الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy



مبادئ عامة في السلامة الرقمية

الفئة المستهدفة
الجمهور العام

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مبادئ عامة في السلامة الرقمية

الفئة المستهدفة

الجمهور العام

كُتَيّب المُدَرّب

الفهرس	رقم الصفحـة
تمهيد	7
المبادرة الوطنية للسلامة الرقمية	8
المحور الأول: المخاطر السيبرانية الشائعة	14
المخاطر الرقمية	15
الهجمات السيبرانية الشائعة	16
التصيُّد الاحتيالي	17
أنواع رسائل التصيُّد	18
البرمجيات الخبيثة	19
برمجيات الفدية	20
الهندسة الاجتماعية	21
أساليب الخداع	22
التزييف العميق	23
سرقة الهوية الرقمية	24

الفهرس	رقم الصفحـة
مؤشرات سرقة الهوية الرقمية	25
المحور الثاني: أساسيات السلامة الرقمية	26
السلامة الرقمية	2
أهمية السلامة الرقمية	28
الأمن السيبراني	29
الفرق بين السلامة الرقمية والأمن السيبراني	30
البيانات الشخصية	31
الوقاية من خرق البيانات	32
التشفير	33
التخزين السحابي	34
برامج الحماية	35
أمن التطبيقات	36
إدارة كلمات المرور	37

الفهرس	رقم الصفحـة
المصادقة الثنائية	38
الاستخدام الآمِن للأجهزة الذكية	39
التحديثات الأمنية	40
مُؤشّرات الخرق	41
الإجراءات عند الخرق	42
الوقاية من التصيُّد الاحتيالي	43
الوقاية من برمجيات الفدية	44
التَّحقُّق من المحتوى	45
إعدادات الخصوصية	46
السلوك الرقمي الآمِن	48
المحور الثالث: التَّصفُّح الآمِن للإنترنت	49
مخاطر التَّصفُّح العشوائي	50
الإعلانات المُضلّلة	51

الفهرس	رقم الصفحـة
الروابط والمواقع المُزيَّفة	52
النوافذ المنبثقة	53
قواعد التَّصفُّح الآمِن	54
التَّحقُّق من المواقع	55
بروتوكول HTTPS	56
البريد الإلكتروني	57
شبكات Wi-Fi العامة	58
الوقاية من مخاطر شبكات Wi-Fi العامة	59
الشبكات الافتراضية الخاصة VPN	60
التسوق الإلكتروني	61
المراجع	62

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 الكتيّب إلى تعزيز الوعي بأبرز التهديدات التقنية التي قد نواجهها في حياتنا اليومية؛ مثل: التصيّد الاحتيالي، والبرمجيات الخبيثة، وبرمجيات الفدية، والهندسة الاجتماعية، والتزييف العميق، وسرقة الهوية الرقمية.

كما يقدّم الكتيّب إرشادات عملية وإجراءات وقائية لحماية الأجهزة الشخصية، وتأمين الحسابات الإلكترونية، والتصرّف السليم عند ملاحظة أيّ مُؤشّرات خرق أو نشاط مريب.

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 المستهدَفة

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
- كبار القَدْر
- المرأة والأسرة

02 السنة الثانية



الدبلوماسيون



الإعلاميون



الجمهور العام



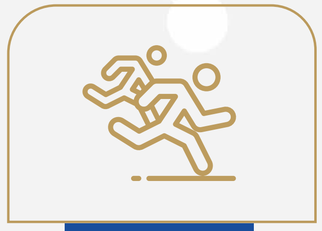
المرأة (العنف الرقمي ضد المرأة)



العاملون في المجال الصحي



المؤسسات العقابية والنيابة والمؤسسات الإصلاحية

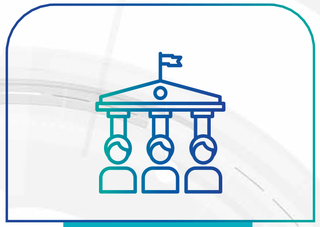


الرياضيون

03 السنة الثالثة



العاملون في قطاع الطاقة



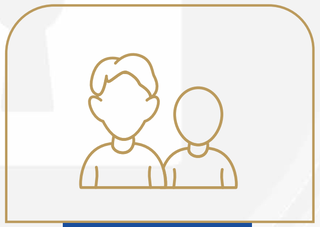
العاملون في وزارتي الدفاع والداخلية



العاملون في قطاع التعليم



ذوو الاحتياجات الخاصة



اليافعون والشباب



الجمهور العام

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

المخاطر السيبرانية الشائعة

المخاطر الرقمية

- استهداف البيانات الشخصية لأغراض الاحتيال أو سرقة الهوية
- خَرْق الحسابات نتيجة ضَعْف كلمات المرور أو الإهمال الرقمي
- التعرُّض للبرمجيات الخبيثة عبر الروابط أو الملفات المشبوهة
- استغلال قلة الوعي الرقمي في تنفيذ هجمات سيبرانية

