الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

حمايـة البيانـات الشخصيـة

الفئة المستهدفة

الجمهـور العـام

كُتَيّب المدرّب

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

حماية البيانات الشخصية

الفئة المستهدفة

الجمهور العام

كُتَيّب المُدَرّب

الفهرس	رقم الصفحـة
تمهيد	7
المبادرة الوطنية للسلامة الرقمية	8
المحور الأول: خصوصية البيانات	14
مفهوم خصوصية البيانات	15
أنواع البيانات الشخصية	16
مخاطر تسرُّب البيانات	17
التشريعات المتعلّقة بحماية البيانات في دولة قطر	18
الهوية الرقمية وحماية الخصوصية	19
استخدام التشفير لحماية البيانات	20
حماية البيانات من البرمجيات الخبيثة	21
حماية البيانات من هجمات التصيّد الاحتيالي	22
حماية البيانات الشخصية من الروابط الخبيثة	23
الحدّ من استغلال البيانات عبر المواقع المزوّرة	24

الفهرس	رقم الصفحـة
حماية البيانات المالية	25
الخصوصية على مواقع التواصل الاجتماعي	26
إدارة صلاحيات التطبيقات	27
إعدادات الخصوصية في الأنظمة التشغيلية	28
حماية الخصوصية في أثناء التصفح	29
الخصوصية في الألعاب الإلكترونية	30
الخصوصية في خدمات التخزين السحابي	31
كلمات المرور وحماية الخصوصية	32
المصادَقة الثنائية	33
الخصوصية في بيئات العمل	34
خصوصية الأطفال والمراهقين على الإنترنت	35
مؤشرات اختراق الخصوصية	36
ممارسات لتعزيز خصوصية البيانات	37

الفهرس	رقم الصفحـة
المحور الثاني: النقل الآمِن للبيانات	38
النقل الآمِن للبيانات	39
مخاطر نقل البيانات غير الآمِن	40
بروتوكولات الاتصال الآمِن	41
حماية البيانات في أثناء استخدام شبكات Wi-Fi العامة	42
مخاطر الشبكات العامة	43
الشبكات الافتراضية الخاصة (VPN)	44
النقل الآمِن للبريد الإلكتروني	45
حماية البيانات في أثناء المكالمات المرئية	46
النقل الآمِن للملفات	47
أمن البيانات في تطبيقات المراسلة	48
حماية البيانات في أثناء العمل عن بُعْد	49
أخطاء شائعة في نقل البيانات	50

الفهرس	رقم الصفحـة
مؤشرات تعرُّض البيانات للاختراق	51
المحور الثالث: الحذف الآمِن للبيانات	52
الحذف الآمِن للبيانات	53
الفرق بين الحذف التقليدي والحذف الآمِن	54
مخاطر بقاء البيانات بعد الحذف	55
الحذف الآمِن للملفات الرقمية	56
الحذف الآمِن من وحدات التخزين الخارجية	57
الحذف الآمِن من الهواتف المحمولة	58
الحذف الآمِن للبيانات السحابية	59
أدوات وبرامج الحذف الآمِن	60
الحذف الآمِن لبيانات الحسابات الرقمية	61
أخطاء شائعة في حذف البيانات	62
المراجع	63

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 الكُتَيّب إلى تعزيز الوعي بأبرز التهديدات التقنية التي قد نواجهها في حياتنا اليومية؛ من خلال توضيح مفاهيم خصوصية البيانات، وأساليب النقل الآمِن للمعلومات، وآليّات الحذف الآمِن، وتقديم إرشادات عملية تساعد الأفراد على التعامل المسؤول مع بياناتهم الشخصية، والحد من مخاطر إساءة استخدامها أو تعرّضها للاختراق

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

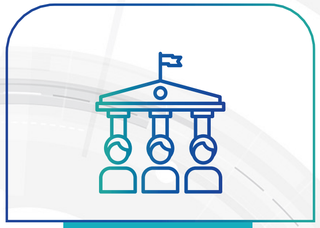
المرأة (العنف الرقمي ضد المرأة)

العاملون في المجال الصحي

المؤسسات العقابية والنيابة والمؤسسات الإصلاحية

الرياضيون

03 السنة الثالثة

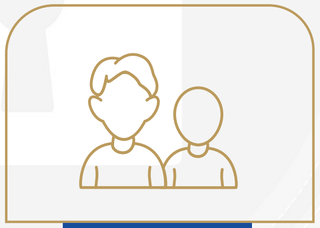


العاملون في وزارتي الدفاع والداخلية

العاملون في قطاع الطاقة

ذوو الاحتياجات الخاصة

العاملون في قطاع التعليم



اليافعون والشباب

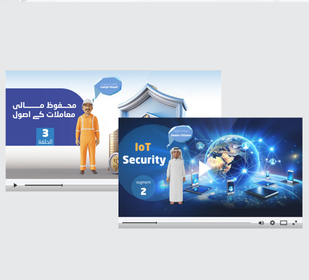
الجمهور العام

أدوات التوعية المعتمَدة في سياق المبادرة

دليل السلامة الرقمية

كُتيّبات توعية مطبوعة

شرائح العرض (للمُدرّبين)



فيديوهات التوعية (أنيميشن)

فيديوهات التوعية (تمثيلية)

الألعاب السيبرانية

بوابة التوعية السيبرانية

الروبوت التفاعلي

وِرَش التوعية

01 المحور الأول

خصـــوصية البيـــانـــات

مفهوم خصوصية البيانات

تُعدّ خصوصية البيانات أساسًا لحماية الأفراد في الفضاء الرقمي من إساءة استخدام معلوماتهم الشخصية

تشمل هذه الخصوصية

- تمكين الأفراد من التحكُّم في كيفية جَمْع بياناتهم واستخدامها ومشاركتها
- حماية البيانات من الوصول غير المصرَّح به أو الاستغلال غير المشروع
- الحد من تتبُّع الأنشطة الرقمية دون عِلْم المستخدِم أو موافقته
- ضمان الشفافية في سياسات جَمْع ومُعالجة البيانات
- تعزيز الثقة بين المستخدمين والمنصات الرقمية المختلفة

أنواع البيانات الشخصية

تتطلّب بعض البيانات مستوى أعلى من الحماية؛ نظرًا لتأثيرها المباشر على خصوصية الفرد وأمنه.

