القسم الثاني

التهديدات الرقمية الشائعة

التصيد — سرقة البيانات — الملاحقة — التجسس

التصيد الاحتيالي والهندسة الاجتماعية

i تعريف التصيد الاحتيالي

هو أسلوب خداع إلكتروني يستخدم المهاجمون فيه رسائل أو مواقع مزيّفة لسرقة كلمات المرور والبيانات الحساسة — يُمثِّل 15% من إجمالي حوادث الأمن السيبراني عالمياً.

أنواع التصيد الرئيسية

النوع	المؤشر
البريد الإلكتروني	ارتفع 202% — الأكثر انتشاراً
التصيد الصوتي Vishing	ارتفع 260% — انتحال صفة بنك
رموز QR — Quishing	تصاعد حاد — رموز مزيفة في الأماكن العامة
الهندسة الاجتماعية	ارتفع 141% — تلاعب نفسي للكشف عن بيانات

علامات رسالة التصيد

- **إلحاح مصطنع:** "فوراً" أو "خلال ساعة" أو "سيُغلَق حسابك"
- **طلب كلمة مرور أو كود OTP** — لا جهة شرعية تطلب ذلك أبداً
- **رابط URL مشبوه:** تحققي بالنقر الأيمن أو virustotal.com
- **أخطاء إملائية ونحوية** ورسائل عامة لا تذكر اسمك
- رموز **QR في أماكن عامة** لم تُنصَب من جهة رسمية معروفة
- **عروض هدايا غير متوقعة** أو تحذيرات تثير الخوف

⚠ قاعدة ذهبية

لا تنقري على أي رابط في رسالة تطلب تسجيل الدخول أو تأكيد بياناتك. افتحي الموقع يدوياً. يمكنك فحص أي رابط مشبوه عبر virustotal.com أولاً.

خطوات الاستجابة الفورية

١. غيِّري كلمة المرور فوراً من جهاز آمن آخر

٢. فعِّلي التحقق الثنائي إذا لم يكن مُفعَّلاً

٣. أبلغي المنصة عن الحساب أو الرسالة المزيّفة

٤. أبلغي البنك وأوقفي البطاقة إذا تعلق الأمر ببيانات مالية

٥. راجعي سجل نشاطات حسابك وأنهي أي جلسات مجهولة

⚠ تذكري دائماً

أفضل وقت لتبتدي فيه حماية معلوماتك الشخصية، كان بالأمس. لذلك تخصيص وقت شهريا لمراجعة حساباتك، وحمياتها، هو أقوى أداة في يدك.

سرقة بيانات الدخول والإنترنت الظلامي

ارتفعت نسبة التصيد الاحتيالي لبيانات تسجيل الدخول بنسبة 703% خلال النصف الثاني من 2024. تُباع بيانات البنوك المسروقة بمئات الدولارات في الدارك ويب.

703%
ارتفاع سرقة بيانات الدخول H2 2024
SlashNext

202%
ارتفاع هجمات البريد الإلكتروني H2 2024
SlashNext —

38M+
رابط احتيالي ضُغط عليه في أفريقيا خلال 2024–2025

كيف يصل المهاجمون إلى بياناتك؟

- رسائل بريد إلكتروني مزيّفة تحاكي مواقع موثوقة
- روبوتات تليغرام وبريد إلكتروني آلية تجمع البيانات
- مواقع الدارك ويب لعرض البيانات المسروقة وبيعها
- هجمات حصان طروادة المصرفية على الأندرويد

⚠ تحذير خاص بمصر

زادت هجمات حصان طروادة المصرفية على البنوك المصرية بنسبة 186%، محتلةً المرتبة الثالثة في الشرق الأوسط وأفريقيا بعد تركيا والكويت. (Kaspersky 2026)

أدوات التحقق المجانية

- **virustotal.com** — فحص أي رابط أو ملف مشبوه
- **Bitdefender Mobile** — مكافحة فيروسات للهاتف (نسخة مجانية)