الهجمات السيبرانية الشائعة

تتنوَّع الهجمات السيبرانية التي تَستهدف المستخدِمين في البيئة الرقمية.

أبرز أنواع الهجمات

- هجمات التصيّد الاحتيالي: تهدف إلى سرقة بيانات تسجيل الدخول أو المعلومات المالية
- البرمجيات الخبيثة: تُزرع في الأجهزة عبر روابط أو مُرفقات غير موثوقة
- محاولات خرق الحسابات باستغلال كلمات مرور ضعيفة أو مُسرَّبة
- انتحال الهوية الرقمية لتنفيذ عمليات احتيال أو إساءة استخدام



التصيّد الاحتيـــالي

يُعـدّ التصيّـد الاحتيالـي مـن أكثـر أسـاليب الخـداع شـيوعًا، ويعتمد علـى إرسـال رسـائل أو روابـط تبـدو حقيقيـة، لكنهـا تهـــدف إلـى سـرقة المعلومـات

تأتـي الرســـائل الاحتياليـة عـادة عبـر البريـد الإلكتروني أو الرسـائل النصيـة أو مواقـع مُزيَّفـة

تطلـــب الرسـائل الاحتياليـة إدخـال بيانـات مثـل كلمـات الـمرور أو أرقـام البطاقـات

تعتمـد على أسـلوب الإقنـاع باسـتخدام عبارات مسـتعجلة أو تهديديـة

يجـــب تجاهُـل الرسـائل المشـبوهة، والتَّحقُّـــق مـن مصدرهـا قبـل أيّ تفاعـل

أنواع رسائل التصيّد

- رسائل بريد إلكتروني تَدّعي وجود مشكلة في الحساب أو الحاجة إلى التَّحقُّق
- رسائل نصية تُعْلِن عن جوائز أو معاملات مالية عاجلة
- إشعارات مُزيَّفة تحمل أسماء بنوك أو جهات خدمية معروفة
- روابط مختصرة تُخفي الوجهة الحقيقية للموقع المستهدَف

البرمجيات الخبيثة

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

قد تختبئ في تطبيقات أو ملفات تبدو طبيعية

تتسبب في بُطْء النظام أو سرقة كلمات المرور أو مراقبة الأنشطة

يمكن الوقاية منها عَبْر تثبيت برامج مكافحة الفيروسات، وتحديثها باستمرار

تجنُّب تحميل البرامج من مواقع غير موثوقة



برمجيـات الفـدية

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 لملفاته

حتى بعد الدَّفع، لا يوجد ضمان لاسترجاع البيانات

الهندسة الاجتماعية



تعتمد الهندسة الاجتماعية على التلاعُب النفسي بدل الخرق التقني؛ حيث يَستهدف المهاجم السلوك البشري لاستدراج الضحية والحصول على معلومات حسّاسة. وتتمثّل أبرز أساليبها في الآتي:

- انتحال صفة موظف دعم أو جهة رسمية لكسب ثقة الضحية
- جَمْع معلومات مسبقة عن المستخدِم لاستخدامها في الإقناع
- استغلال الخوف أو الاستعجال للحصول على معلومات حساسة
- تجاوز أنظمة الحماية عبر استهداف السلوك البشري