من أبرز هذه البيانات

- **البيانات التعريفية**، مثل: الاسم الكامل، رقم الهوية، وتاريخ الميلاد
- **بيانات الاتصال**، مثل: رقم الهاتف، البريد الإلكتروني، والعنوان السكني
- **البيانات المالية**، مثل: أرقام البطاقات البنكية وسجلات المعاملات
- **البيانات الصحية**، مثل: السجلات الطبية والمعلومات العلاجية
- **بيانات الموقع الجغرافي**، التي تُحدِّد تحرُّكات المستخدِم ومكان وجوده

مخاطر تسرُّب البيانات

سرقة الهوية

قد تُستخدَم البيانات المُسرَّبة لانتحال شخصية الأفراد، وإجراء معاملات غير قانونية

الاحتيال المالي

يؤدّي تسرُّب البيانات إلى مخاطر، مثل: اختراق الحسابات البنكية أو استخدام المعلومات الحساسة في عمليات الاحتيال

الإضرار بالسُّمعة

يمكن أن يُؤدّي تسرُّب البيانات إلى نشر معلومات شخصية حسَّاسة تضرّ بسُمعة الأفراد أو المؤسسات

الخسائر الاقتصادية

تسرُّب البيانات يُكلّف المؤسسات أموالًا طائلةً لإصلاح الأضرار الناتجة، وقد يؤدّي إلى عقوبات قانونية

فقدان الثقة

يُؤثّر التسرُّب على ثقة العملاء بالمؤسسات ويُضعف العلاقات التجارية؛ مما ينعكس سلبًا على الأداء المؤسسي

التشريعات المتعلّقة بحماية البيانات في دولة قطر

صدر القانون رقم (13) لسنة 2016 في دولة قطر بهدف حماية خصوصية البيانات الشخصية، وضمان حقوق الأفراد في بيئة رقمية آمِنَة.

يُحدّد القانون إطارًا قانونيًّا صارمًا يُنظّم عمليات جَمْع البيانات ومعالجتها وتخزينها ونقلها، بما يضمن الحد من سوء استخدامها أو تسريبها.

يمنح الأفراد الحق في التحكُّم ببياناتهم الشخصية، بما في ذلك الموافقة على جمعها، طلب تصحيحها أو حذفها، ومعرفة كيفية استخدامها مِن قِبَل المؤسسات.

يَفْرض التزامات قانونية على الجهات التي تجمع أو تعالج البيانات، مثل ضرورة اتخاذ تدابير أمنية مُشدَّدة لحمايتها، وضمان الشفافية في استخدامها.

يتماشى القانون مع المعايير الدولية، مثل اللائحة العامة لحماية البيانات (GDPR)، مما يجعله متوافقًا مع أفضل الممارسات العالمية في مجال حماية البيانات الشخصية.

يشمل القانون عقوبات صارمة على الجهات التي تنتهك أحكامه، تتراوح بين الغرامات المالية الضخمة وتعليق الأنشطة؛ لضمان الالتزام الصارم بحماية الخصوصية الرقمية.

الهوية الرقمية وحماية الخصوصية

تمثّل الهوية الرقمية الصورة المتكاملة للفرد في العالم الافتراضي، وتتكوّن من البيانات والممارسات التي تعكس وجوده على الإنترنت

ويتحقق الحفاظ على الهوية الرقمية من خلال

- الوعي بأن كلّ نشاط رقمي يترك أثرًا يمكن تجميعه لتكوين ملف رقمي عن المستخدِم
- تقليل ربط الحسابات المختلفة ببعضها للحد من تتبُّع السلوك الرقمي عبر المنصات
- استخدام أسماء مستخدمين مختلفة بحسب طبيعة المنصة ومستوى الخصوصية المطلوب
- مراجعة المعلومات الظاهرة للعامة في الحسابات الرقمية وإخفاء غير الضروري منها
- إدارة السمعة الرقمية بحذر لتجنُّب تكوين صورة رقمية غير دقيقة أو ضارّة

استخدام التشفير لحماية البيانات

تشفير البيانات يُوفّر وسيلةً فعّالةً لحمايتها من الوصول غير المُصرَّح به.

وينبغي مراعاة ما يلي

- تطبيق التشفير على البيانات المخزَّنة على الأجهزة المحمولة وأجهزة الحاسوب
- استخدام برامج تشفير قوية لتأمين الملفّات الحساسة
- تخزين البيانات في خدمات سحابية تُقدِّم التشفير التام لضمان الأمان
- تشفير البريد الإلكتروني والمرفقات عند إرسال معلومات حسَّاسة
- تفعيل خيارات التشفير على الأجهزة الذكية المتاحة في الإعدادات الافتراضية

حماية البيانات من البرمجيات الخبيثة

البرمجيات الخبيثة يمكن أن تؤدّي إلى فقدان البيانات أو استخدامها بشكل غير قانوني؛ لذا يجب اتخاذ تدابير للوقاية.

