دليل السلامة الرقمية
للنســـاء

كلمة افتتاحية

في ظل التحوّل الرقمي المتسارع الذي يعيشه العالم، باتت التكنولوجيا سلاحاً ذا حدَّين؛ فهي من جهة أداةٌ للتواصل والتعبير والتمكين، ومن جهة أخرى ساحةٌ للعنف والإيذاء والانتهاك. وتقع النساء والفتيات — ولا سيما اللواتي ينتمين إلى مجتمعات الأقليات الدينية أو الفئات الأكثر هشاشةً رقمياً في قلب هذه المخاطر.

يندرج هذا الدليل ضمن مشروع SAFE الرامي إلى تعزيز السلامة الرقمية لدى المجتمعات الأكثر عرضةً للخطر في مصر. وقد صُمِّم بلغة عربية واضحة ومُبسَّطة، لتكون أداةً عملية في يد كل من تحتاج إلى حماية رقمية.

هدف الدليل

يُعرِّفك هذا الدليل بأبرز التهديدات الرقمية التي تطال النساء والفتيات، ويُزوِّدك بخطوات عملية للحماية والاستجابة.

يغطي الدليل **ثمانية محاور رئيسية**: التزييف العميق، والمعلومات المضللة، والتحرش الإلكتروني، والتجسس والمراقبة، والتصيد الاحتيالي، وسرقة الهوية، ونشر الصور دون موافقة، وحملات الإيذاء المنظَّمة.

كيفية الاستفادة من هذا الدليل

يمكن قراءته من البداية للنهاية للحصول على صورة شاملة، أو الانتقال مباشرةً إلى القسم المتعلق بالتهديد الذي تواجهينه.

فهرس المحتويات

فهرس المحتويات

القسم الأول

أسس السلامة الرقمية

قبل مواجهة أي تهديد رقمي، تحتاجين إلى فهم بيئتك الرقمية وتقييم مخاطرك الخاصة.

مقدمة في السلامة الرقمية

السلامة الرقمية لا تعني امتلاك أحدث التقنيات، بل تعني فهم المخاطر واتخاذ قرارات واعية بشأن الأجهزة والتطبيقات والمعلومات التي نشاركها.
يرتكز **نهج السلامة الرقمية** علي ثلاث محاور متكاملة:

الحماية الوقائية
اتخاذ إجراءات استباقية لتقليل نقاط الضعف قبل وقوع الهجوم

الرصد والتنبيه
التعرف علي علامات التهديد المبكرة والاستجابة الفورية

الاستجابة والتعافي
خطة واضحة للتصرف بعد وقوع الحادثة والتعافي منها

لماذا يستهدف العنف الرقمي النساء أكثر؟

تُشير الإحصاءات العالمية إلى أن النساء يتعرّضن للتحرش الإلكتروني والعنف الرقمي بمعدل يفوق الرجال بمراتٍ عدة. في السياق المصري، تُضاف عوامل: التمييز الديني، القيود الاجتماعية، ومحدودية الوصول إلى آليات الإبلاغ.

أكثر من 73%
من النساء في العالم العربي تعرضن لشكل من التحرش الإلكتروني

أكثر من 8 مليون
امرأة مصرية تتعرض للإساءة الرقمية سنوياً

أكثر من 80%
من النساء عالمياً يواجهن شكلاً من العنف الإلكتروني

محاور الأمن الرقمي الثلاثة

الحماية الوقائية: اتخاذ إجراءات استباقية لتقليل نقاط الضعف
الرصد والتنبه: التعرّف على علامات التهديد المبكرة والاستجابة
الاستجابة والتعافي: خطة واضحة للتصرف بعد وقوع الحادثة

⚠ انتبهي
الشعور بالأمان الزائف هو أحد أخطر نقاط الضعف. كثيرات يظنّن أن مجتمعهم الصغير أو خصوصية حساباتهن تكفي للحماية — وهذا **غير صحيح.**

نموذج التهديد الشخصي

نموذج التهديد هو عملية تفكير منظَّمة تساعدك على فهم: **من قد يستهدفني؟ وبأي طريقة؟ ولحماية أي معلومات؟**

ليست كل امرأة في نفس موقع الخطر — الناشطة الحقوقية والصحفية تواجه تهديدات تختلف عن تهديدات طالبة الجامعة على سبيل المثال وليس الحصر. نموذج التهديد يساعدك على تخصيص حمايتك.