أساليب الخداع

استخدام لغة رسمية أو وُدِّيَّة لبناء الثقة مع المستخدِم

تقديم عروض مُغْرية أو تهديدات وهمية لدفع المستخدِم للتفاعل

استغلال الأحداث العامة أو الطارئة؛ لإضفاء مصداقية زائفة

تكرار المحاولات حتى تحقيق الهدف المطلوب

التزييف العميق

تقنية قائمة على الذكاء الاصطناعي تُستخدَم لتوليد صور أو فيديوهات مُزيَّفة

يمكن أن تُستخدَم لانتحال الهوية أو نَشْر محتوى مُضلّل

يصعب على المستخدم العادي اكتشافها دون أدوات تحليل

يُنْصَح بعدم إعادة نَشْر أيّ محتوى قبل التَّحقُّق من مصدره

سرقة الهوية الرقمية

تحدث عندما يتمكّن 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 لذلك

المراقبة الدورية للنشاطات المالية تساعد في الاكتشاف المبكّر



مؤشرات سرقة الهوية الرقمية

- نشاط غير مُعتاد في الحسابات أو المعاملات المالية
- تلقّي إشعارات تسجيل دخول لم يَقُم بها المستخدِم
- تَغيُّر بيانات الحساب دون عِلْم صاحبه
- رسائل تطالب بتأكيد معلومات لم يتم طلبها سابقًا



02 المحور الثاني

أساسيات السلامة الرقمية



السلامة الرقمية

أساس الاستخدام الآمِن والمسؤول للتقنيات الحديثة

تهـدف إلـى حمايـة البيانـات الشـخصية مـن المخاطـر الرقميـة

تُعنَـى بالحفـاظ علـى سريـة المعلومـات وسلامتهـا وتوافرهـا عنـد الحاجـة

تشـمل الممارسـات التقنيـة مثـل: التشـفير، والسـلوكية مثـل: تَجاهُـل الروابـط المجهولـة

تُمكِّـن المسـتخدِم مـن اسـتخدام الفضـاء الرقمـي بثقـة ومسـؤولية

تُسـهم فـي الحـدّ مـن المخاطـر قبـل وقوعهـا لا بعـد حدوثهـا

أهمية السلامة الرقمية

ترتبط السلامة الرقمية بجميع الأنشطة اليومية التي تتم عبر الوسائط الرقمية

حماية المعلومات الشخصية والمالية في أثناء استخدام الخدمات الإلكترونية المختلفة

تقليل مخاطر الاحتيال الإلكتروني الناتجة عن الاستخدام غير الآمِن للإنترنت

ضمان الوصول الآمِن والمستمر إلى الحسابات والمنصات الرقمية

الحدّ من الخسائر الرقمية الناتجة عن تسريب البيانات أو خَرْق الحسابات

الأمن السيبراني

يهدف الأمن السيبراني إلى حماية الأنظمة والبيانات من التهديدات الرقمية المتزايدة، وذلك من خلال:

- حماية الأجهزة والشبكات من محاولات الخرق التي قد تُؤدّي إلى تعطيل الخدمات أو سرقة المعلومات الحساسة
- تأمين البيانات الرقمية من التلاعب أو التسريب أو الاستخدام غير المُصرَّح به
- تقليل الأضرار الناتجة عن الهجمات الإلكترونية على الأفراد والمؤسسات والخدمات الحيوية
- دَعْم استمرارية الأعمال والخدمات الرقمية من خلال تطبيق إجراءات وقائية فعَّالة



الفَرْق بين السلامة الرقمية والأمن السيبراني

يُشكِّل كلّ من السلامة الرقمية والأمن السيبراني عنصرين متكاملين للحماية

تركز السلامة الرقمية على وَعْي المستخدِم وسلوكه في أثناء التفاعل مع التكنولوجيا

يهتمّ الأمن السيبراني بحماية الأنظمة والشبكات من الهجمات التقنية

يعتمد كلا الجانبين على الوقاية المسبقة بدلًا من الاستجابة بعد وقوع الخطر

تعزيز الحماية الشاملة عبر الجمع بين السلوك السليم والحلول التقنية

البيانـــات الشخصية

01 تُعدّ البيانات الشخصية من أكثر الأصول حساسية في الحياة الرقمية

02 تشمل كلّ ما يمكن أن يكشف عن الهوية أو التفاصيل الشخصية

03 تضمّ البيانات الشخصية الأسماء، الصور، أرقام الهواتف، والمعلومات البنكية

04 يُستحسَن تقليل مشاركتها عبر الإنترنت، وتقييد ظهورها على المنصات العامة

05 يجب مراجعة إعدادات الخصوصية في التطبيقات بشكل دوري

06 يجب تخزين النُّسَخ الاحتياطية المشفَّرة للمستندات المهمة في أماكن آمنة

الوقاية من خرق البيانات

استخدام كلمات مرور قوية وفريدة لكل حساب، وربطها بمدير كلمات مرور موثوق

تفعيل المصادقة الثنائية لجميع الحسابات المهمة لتعزيز طبقات الحماية

تحديث الأنظمة والتطبيقات بانتظام لسدّ الثغرات المكتشفة حديثًا

مراقبة الحسابات والأنشطة الرقمية لاكتشاف أيّ محاولات خرق مبكرًا

التشفير

يُعَدّ التشفير أداةً أساسية في حماية البيانات الرقمية؛ إذ يضمن سِرّية المعلومات في أثناء التخزين أو النقل، ويمنع أيّ وصول غير مصرَّح به.