من أهمّ هذه التدابير:

- تثبيت برامج مكافحة الفيروسات ومكافحة البرمجيات الخبيثة، وتحديثها باستمرار
- الحذر عند تنزيل برامج أو ملفات من مصادر غير معروفة أو غير مَوْثوقة
- تفعيل خاصية المسح التلقائي للملفات عند تحميلها من الإنترنت
- تجنُّب فتح المرفقات أو الروابط الواردة في رسائل البريد الإلكتروني المشبوهة
- مراقبة أداء الجهاز لاكتشاف أيّ سلوك غير طبيعي قد يشير إلى وجود برمجيات خبيثة

حماية البيانات من هجمات التصيّد الاحتيالي

تستهدف هجمات التصيّد الاحتيالي خداع المستخدمين للحصول على بياناتهم الحساسة.

ويمكن الحدّ من مخاطرها من خلال:

- التحقُّق من هوية المرسِل، وعدم الثقة بالرسائل غير المتوقعة أو العاجلة
- تجنّب إدخال البيانات الشخصية عبر روابط واردة في رسائل مشبوهة
- الانتباه للأخطاء اللغوية أو الصياغات غير الاحترافية في الرسائل
- عدم مشاركة معلومات الدخول أو رموز التحقُّق مع أيّ جهة
- الإبلاغ عن رسائل التصيّد عبر القنوات الرسمية المتاحة

حماية البيانات الشخصية من الروابط الخبيثة

تُستخدم الروابط الخبيثة وسيلةً شائعةً لاختراق الأجهزة وسرقة البيانات

وللوقاية منها ينبغي:

- تجنُّب النقر على الروابط المجهولة أو المختصرة دون التحقُّق من مصدرها
- تمرير مؤشر الفأرة على الرابط لمعرفة العنوان الحقيقي قبل فتحه
- استخدام برامج الحماية التي تفحص الروابط وتمنع المواقع الضارة
- عدم تحميل ملفات من روابط غير موثوقة أو غير معروفة
- تحديث المتصفح ونظام التشغيل لتقليل فرص الاستغلال

الحدّ من استغلال البيانات عبر المواقع المزوّرة

تُنشأ المواقع المزوّرة لتقليد الجهات الموثوقة واستغلال بيانات المستخدمين.

ويمكن الحدّ من ذلك عبر:

- التأكُّد من صحة عنوان الموقع ووجود بروتوكول الاتصال الآمِن (https)
- عدم إدخال البيانات الشخصية أو المالية في مواقع غير معروفة
- تجنّب الوصول إلى المواقع عبر روابط واردة في رسائل مشبوهة
- استخدام محركات البحث للوصول إلى المواقع الرسمية بدل الروابط المباشرة
- الإبلاغ عن المواقع المزوّرة لحماية المستخدِمين الآخرين

حماية البيانات المالية

البيانات المالية حسَّاسة للغاية، وتتطلب إجراءات إضافية لضمان حمايتها من السرقة.

من أهم تلك الإجراءات

- استخدام بطاقات دَفْع إلكترونية مُؤمَّنة عند التسوُّق عبر الإنترنت
- التحقُّق من صحة المواقع التجارية قبل إدخال بيانات بطاقات الدفع
- الامتناع عن مشاركة بيانات الحسابات البنكية مع أطراف غير مَوْثوقة
- متابعة كشوف الحسابات البنكية بانتظام لاكتشاف أيّ نشاط مشبوه
- تفعيل الإشعارات الفَوْرية للحركات المالية لمراقبة الحسابات في الوقت الفعلي

الخصوصية على مواقع التواصل الاجتماعي

لضمان خصوصية البيانات الشخصية على منصات التواصل الاجتماعي؛ يجب اتخاذ خطوات استباقية تمنع سوء استخدامها.

من أهم تلك الخطوات ما يلي:

- ضبط إعدادات الخصوصية؛ بحيث تقتصر مشاركة المحتوى على الأصدقاء فقط
- تعطيل خاصية الإشارة التلقائية في الصُّوَر والمنشورات لتجنُّب انتهاك الخصوصية
- تجنُّب نَشْر المعلومات الحساسة، مثل: العنوان، رقم الهاتف، أو تفاصيل الحساب البنكي
- مراجعة إعدادات الخصوصية بشكلٍ دوريّ لتتوافق مع التحديثات الجديدة في المنصة
- قبول طلبات الصداقة فقط من الأشخاص المعروفين؛ لتقليل خطر التعرُّض للاحتيال أو التصيد

إدارة صلاحيات التطبيقات

التطبيقات المُثبَّتة على الأجهزة قد تطلب صلاحيات مفرطة تُؤثّر على الخصوصية والأمان. ولذا ينبغي مراعاة ما يلي:

مراجعة الصلاحيات المطلوبة من التطبيقات قبل تثبيتها

إلغاء الصلاحيات غير الضرورية، مثل: الوصول إلى الكاميرا أو الموقع الجغرافي

التحقُّق من سياسة خصوصية التطبيقات للتأكُّد من كيفية استخدام البيانات

إزالة التطبيقات غير المستخدَمة بشكلٍ منتظمٍ للحفاظ على الأمان

استخدام إعدادات الجهاز لإدارة الصلاحيات بشكلٍ دوريّ

إعدادات الخصوصية في الأنظمة التشغيلية

توفّر أنظمة التشغيل أدوات متقدّمة للتحكُّم في خصوصية البيانات على مستوى الجهاز.

