malware

5. Information Commissioner's Office (ICO) What is personal data?, on site: https://icoorguk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/

6. National Cyber Security Centre (NCSC) Phishing, on site: https://wwwncscgovuk/guidance/phishing

المراجع

7. National Cyber Security Centre (NCSC) Turn on 2-step verification (2SV), on site: https://wwwncscgovuk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email

8. Orłowska, Agnieszka Cybersecurity and Cyberthreats in Social Media, December 2022, on site: https://wwwresearchgatenet/publication/367048439_Cybersecurity_and_Cyberthreats_in_Social_Media

9. Susnjara, Stephanie IBM What is cloud computing?, on site: https://wwwibmcom/think/topics/cloud-computing

10. US General Services Administration, Office of Inspector General (GSA OIG) Scam Alert: Beware of fake websites that mimic legitimate official US government websites, on site: https://wwwgsaiggov/news/scam-alert-beware-fake-websites-mimic-legitimate-official-us-government-websites

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