ويُطبَّق التشفير عمليًّا من خلال مجموعة من الممارسات، من أبرزها:

- عند إرسال رسائل البريد الإلكتروني الحسَّاسة لضمان حماية المحتوى من التنصت
- قبل مشاركة المستندات على الإنترنت أو عبر السحابة
- الاعتماد على بروتوكولات تشفير قوية في الأجهزة والتطبيقات
- استخدام الشبكات الافتراضية الخاصة (VPN) لتشفير الاتصال عند التعامل مع الشبكات العامة
- التأكُّد من أن منصات التخزين السحابي تَدْعم التشفير الكامل للبيانات المُخزَّنة

التخزين السحابي

اختيار مزود خدمة سحابية موثوق وذي سُمعة جيدة لتقليل المخاطر

تشفير الملفات قبل رَفْعها على السحابة لتعزيز مستوى الأمان

تفعيل المصادقة الثنائية للوصول إلى الحسابات السحابية؛ لضمان حماية إضافية

مراقبة سجلات الدخول للحسابات السحابية للكشف المبكّر عن أيّ نشاط غير مُعتَاد

إدارة الصلاحيات بدقة لمن يمكنه الوصول إلى الملفات والمجلدات المشتركة



برامج الحماية

تلعب برامج الحماية دورًا أساسيًّا في الأمن السيبراني، وذلك من خلال:

- كشف البرمجيات الخبيثة ومنع تثبيتها على الأجهزة
- مُراقبة الأنشطة المشبوهة وتنبيه المستخدِم
- تحديث قواعد الحماية لمواجهة التهديدات الجديدة
- تعزيز مستوى الأمان العام للأجهزة والبيانات

أمن التطبيقات

التطبيقات الرقمية أصبحت جزءًا أساسيًّا من الحياة اليومية، ولكنّها قد تتحوَّل إلى بوابة لخرق البيانات إذا لم تتم إدارتها بشكل صحيح من خلال:

تحميل التطبيقات فقط من المتاجر الرسمية والمعتمدة؛ لتقليل خطر البرمجيات الضارة

مراجعة الصلاحيات المطلوبة للتطبيقات، والتأكد من توافقها مع وظائف التطبيق الفعلية

تحديث التطبيقات بشكل دوري لسدّ الثغرات الأمنية المكتشفة حديثًا



استخدام برامج مكافحة الفيروسات والمراقبة الأمنية على الأجهزة الشخصية

حذف التطبيقات غير المستخدَمة لتقليل فرص استغلالها مِن قِبَل المهاجمين

إدارة كلمات المرور

تُعدّ كلمات المرور الركيزة الأساسية لحماية الأجهزة والحسابات الرقمية، وهي غالبًا أول ما يَستهدفه المهاجمون.

نصائح إدارة كلمات المرور



- يُفضَّل أن تكون كلمة المرور طويلة ومُعقَّدة وتختلف بين الحسابات
- يُستحسَن استخدام برامج متخصصة لإدارة كلمات المرور بأمان
- تجنُّب استخدام المعلومات الشخصية مثل تاريخ الميلاد أو الاسم
- تغيير كلمات المرور بشكل دوري خاصةً بعد أيّ نشاط مريب

المصادقة الثنائية

- إضافة طبقة ثانية من الأمان تُمثّل أحد أهم الممارسات الحديثة في حماية الحسابات
- تُتيح التَّحقُّق بخطوتين وقاية فعَّالة لمحاولات الخرق حتى في حال تسريب كلمة المرور
- تعتمد على إدخال رمز تحقُّق يُرسل إلى الهاتف أو البريد بعد كلمة المرور
- تَقِي من محاولات الدخول العشوائية أو الخداع الإلكتروني
- يُنْصَح بتفعيلها في البريد الإلكتروني والحسابات المصرفية ومواقع التواصل
- يُفضَّل استخدام تطبيقات المصادقة بدل الرسائل النصية لزيادة الحماية



الاستخدام الآمِن للأجهزة الذكية

الأجهزة الذكية أصبحت جزءًا لا يتجزَّأ من الحياة اليومية، ولكنها في الوقت نفسه مدخل رئيسي للمخاطر الإلكترونية إذا لم تُؤمَّن جيدًا.