من أبرز الممارسات

ضبط أذونات الوصول للتطبيقات بحسب نوع البيانات

تعطيل خدمات التتبُّع غير الضرورية، مثل: الموقع والخلفية

تفعيل خيارات الحماية الافتراضية المُوصَى بها من النظام

تحديث النظام دوريًّا لسدّ الثغرات الأمنية المحتملة

حماية الخصوصية في أثناء التصفح

يُعدّ التصفح الآمِن عنصرًا أساسيًّا للحد من تتبُّع الأنشطة الرقمية وحماية البيانات الشخصية.

يتحقق ذلك من خلال

- استخدام المتصفحات التي تُوفِّر إعدادات خصوصية متقدّمة
- تفعيل حظر ملفات تعريف الارتباط غير الضرورية وأدوات التتبُّع
- تجنُّب زيارة المواقع غير الموثوقة أو مجهولة المصدر
- التأكّد من استخدام بروتوكول الاتصال الآمِن (https) عند تصفُّح المواقع
- تحديث المتصفّح بانتظام لمعالجة الثغرات الأمنية

الخصوصية في الألعاب الإلكترونية

تتطلب الألعاب الإلكترونية وعيًا خاصًّا بالخصوصية؛ نظرًا لتفاعلها المستمر مع الإنترنت.

تشمل الممارسات الآمِنة ما يلي

- عدم مشاركة المعلومات الشخصية داخل منصات اللعب أو الدردشة
- استخدام أسماء مستخدمين لا تكشف عن الهوية الحقيقية
- ضبط إعدادات الخصوصية للتحكُّم في التواصل مع اللاعبين الآخرين
- الانتباه لعمليات الشراء داخل الألعاب وحماية البيانات المالية
- مراجعة سياسات الخصوصية الخاصة بمنصات الألعاب المختلفة

الخصوصية في خدمات التخزين السحابي

تُوفّر خدمات التخزين السحابي سهولة الوصول إلى البيانات، لكنّها تتطلب إدارة دقيقة للخصوصية.

من أبرز الإجراءات

- استخدام كلمات مرور قوية لحسابات التخزين السحابي
- تفعيل التشفير لحماية الملفات المخزَّنة
- تحديد صلاحيات الوصول عند مشاركة الملفات مع الآخرين
- مراقبة الأنشطة غير المعتادة على الحسابات السحابية
- حذف الملفات الحساسة غير الضرورية بشكل دوري

كلمات المرور وحماية الخصوصية

كلمات المرور هي خط الدفاع الأوَّل ضد الوصول غير المُصرَّح به للحسابات، وينبغي أن تكون قوية ومحمية.

اختيار كلمات مرور تتألف من 12 حرفًا أو أكثر، وتشمل حروفًا كبيرة وصغيرة وأرقامًا ورموزًا خاصة

تخصيص كلمة مرور فريدة لكل حساب أو جهاز؛ لتجنُّب التعرُّض للاختراق عند تسريب واحدة منها

الابتعاد عن الكلمات الشائعة، مثل: "123456"، أو الأسماء الشخصية لضمان صعوبة تخمينها

تغيير كلمات المرور بشكلٍ دَوْريّ لتقليل فرص الاستغلال في حالة الكشف عنها

استخدام برامج إدارة كلمات المرور لتخزين البيانات بشكلٍ آمِن بدلًا من حفظها يدويًّا

المصادقة الثنائية

إضافة طبقة حماية مزدوجة باستخدام المصادقة الثنائية يساعد على تأمين الحسابات بشكل أكبر، ولذا ينبغي مراعاة ما يلي:

تفعيل المصادقة الثنائية عند توفُّرها لحسابات البريد الإلكتروني ووسائل التواصل الاجتماعي

استخدام تطبيقات متخصّصة، مثل: Google Authenticator للحصول على رموز تحقُّق آمِنة

إعداد أسئلة أمان قوية يصعب على الآخرين تخمينها؛ لضمان تأمين الحسابات بشكلٍ أفضل

التأكد من أن الحسابات المصرفية والخدمات المالية تدعم هذه التقنية

الاحتفاظ بخطط استرداد الحساب في حال فقدان رموز المصادقة لتجنُّب إغلاق الحساب

الخصوصية في بيئات العمل

تتطلب بيئات العمل الرقمية توازنًا دقيقًا بين الإنتاجية وحماية البيانات الشخصية والمهنية

يتحقق ذلك من خلال

- الالـتزام بسياسـات الخصوصيـة المعتمـدة داخـل جهـة العمـل
- الفصـل بيـن الحسـابات والأجهـزة الشـخصية وحسـابات العمـل
- حماية بيانات العمل عند استخدام الشبكات والأجهزة الخارجية
- تقييـد الوصـــول إلـى المعلومـــات الحساســة وفـق الصلاحيـــات الوظيفيـــة
- الإبلاغ الفوري عن أيّ حادثة اشتباه بانتهاك الخصوصية

خصوصية الأطفال والمراهقين على الإنترنت

تُعدّ حماية خصوصية الأطفال والمراهقين أولوية؛ نظرًا لضعف وعيهم بالمخاطر الرقمية.