سرقة الهوية واختراق الحسابات

+ 80%
من اختراقات البيانات سببها كلمات مرور ضعيفة أو مُعاد استخدامها

53%
من جرائم سرقة الهوية يحدث لحسابات التواصل الاجتماعي

+ 20%
ارتفاع خسائر سرقة الهوية في 2024 مقارنةً بـ 2023

أكثر الثغرات شيوعاً

- **كتابة كلمة مرور سهلة** التخمين أو تكرارها في حسابات متعددة
- **الإفراط في مشاركة المعلومات الشخصية** على منصات التواصل
- **اللعب في اختبارات Quiz** والإعلانات المُصمَّمة لجمع البيانات
- **ترك حسابات قديمة** دون إغلاق أو تعطيل
- **مشاركة بيانات الدفع البنكي (PIN)** مع الشريك أو الأسرة

الحماية العملية — 5 خطوات

- **استخدمي Bitwarden** لإنشاء كلمة مرور فريدة لكل حساب (+14 حرف وأرقام ورموز)
- **فعِّلي المصادقة الثنائية** على كل الحسابات الحساسة
- **راجعي إعدادات الخصوصية شهرياً** وأزيلي التطبيقات غير الضرورية
- **عطِّلي الموقع الجغرافي على التطبيقات** التي لا تحتاجينها
- **أغلقي الحسابات القديمة** غير المُستخدَمة

📖 علامات اختراق حسابك

إشعارات بتسجيل دخول مجهول | أصدقاؤك يتلقون رسائل لم ترسليها | لا تستطيعين الدخول بكلمة المرور المعتادة | منشورات لم تنشريها | تغيير البريد المرتبط بالحساب

التجسس والملاحقة الرقمية

⚠ تهديد ممنهج

المراقبة الرقمية تُستخدَم أداةً للسيطرة والإسكات — خاصةً في سياقات العنف الأسري أو مراقبة الناشطات.

26%
من الشابات المصريات تعرضن للملاحقة الرقمية

73%
من ضحايا المراقبة الرقمية نساء

67%
من الضحايا يشعرون بخوف من الأذى الجسدي

أدوات الملاحقة الرقمية

- **رسائل تهديد متكررة** عبر البريد الإلكتروني أو واتساب أو SMS
- **انتحال شخصية الضحية** عبر حسابات وهمية
- **زرع أجهزة تتبع GPS** في السيارة أو الأغراض الشخصية
- **برامج تجسس مُثبَّتة** سراً على الهاتف (Stalkerware)
- **مراقبة مزودي خدمة الإنترنت** — DPI (ثُبِّت استخدامه في مصر، AFTE 2018)

برامج التجسس المخفية — الأشهر عالمياً

- **mSpy** — تتبع الموقع والرسائل وسجل المكالمات
- **FlexiSpy** — وصول للكاميرا والميكروفون
- **xNSpy** — يعمل خفية باسم "System Service" أو "Device Care"
- **uMobix** — مخصص لمراقبة الأندرويد

التجسس والملاحقة الرقمية

⚠ برامج التجسس لا تود أن يتم كشفها

لذلك يمكن أن لا تكون التغييرات ظاهرة بشكل واضح، ويجب المراجعة بشكل دوري على أي نشاط غريب أو علامات غير طبيعية.

علامات الإصابة ببرنامج تجسس

- **البطارية تفرغ** بسرعة غير معتادة
- **الهاتف يسخن باستمرار** حتى في الراحة
- **ارتفاع استهلاك البيانات** في أوقات الراحة
- **تطبيقات مجهولة** بأسماء نظام مشبوهة
- **شخص يعلم** بما لم تخبريه

الحماية والإزالة

- **افحصي هاتفك** بشكل دوري
- **لا تناقشي الموضوع على الجهاز المشتبه به**
- **تواصلي** مع Access Now Helpline — مجاناً
- **أعيدي ضبط المصنع** إذا استمر الاشتباه واحتفظي بنسخة احتياطية أولاً

ملاحقة السلطات والأصول الرقمية في مصر

📖 تقرير مؤسسة حرية الفكر والتعبير (AFTE) 2018

وثّقت AFTE أن شركات الاتصالات في مصر (فودافون، اتصالات، WE) استخدمت أجهزة DPI للتدخل في حركة البيانات — السماح أو التعطيل أو التبطيء — عبر بروتوكول SSL. كما استغلّت البيانات المجموعة في حملات إعلانية وإعادة توجيه الروابط.