ممارسات الأمان

- وضع كلمة مرور قوية أو بصمة لحماية الجهاز من الوصول غير المصرَّح به
- تحديث نظام التشغيل والتطبيقات بشكلٍ منتظم لسدّ الثغرات الأمنية
- تجنُّب تحميل التطبيقات من مصادر غير موثوقة
- تفعيل خاصية "العثور على الجهاز" للمساعدة في استرجاعه عند الفقدان



التحديثات الأمنية

تُعدّ التحديثات الدورية خط الدفاع الأخير ضد التهديدات الجديدة

تحتوي التحديثات على تصحيحات لثغرات تُستغل في الخروقات

تأجيل التحديثات يجعل الجهاز عُرضة للبرمجيات الحديثة

تفعيل خاصية التحديث التلقائي لجميع التطبيقات والأنظمة

إعادة تشغيل الجهاز بعد التحديث لضمان تثبيت الحماية بالكامل



مؤشرات الخرق

يُعدّ التعرُّف المبكّر على علامات الخرق خطوة أساسية للتعامل الفعّال مع الخطر قبل أن يتفاقم.

أبرز مُؤشّرات الخَرق

- بُطْء مفاجئ في أداء الجهاز أو استهلاك مُفْرِط للطاقة
- ظهور برامج أو نوافذ غير مألوفة دون تثبيت مسبق
- رسائل صادرة من البريد أو الحساب دون عِلْم المستخدم
- تغيّرات مفاجئة في الإعدادات أو إشعارات تسجيل دخول من مواقع غريبة

الإجراءات عند الخرق

عند ملاحظة أيّ سلوك غير طبيعي في الحسابات أو الأجهزة، يجب التصرُّف بسرعة واتباع خطوات مُحدَّدة للحد من الضرر؛ وتلك الخطوات تتمثَّل في الآتي:

- فصل الجهاز فورًا عن الإنترنت؛ لمنع تسريب البيانات
- تغيير كلمات المرور من جهاز آخر آمِن
- إجراء فحص شامل بواسطة برنامج موثوق لمكافحة الفيروسات
- حفظ الأدلة الرقمية وإبلاغ الجهة التقنية أو مزوّد الخدمة



الوقاية من التصيُّد الاحتيالي

التَّحقُّق من عنوان المُرسِل بعناية، وعدم الاعتماد على الاسم الظاهر فقط

تجنُّب النقر على الروابط المشبوهة أو إدخال أيّ بيانات عبرها

الدخول إلى المواقع الرسمية يدويًّا بدلًا من استخدام الروابط المُرسَلة

حَذْف الرسائل المشبوهة والإبلاغ عنها

الوقاية من برمجيات الفدية

- الاحتفاظ بنُسَخ احتياطية مُحدَّثة للملفات المهمة
- تجنُّب فتح المرفقات أو الروابط غير المعروفة
- تحديث الأنظمة والبرامج لسدّ الثغرات الأمنية
- استخدام برامج حماية موثوقة ومُحدَّثة