تشمل الإجراءات الأساسية

- توعية الأطفال بأساسيات الخصوصية الرقمية بلغة مبسطة
- تفعيل أدوات الرقابة الأبوية المناسبة لأعمارهم
- تقليل مشاركة الصور والمعلومات الشخصية الخاصة بهم
- مراقبة التطبيقات والألعاب المستخدَمة بانتظام
- تشجيع التواصل المفتوح للإبلاغ عن أيّ مواقف مقلقة

مؤشرات اختراق الخصوصية

يساعد التعرّف على مؤشرات اختراق الخصوصية في الحدّ من الأضرار المحتملة.

من أبرز هذه المؤشرات

- وصول غير مُبرّر إلى الحسابات أو تغيير الإعدادات دون عِلْم المستخدِم
- تلقّي رسائل أو إشعارات لم يتم تنفيذها مِن قِبَل المستخدِم
- ظهور إعلانات أو محتوى مخصَّص بشكلٍ غير معتاد
- بُطْء مفاجئ في أداء الأجهزة أو استهلاك غير طبيعي للبيانات
- تلقّي تنبيهات أمنية من الخدمات أو مزوّدي البريد الإلكتروني

ممارسات لتعزيز خصوصية البيانات

تعتمد حماية الخصوصية على عادات يومية بسيطة ولكن فعّالة.

تشمل هذه الممارسات

- تسجيل الخروج من الحسابات بعد الانتهاء من استخدامها
- تجنُّب مشاركة البيانات عبر الروابط أو الرسائل المجهولة
- قفل الأجهزة بكلمات مرور أو وسائل تَحقُّق بيومترية
- مراجعة الأذونات الممنوحة للتطبيقات بشكل دوري
- تحديث الأنظمة والتطبيقات للحفاظ على أعلى مستوى أمان

02 المحور الثاني

النقـــل الآمِـــن للبيـانـــات

النقل الآمِن للبيانات

يُقصَد بالنقل الآمِن للبيانات: حماية المعلومات في أثناء انتقالها بين الأجهزة أو الأنظمة المختلفة.

يتحقق ذلك من خلال:

- منع اعتراض البيانات أو الاطلاع عليها من جهات غير مُصرَّح لها
- ضمان سلامة البيانات، وعدم تعديلها في أثناء عملية النقل
- التحقُّق من هوية أطراف الاتصال قبل تبادل البيانات
- استخدام تقنيات أمان تحمي البيانات في أثناء الإرسال
- تقليل فرص الاختراق المرتبطة بالاتصالات الشبكية

مخاطر نقل البيانات غير الآمِن

يُؤدّي نقل البيانات دون وسائل حماية مناسبة إلى تهديدات أمنية متعددة.

من أبرز هذه المخاطر

- التلاعب بمحتوى البيانات في أثناء انتقالها
- تعرُّض البيانات للاعتراض مِن قِبَل أطراف غير مصرح لها
- فقدان الثقة بالأنظمة والخدمات الرقمية
- سرقة المعلومات الحساسة، مثل: بيانات الدخول أو المعاملات المالية
- زيادة احتمالية الهجمات الإلكترونية والتصيد الاحتيالي

بروتوكولات الاتصال الآمِن

توفّر بروتوكولات الاتصال الآمِن إطارًا تقنيًّا لحماية البيانات المتبادلة عبر الشبكات.

تشمل أهم وظائفها:

- تأمين قنوات الاتصال بين الأجهزة والخوادم
- التحقُّق من هوية المواقع والخدمات المتصلة
- تشفير البيانات المتبادلة تلقائيًّا في أثناء الاتصال
- منع هجمات التنصّت والتلاعب بالبيانات
- تعزيز موثوقية الاتصالات الرقمية

حماية البيانات في أثناء استخدام شبكات Wi-Fi العامة

شبكات Wi-Fi العامة قد تكون غير آمِنة؛ مما يجعلها عُرْضةً للاختراق. ولضمان الحماية في أثناء استخدامها ينبغي اتباع ما يلي:

- استخدام شبكات VPN لتشفير حركة البيانات، وضمان عدم قراءتها مِن قِبَل أطراف ثالثة
- الامتناع عن إدخال كلمات المرور أو البيانات الحساسة في أثناء استخدام شبكات مفتوحة
- تعطيل خاصية الاتصال التلقائي بالشبكات العامة؛ لتجنُّب الاتصال بشبكات غير موثوقة
- التحقُّق من أنّ المواقع التي يتم تصفُّحها تدعم بروتوكول HTTPS لحماية البيانات
- تجنُّب تنزيل الملفات من مصادر غير معروفة في أثناء استخدام شبكات عامة

مخاطر الشبكات العامة

تُشكّل الشبكات العامة بيئة عالية الخطورة لنقل البيانات.

من أبرز مخاطرها:

- انتشار هجمات التصيّد وسرقة بيانات الدخول
- سهولة اعتراض البيانات مِن قِبَل مستخدمين آخرين
- غياب التشفير أو ضعف آليات الحماية
- صعوبة التحقّق من موثوقية الشبكة ومزودها
- زيادة احتمالية إصابة الأجهزة بالبرمجيات الخبيثة

الشبكات الافتراضية الخاصة (VPN)

تُسهم الشبكات الافتراضية الخاصة في تعزيز أمان البيانات في أثناء النقل.