📖 تقرير Human Rights Watch 2022

وثّق HRW أن السلطات المصرية استهدفت المثليين/ات والمتحولين/ات جنسياً عبر الفضاء الإلكتروني، واستخدمت أدلة رقمية حصلت عليها بطريقة غير مشروعة من تطبيقات المواعدة ووسائل التواصل الاجتماعي.

الأصول الرقمية — ما يجب حمايته

- **الرسائل** والبريد الإلكتروني وسجلات المكالمات
- **الصور** ومقاطع الفيديو
- **الهواتف المحمولة** وأجهزة اللابتوب
- **أي أجهزة** متصلة بالإنترنت

حماية اتصالاتك في بيئة المراقبة

- **استخدمي تطبيق Signal للمراسلة** — تشفير كامل من الطرفين
- **استخدمي ProtonVPN المجاني** عند الحاجة للتصفح الآمن
- **استخدمي متصفح Tor** للأنشطة الحساسة
- **احذري من شبكات الواي-فاي العامة** — خاصةً قرب المقرات الأمنية

الأمان على الشبكات والبيانات

⚠ الواي-فاي العام — خطر دائم

الشبكات العامة غير مشفَّرة — أي شخص على نفس الشبكة يمكنه رؤية بياناتك.
استخدمي VPN دائماً أو تجنّبي الأعمال الحساسة عليها.

حماية الاتصالات — أولويات

- **VPN موثوق:** ProtonVPN (مجاني) أو Mullvad
- **Signal للمراسلة الحساسة** بدلاً من واتساب
- **البريد الإلكتروني المشفَّر:** ProtonMail
- **متصفح** Brave أو Firefox مع uBlock Origin

حماية البيانات والملفات الحساسة

- **وثائق الهوية والمراسلات الحساسة:** خزِّنيها محلياً مُشفَّرة (VeraCrypt)
- **النسخ الاحتياطي:** استخدمي تخزين سحابي مشفَّر أو قرص صلب خارجي
- **احذفي الملفات الحساسة نهائياً** (Secure Delete) وليس فقط سلة المهملات
- **بيانات EXIF في الصور:** احذفيها قبل النشر (Photo Metadata Remover)

إعدادات الأمان على منصات التواصل

المنصة	الإعدادات المهمة
Facebook	مراجعة الجلسات + إيقاف تتبع الموقع + حذف التطبيقات المرتبطة
Instagram	حساب خاص + قيود التعليقات + إيقاف موقع القصص
TikTok	حساب خاص + قيود الرسائل + مراجعة الوصول
Twitter/X	إيقاف تتبع الموقع + مراجعة التطبيقات المرتبطة

مراجعة شاملة لأمانك الرقمي — شهرياً

1. 15 دقيقة مراجعة الجلسات النشطة على كل حساباتك
2. فحص التطبيقات المرتبطة بحساباتك وحذف غير الضرورية
3. مراجعة إعدادات الخصوصية — خاصةً بعد تحديثات المنصة
4. تحديث نظام التشغيل والتطبيقات (الثغرات تُصلَح بالتحديثات)

الاتصالات الآمنة في العمل الحقوقي

للمحادثات الحساسة

استخدمي Signal دائماً مع تفعيل "الرسائل المختفية"

للاجتماعات الرقمية

Jitsi Meet أو Signal Calls أفضل من Zoom للاجتماعات الحساسة