التَّحقُّق من المحتوى

يساعد التَّحقُّق من المحتوى الرقمي في الحدّ من انتشار التضليل

مراجعة مصدر الصور والفيديوهات قبل تصديقها أو مشاركتها

استخدام أدوات الكشف عن التزييف عند توافرها

تجنُّب إعادة نشر المحتوى دون تحقّق

نَشْر الوعي بأهمية التفكير النقدي الرقمي



إعدادات الخصوصية

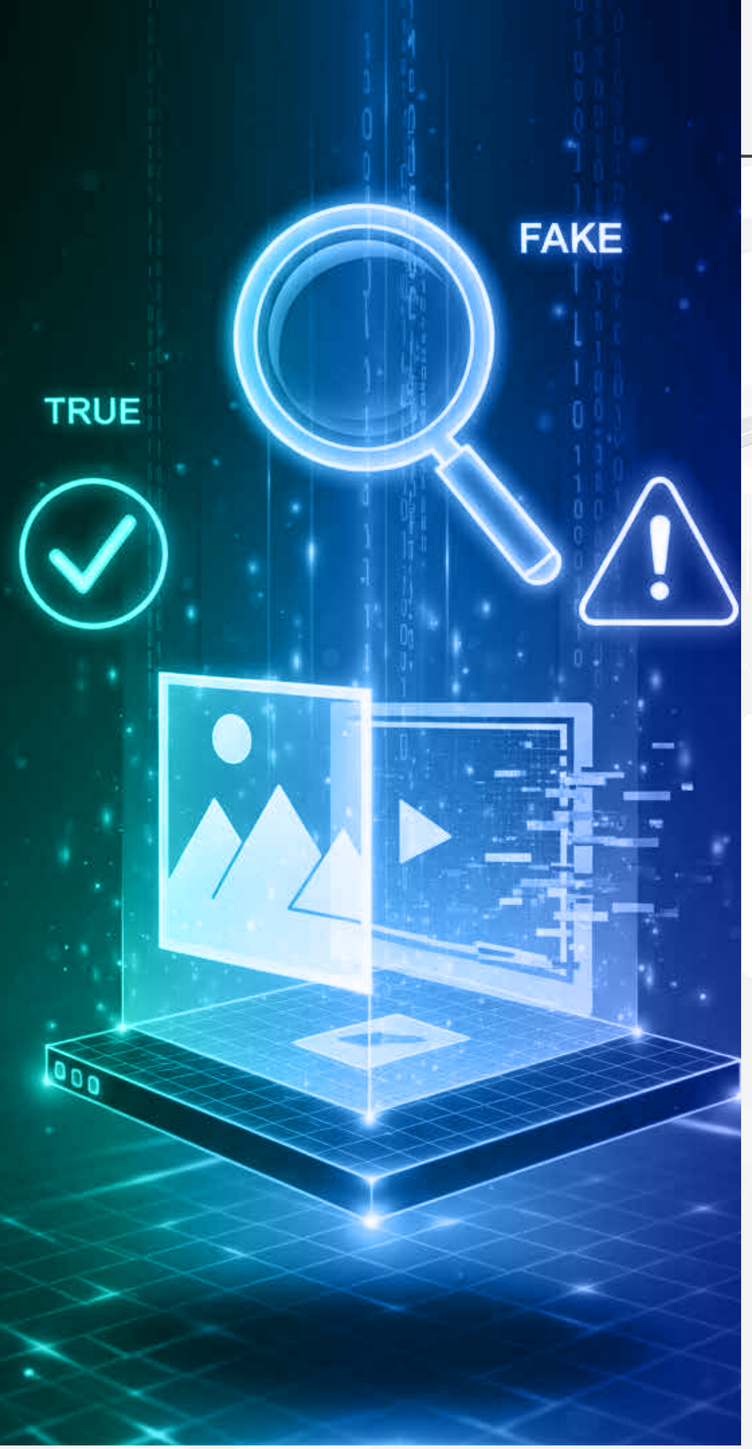
تلعب إعدادات الخصوصية دورًا مهمًّا في تقليل التتبُّع الرقمي وحماية البيانات الشخصية. ويتحقّق ذلك من خلال مجموعة من الإجراءات العملية، من أبرزها:

- مراجعة إعدادات الحسابات الاجتماعية، وتحديد مَن يمكنه رؤية المنشورات
- حَصْر قبول طلبات الصداقة بالأشخاص المعروفين
- عدم مشاركة تفاصيل الحياة اليومية بشكلٍ مُتكرّر
- ضَبْط إعدادات المتصفّح للحدّ من جمع البيانات

مَنْع المواقع من الوصول إلى الموقع الجغرافي
دون حاجة

مراجعة سياسات الخصوصية قبل الموافقة عليها

إعدادات الخصوصية غير المُفعَّلة قد تمنح الغرباء
إمكانية الوصول إلى البيانات الشخصية



السلوك الرقمي الآمِن

يُمثّل السلوك الرقمي السليم خطّ الدفاع الأول ضدّ التهديدات الإلكترونية. وتُعدّ الإجراءات التالية من أساسيات هذا السلوك:

- التفكير قبل النقر أو مشاركة أيّ محتوى عبر الإنترنت
- التَّحقُّق من مصادر الرسائل والمعلومات الرقمية قبل التفاعل معها
- تجنّب الاستجابة للرسائل المستعجلة أو المثيرة للقلق
- الالتزام بالإرشادات الأساسية للاستخدام الآمِن للتكنولوجيا



03 المحور الثالث

التَّصفُّح الآمِن للإنترنت



مخاطر التَّصفُّح العشوائي

ينطوي التَّصفُّح العشوائي للإنترنت على مخاطر متعددة قد لا تكون ظاهرة للمستخدِم

زيارة مواقع غير موثوقة قد تؤدي إلى تحميل برمجيات خبيثة دون عِلْم المستخدِم

التفاعل مع محتوى مُضلِّل أو احتيالي يزيد من فرص سرقة البيانات الشخصية

إدخال معلومات حسَّاسة في مواقع غير آمنة يُعرِّض المستخدم لخطر الاحتيال المالي

غياب الوعي الرقمي يجعل المستخدِم هدفًا سهلًا للهجمات الإلكترونية

الإعلانات المُضلّلة

تُستخدَم بعض الإعلانات المُموَّلة على الإنترنت كوسيلة لنشر الروابط الخبيثة

قد تدّعي تقديم خصومات أو فُرَص ربح فورية

النقر عليها يؤدّي إلى صفحات تُحمِّل برمجيات غير آمِنَة

استخدام إضافات حَجْب الإعلانات على المتصفّح يُعزّز الأمان

الروابط والمواقع المُزيَّفة



تنتشر المواقع المُزيَّفة التي تُحاكي واجهات المَتاجِر أو المؤسسات الرسمية لخداع المُستخدِمين

قد تحمل أسماء نطاق شبيهة بالمواقع الأصلية مع تغييرات طفيفة

تُستخدَم لجمع بيانات تسجيل الدخول أو معلومات الدفع

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

يُفضَّل الوصول للمواقع مُباشرةً من مُحرّك البحث وليس من روابط مُرسَلة



النوافذ المنبثقة

تُعدّ النوافذ المنبثقة وسيلة شائعة لخداع المستخدِمين في أثناء التَّصفُّح من خلال:

- إظهار رسائل تحذير وهمية تَدّعي إصابة الجهاز بفيروس
- دَفْع المستخدِم لتحميل برامج غير موثوقة بحجة الحماية
- تعطيل تجربة التَّصفُّح وتشتيت انتباه المستخدِم
- استغلال الضغط السريع على زِرّ الموافقة دون قراءة المحتوى



قواعد التَّصفُّح الآمِن

يشير التَّصفُّح الآمِن إلى استخدام الإنترنت بطريقةٍ تُقلِّل من المخاطر الرقمية المحتملة

الالتزام بالممارسات الصحيحة في أثناء تصفُّح المواقع يُسهم في حماية البيانات الشخصية من السرقة أو الاستغلال

الانتباه للمحتوى الذي يتم التفاعل معه يساعد في تجنُّب الوقوع ضحية لعمليات الاحتيال الإلكتروني

استخدام أدوات الحماية الأساسية في المتصفح يُعزّز مستوى الأمان أثناء التَّصفُّح اليومي

الوعي بالمخاطر المرتبطة بالإنترنت يُشكِّل خط الدفاع الأول للمستخدِم

التَّحقُّق من المواقع

يساعد التَّحقُّق من موثوقية المواقع في تقليل مخاطر الاحتيال الإلكتروني

التأكُّد من وجود بروتوكول HTTPS وعلامات الأمان في شريط العنوان

مراجعة عنوان الموقع بعناية قبل إدخال أيّ معلومات شخصية

تجنّب المواقع التي تحتوي على أخطاء لغوية أو تصميم غير احترافي

استخدام أدوات المُتصفّح التي تُنبِّه إلى المواقع غير الآمِنَة

بروتوكول HTTPS

يُعدّ بروتوكول HTTPS مؤشرًا أساسيًّا على أمان الاتصال بالموقع؛ إذ يهدف إلى حماية البيانات المتبادَلة وتعزيز موثوقية الموقع، وذلك من خلال:

- تشفير البيانات المتبادَلة بين المستخدِم والموقع لمنع اعتراضها
- تقليل فرص التلاعب بالمحتوى في أثناء نقله عبر الشبكة
- حماية معلومات تسجيل الدخول وبيانات الدَّفْع من التنصت
- تعزيز الثقة في الموقع المستخدم مقارنةً بالمواقع غير المشفّرة