من خلال

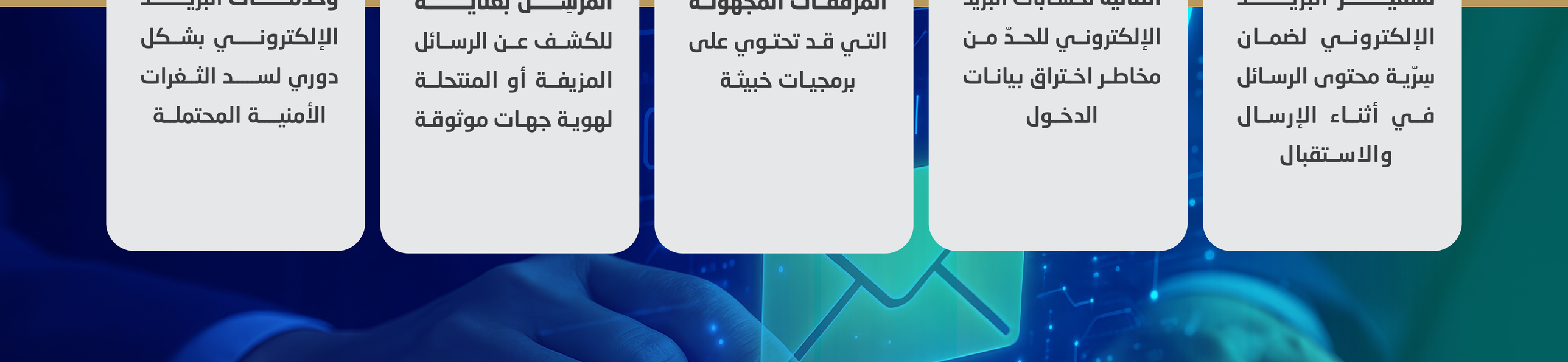
- تشفير حركة البيانات بين الجهاز والإنترنت
- إخفاء عنوان الإنترنت الحقيقي للمستخدِم
- حماية الاتصالات عند استخدام الشبكات العامة
- تقليل مخاطر التتبُّع والمراقبة الرقمية
- تعزيز الخصوصية في أثناء التصفُّح ونقل البيانات

النقل الآمِن للبريد الإلكتروني

يُعدّ البريد الإلكتروني من أكثر وسائل نقل البيانات استخدامًا، مما يجعله هدفًا شائعًا للهجمات الرقمية.

يتطلب تأمينه ما يلي

- استخدام بروتوكولات تشفير البريد الإلكتروني لضمان سِرّية محتوى الرسائل في أثناء الإرسال والاستقبال
- تفعيل المصادقة الثنائية لحسابات البريد الإلكتروني للحدّ من مخاطر اختراق بيانات الدخول
- تجنّب فتح الروابط أو المرفقات المجهولة التي قد تحتوي على برمجيات خبيثة
- التحقّق من عنوان المرسِل بعناية للكشف عن الرسائل المزيفة أو المنتحلة لهوية جهات موثوقة
- تحديث تطبيقات وخدمات البريد الإلكتروني بشكل دوري لسد الثغرات الأمنية المحتملة



حماية البيانات في أثناء المكالمات المرئية

تَعتمد المكالمات المرئية على نقل بيانات صوتية ومرئية حساسة تتطلب مستوًى عاليًا من الحماية. يتحقّق ذلك عبر

- استخدام منصات مكالمات مرئية تدعم التشفير الكامل للمحادثات الصوتية والمرئية
- تفعيل إعدادات الخصوصية التي تمنع انضمام أشخاص غير مخوّلين إلى الاجتماعات الافتراضية
- تجنّب مشاركة روابط الاجتماعات بشكل علني أو عبر قنوات غير آمنة
- التأكّد من تحديث تطبيقات المكالمات المرئية للاستفادة من تحسينات الأمان المستمرة
- إغلاق الكاميرا أو الميكروفون عند عدم الحاجة لتقليل مخاطر الوصول غير المصرّح به

النقل الآمِن للملفات

يُعدّ نقل الملفات الرقمية من العمليات الحساسة التي تتطلب حماية متقدّمة للبيانات.

يتم ذلك من خلال

- استخدام قنوات نقل مشفّرة تضمن حماية الملفات في أثناء الإرسال بين الأطراف المختلفة
- فحص الملفات قبل وبعد النقل للتأكد من خلوّها من البرمجيات الضارة
- تحديد صلاحيات الوصول للملفات بما يقتصر على الأشخاص المخوّلين فقط
- تجنّب استخدام وسائل نقل غير موثوقة أو غير معروفة المصدر
- حذف الملفات المنقولة من الأجهزة الوسيطة بعد اكتمال عملية النقل

أمن البيانات في تطبيقات المراسلة

تتطلب تطبيقات المراسلة حماية عالية؛ نظرًا لتبادل المعلومات الشخصية والمهنية عبرها.

يتحقّق أمن البيانات فيها عبر

- استخدام تطبيقات مراسلة تدعم التشفير التام بين طرفي الاتصال
- ضبط إعدادات الخصوصية للتحكّم فيمن يمكنه التواصل أو الاطلاع على المعلومات
- تجنّب مشاركة المعلومات الحساسة عبر تطبيقات غير موثوقة
- تحديث تطبيقات المراسلة بشكل منتظم لمعالجة الثغرات الأمنية
- تفعيل قفل التطبيق ووسائل التحقّق الإضافية لحماية المحادثات

حماية البيانات في أثناء العمل عن بُعد

أدَّى العمل عن بُعْد إلى زيادة الاعتماد على نَقْل البيانات عبر الشبكات، مما يتطلب ضوابط أمنية واضحة.

يتحقق ذلك من خلال

- استخدام شبكات اتصال آمِنَة ومشفّرة عند الوصول إلى أنظمة العمل من خارج مقر المؤسسة
- الفصل بين الأجهزة الشخصية وأجهزة العمل لتقليل مخاطر تسرب البيانات أو إساءة استخدامها
- الالتزام باستخدام أدوات وتطبيقات مُعتمدة من جهة العمل لنقل الملفات والمعلومات
- تفعيل وسائل التحقق متعددة العوامل لحماية حسابات العمل من محاولات الاختراق
- تحديث الأنظمة والأجهزة بشكل منتظم لمعالجة الثغرات الأمنية المرتبطة بالعمل عن بُعْد

أخطاء شائعة في نقل البيانات

تؤدي بعض الممارسات الخاطئة إلى تعريض البيانات لمخاطر غير ضرورية في أثناء النقل.

من أبرز هذه الأخطاء

- الاعتماد على أدوات أو تطبيقات غير موثوقة لنقل البيانات
- نقل البيانات عبر شبكات غير آمِنَة أو مفتوحة دون وسائل حماية
- مشاركة بيانات الدخول أو كلمات المرور بين المستخدمين
- إهمال استخدام التشفير عند إرسال المعلومات الحساسة
- عدم التحقّق من هوية الجهة المستقبِلة قبل إرسال البيانات

مؤشرات تعرُّض البيانات للاختراق

يساعد الانتباه إلى المؤشرات التحذيرية في تقليل الأضرار الناتجة عن تعرُّض البيانات للاختراق.

من أبرز هذه المؤشرات

- ظهور رسائل تحذير أمنية في أثناء أو بعد عمليات نقل البيانات
- بُطْء غير مُبرَّر في عمليات الإرسال أو الاستقبال
- تغيُّر محتوى البيانات أو تلف الملفات بعد اكتمال النقل
- تسجيل محاولات وصول غير معتادة في سجلات الأنظمة
- تلقّي إشعارات من الأنظمة بوجود نشاط شبكي مشبوه

03 المحور الثالث

الحذف الآمِن للبيانات

الحذف الآمِن للبيانات

يُقصَد بالحذف الآمِن للبيانات: إزالة المعلومات بشكل يمنع استعادتها أو الوصول إليها مستقبلًا.

يتحقق ذلك من خلال

- استخدام تقنيات متخصصة تضمن محو البيانات نهائيًّا من وسائط التخزين المختلفة دون إمكانية الاسترجاع
- حماية البيانات الحساسة من الوقوع في أيدي غير مُصرَّح لها بعد التخلُّص منها أو نقل ملكية الأجهزة
- الالتزام بالمعايير الأمنية التي تُنظِّم آليات حذف البيانات في البيئات الرقمية والمؤسسية
- تقليل مخاطر التسريب غير المقصود للمعلومات الناتج عن بقاء آثار رقمية للبيانات المحذوفة
- دعم الامتثال للسياسات والتشريعات المتعلقة بحماية البيانات والخصوصية

الفرق بين الحذف التقليدي والحذف الآمِن

يختلف الحذف الآمِن عن الحذف التقليدي من حيث مستوى الحماية الفعلية للبيانات. **يتضح الفرق في الآتي:**

01	الحذف التقليدي يزيل مرجع الملف فقط، بينما يضمن الحذف الآمِن إزالة البيانات نفسها من وسيط التخزين
02	يمكن استعادة البيانات المحذوفة حذفًا تقليديًّا باستخدام أدوات متخصصة، وهو ما يمنعه الحذف الآمِن
03	الحذف الآمِن يستخدم أساليب تقنية متقدمة مثل الكتابة فوق البيانات عدة مرات
04	يوفّر الحذف الآمِن حماية أعلى للبيانات الحساسة مقارنة بالحذف التقليدي
05	يُعدّ الحذف الآمِن خيارًا ضروريًّا عند بيع الأجهزة أو التخلص منها

مخاطر بقاء البيانات بعد الحذف

يؤدي بقاء البيانات بعد حذفها ظاهريًّا إلى مخاطر أمنية جسيمة. **من أبرز هذه المخاطر:**

- تمكين جهات غير مصرّح لها من استعادة المعلومات الحساسة بسهولة
- تعرُّض الأفراد أو المؤسسات لسرقة الهوية أو الاحتيال المالي
- انتهاك الخصوصية نتيجة الوصول إلى بيانات شخصية أو مهنية قديمة
- عدم الامتثال للمتطلبات القانونية المتعلّقة بحذف البيانات
- الإضرار بالسُّمعة المؤسسية أو الشخصية نتيجة تسريب البيانات

الحذف الآمِن للملفات الرقمية

يتطلب حذف الملفات الرقمية نهائيًّا اتباع إجراءات تتجاوز الحذف التقليدي. يتم ذلك من خلال

- استخدام أدوات حذف آمِن تضمن محو محتوى الملفات من وحدات التخزين
- التأكُّد من تطبيق الحذف الآمِن على جميع النُّسَخ الاحتياطية للملفات
- اختيار مستويات الحذف المناسبة بحسب حساسية البيانات
- التحقُّق من نجاح عملية الحذف وعدم إمكانية استرجاع الملفات

الحذف الآمِن من وحدات التخزين الخارجية

تتطلب وحدات التخزين الخارجية إجراءات خاصة لضمان عدم استرجاع البيانات.