البريد الإلكتروني

البريد الإلكتروني من أكثر الأدوات استخدامًا في الحياة الرقمية، لكنَّه في الوقت نفسه من أكثر القنوات التي تُستغَلّ في الهجمات السيبرانية. لذلك يتطلّب التعامل الآمِن مع رسائل البريد الإلكتروني الإجراءات التالية:

- التَّحقُّق من عنوان المرسل قبل فتح أيّ مُرفَق أو رابط
- عدم تحميل الملفات غير المتوقَّعة حتى من جهات معروفة دون تأكيد مسبق
- تجنُّب استخدام البريد الشخصي في التعاملات المهنية أو العامة
- حذف الرسائل المجهولة فورًا وعدم الردّ عليها

شبكات Wi-Fi العامة

على الرغم من سهولة الوصول إلى الشبكات العامة في المقاهي والمطارات؛ فإنها تُعدّ بيئة غير آمِنَة لتبادل البيانات الحساسة للأسباب التالية:

01 إمكانية اعتراض البيانات المتبادَلة بين الجهاز والشبكة

02 سهولة استهداف المستخدِمين المتصلين بنفس الشبكة

03 ضعف مستوى التشفير أو غيابه في معظم الشبكات العامة

04 زيادة خطر سرقة كلمات المرور والمعلومات الشخصية



الوقاية من مخاطر شبكات Wi-Fi العامة

تجنّب إدخال أيّ بيانات حسّاسة في أثناء الاتصال بشبكات عامة

استخدام خدمة VPN لتشفير الاتصال عند الضرورة

تعطيل الاتصال التلقائي بالشبكات غير المعروفة

التأكُّد من أن الموقع المستخدَم يبدأ ببروتوكول https

الشبكات الافتراضية الخاصة VPN

تساعد الشبكات الافتراضية الخاصة في تعزيز أمان التَّصفُّح من خلال:

- تشفير الاتصال بين الجهاز والإنترنت ومنع اعتراض البيانات
- حماية الخصوصية عند استخدام الشبكات العامة
- إخفاء عنوان الجهاز الحقيقي في أثناء التَّصفُّح
- تقليل مخاطر التجسُّس أو التتبُّع الرقمي

التسوُّق الإلكتروني

يتطلَّب التسوُّق الإلكتروني مستوى عاليًا من الحذر والوعي الرقمي؛ لذلك من الأفضل اتّباع مجموعة من الممارسات الوقائية التي تُسهم في تقليل مخاطر الاحتيال وحماية البيانات المالية، وتشمل ما يلي:

- إدخال بيانات الدفع في مواقع غير موثوقة يُعرِّض المستخدِم للخطر
- الاعتماد على عروض غير واقعية قد يكون مؤشرًا للاحتيال
- ضرورة التَّحقُّق من سُمعة المتجر قبل الشراء
- الاحتفاظ بسجلات المعاملات لمراجعتها عند الحاجة
- استخدام بطاقات الدفع الافتراضية أو محدودة القيمة قَدْر الإمكان
- تجنُّب إدخال المعلومات المصرفية في أجهزة أو شبكات عامة

المراجع

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

2. Cybersecurity and Infrastructure Security Agency (CISA). Malware, phishing, and ransomware., on site: https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

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

4. 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

5. IBM. Cost of a Data Breach Report 2025, on site: https://www.ibm.com/reports/data-breach

6. IBM. What is malware?, on site: https://www.ibm.com/think/topics/malware

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

8. Kaspersky. Ransomware WannaCry: All you need to know, on site: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

9. Kaspersky. What is a VPN? How it works, types, and benefits of VPNs., on site: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

10. Kosinski, Matthew. IBM. What is phishing?, on site: https://www.ibm.com/think/topics/phishing

11. Kosinski, Matthew. IBM. What is ransomware?, on site: https://www.ibm.com/think/topics/ransomware

12. National Cyber Security Centre (NCSC). Phishing., on site: https://www.ncsc.gov.uk/guidance/phishing

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

14. Orłowska, Agnieszka. Cybersecurity and Cyberthreats in Social Media., December 2022, on site: https://www.researchgate.net/publication/367048439_Cybersecurity_and_Cyberthreats_in_Social_Media

15. Susnjara, Stephanie. IBM. What is cloud computing?, on site: https://www.ibm.com/think/topics/cloud-computing





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