يتحقق ذلك عبر

- استخدام أدوات مسح آمِن مخصَّصة للأقراص الخارجية ووسائط التخزين المحمولة
- تنفيذ عمليات الكتابة فوق البيانات لإلغاء إمكانية الاستعادة
- التحقّق من نجاح عملية الحذف قبل إعادة استخدام الوحدة أو التخلُّص منها
- تجنُّب الاعتماد على الحذف اليدوي أو السريع للملفات الحساسة
- الالتزام بسياسات التخلُّص الآمِن من وسائط التخزين المعتمدة

الحذف الآمِن من الهواتف المحمولة

تحتوي الهواتف المحمولة على بيانات مهمة وشخصية تتطلب حذفًا آمنًا قبل فقدانها أو نقل ملكيتها. يتحقق ذلك من خلال

تنفيذ إعادة ضبط المصنع باستخدام خيارات الحذف الآمِن المعتمدة في نظام التشغيل لضمان إزالة جميع البيانات

تسجيل الخروج من جميع الحسابات المرتبطة بالجهاز، وفصل خدمات النسخ الاحتياطي قبل بدء عملية الحذف

تشفير بيانات الهاتف مسبقًا لزيادة مستوى الحماية في حال تعذُّر الحذف الكامل

إزالة بطاقات الذاكرة الخارجية وبطاقات الاتصال التي قد تحتوي على بيانات إضافية

التحقُّق من عدم إمكانية استرجاع البيانات بعد اكتمال عملية الحذف

الحذف الآمِن للبيانات السحابية

يتطلب حذف البيانات المخزنة سحابيًّا إجراءات دقيقة لضمان عدم بقائها على الخوادم.

يتحقق ذلك عبر

- حذف الملفات نهائيًّا من الحسابات السحابية وعدم الاكتفاء بنقلها إلى سلة المهملات
- التأكُّد من حذف البيانات من جميع النسخ الاحتياطية المرتبطة بالحساب السحابي
- مراجعة سياسات مزود الخدمة لمعرفة آليات الحذف النهائي للبيانات
- إلغاء مشاركة الملفات مع الآخرين قبل تنفيذ عملية الحذف
- إغلاق الحسابات السحابية غير المستخدَمة لمنع بقاء البيانات دون رقابة

أدوات وبرامج الحذف الآمِن

توفّر أدوات الحذف الآمِن حلولًا تقنية تضمن إزالة البيانات نهائيًّا.

يتمثل دورها في

- استخدام برامج متخصصة تُطبّق معايير دولية معتمدة لمسح البيانات
- توفير تقارير تؤكّد نجاح عملية الحذف في البيئات المؤسسية
- تمكين الكتابة المتكررة فوق البيانات لمنع استعادتها بأيّ وسيلة
- تقليل الاعتماد على الحذف اليدوي غير الآمِن للملفات الحساسة
- دعم حذف البيانات من مختلف وسائط التخزين الرقمية
- الاعتماد على أدوات موثوقة ومعروفة مثل: Blancco - DBAN Eraser - BitRaser - Microsoft SDelete لتنفيذ الحذف الآمِن

الحذف الآمِن لبيانات الحسابات الرقمية

تتطلب بيانات الحسابات الرقمية حذفًا آمنًا عند إغلاق الحسابات أو تغيير استخدامها.

يتحقق ذلك عبر

- حذف الحسابات نهائيًّا من المنصات الرقمية وعدم الاكتفاء بتعطيلها مؤقتًا
- إزالة البيانات المرتبطة بالحساب من جميع الأجهزة المتصلة
- تغيير بيانات الدخول قبل الحذف لمنع أيّ وصول غير مصرّح به
- مراجعة سياسات المنصات لمعرفة آلية حذف البيانات نهائيًّا
- التحقّق من عدم بقاء أيّ معلومات شخصية مرتبطة بالحساب بعد الحذف

أخطاء شائعة في حذف البيانات

تؤدي بعض الممارسات الخاطئة إلى تعرض البيانات للخطر حتى بعد محاولة حذفها.

من أبرز هذه الأخطاء

- الاعتماد على الحذف اليدوي التقليدي دون استخدام أدوات آمِنَة
- عدم إزالة النسخ الاحتياطية أو البيانات المخزنة في السحابة
- تجاهل تشفير البيانات قبل الحذف، مما يسهل استرجاعها
- السماح بتنفيذ الحذف مِن قِبَل جهات غير مخوّلة أو غير مدربة
- عدم التحقّق من نجاح عملية الحذف بعد تنفيذها

المراجع

1. International Organization for Standardization. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO. on site: https://www.iso.org/standard/27001

2. International Organization for Standardization. (2019). ISO/IEC 27002:2019 — Information security controls. ISO. on site: https://www.iso.org/standard/75652.html

3. National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST SP 800-53 Rev. 5). U.S. Department of Commerce. on site: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

4. National Institute of Standards and Technology. (2014). Guidelines for media sanitization (NIST SP 800-88 Rev. 1). U.S. Department of Commerce. on site: https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

5. European Union. (2016). General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). Official Journal of the European Union. on site: https://eur-lex.europa.eu/eli/reg/2016/679/oj

6. European Union Agency for Cybersecurity. (2021). Guidelines on data protection and secure data transmission. ENISA. on site: https://www.enisa.europa.eu/topics/data-protection

7. Organisation for Economic Co-operation and Development. (2013). OECD guidelines on the protection of privacy and transborder flows of personal data. OECD Publishing. on site: https://www.oecd.org/privacy/oecd_privacy_framework.pdf

8. International Telecommunication Union. (2020). Guidelines on child online protection. ITU. on site: https://www.itu.int/cop

9. Cloud Security Alliance. (2021). Security guidance for critical areas of focus in cloud computing v4.0. CSA. on site: https://cloudsecurityalliance.org/research/guidance

10. SANS Institute. (2022). Data protection, encryption, and secure data disposal best practices. SANS. on site: https://www.sans.org/white-papers

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