خطوات بناء نموذج التهديد الشخصي:

١. حدِّدي ما تريدين حمايته
٢. اعرفي من قد يريد الوصول إليه
٣. فهم احتمالية ذلك
٤. ضعي إجراءات مناسبة لمستوى الخطر
٥. راجعي النموذج دورياً

📖 "من حياتهم — قصة حقيقية"

س. صحفية على جهاز الكمبيوتر الخاص بها: تسجيلات مقابلات، وأسماء مصادر، ومسودات تقارير لم تُنشر بعد. لو وصل أحدٌ إلى هذه الملفات لم يكن شغلها وحده من سيتضرر — بل الأشخاص الذين وثقوا بها سيتعرضون للخطر.

حين فكّرت سارة في نموذج تهديدها الشخصي، أدركت أن خوفها الأكبر ليس الاختراق المباشر — بل أن تستيقظ يوماً لتجد جهازها مُصاباً وكل شيء قد مُحي. فاتخذت قراراً بسيطاً: **ضبطت تنبيهاً أسبوعياً يذكّرها برفع نسخة احتياطية مشفّرة.**

اليوم، لا تفكر سارة كثيراً في هذا الأمر — أصبح عادةً راسخة. التهديد لم يختفِ، لكنّ خطتها باتت واضحة. هذا بالضبط ما يفعله نموذج التهديد الشخصي — لا يُخيفكِ، بل يجعلكِ ترين الصورة بوضوح.

نموذج التهديد الشخصي

أسئلة لتقييم مستوى خطرك الرقمي

- هل تعملين في قضايا حقوقية أو دينية أو سياسية؟
- هل سبق أن تلقيتِ رسائل تهديد أو تحرش عبر الإنترنت؟
- هل تستخدمين نفس كلمة المرور لأكثر من حساب؟
- هل تستخدمين شبكات واي-فاي عامة بشكل منتظم؟
- هل تشاركين موقعك الجغرافي في التطبيقات أو المنشورات؟

مستوى الخطر	الوصف	التوصية
منخفض	مستخدمة عادية، مخاطر عامة	الإجراءات الأساسية
متوسط	ناشطة، صحفية، موظفة في منظمات	حماية مُعززة
مرتفع	مستهدفة بتهديدات محددة	بروتوكول أمان كامل

كلمات المرور وإدارة الهوية الرقمية

كلمة المرور هي أول خط دفاع. يستغرق اختراق كلمة مرور من 6 أحرف بسيطة أقل من ثانية، في حين تستغرق كلمة من 16 حرفاً مختلطاً آلاف السنين.

⚠ الأخطاء الشائعة

استخدام اسمك أو تاريخ ميلادك | كلمة واحدة لكل الحسابات | مشاركتها مع الشريك أو الأسرة | كتابتها في ملاحظات الهاتف

مواصفات كلمة المرور القوية

- 16 حرفاً على الأقل (معيار NIST 2024)
- تحتوي على أرقام وحروف كبيرة وصغيرة ورموز
- مختلفة لكل حساب
- لا تحتوي على معلومات شخصية

مثال: #h8_o+7G5u0=es **أو جملة:** أُحبّ-القهوة-في-الصباح-33!

i ما هو مدير كلمات المرور — Bitwarden

تطبيق يحفظ جميع كلمات مرورك بشكل آمن ومُشفَّر ويُنشئ كلمات مرور قوية تلقائياً. تحتاجين لتذكّر كلمة مرور رئيسية واحدة فقط.

التطبيق	التوصية	المنصات
Bitwarden	موصي به	مجاني، iOS, Android, Web
KeePassXC	ممتاز للكمبيوتر	مجاني، Windows, Mac, Linux
1Password	احترافي	مدفوع ولكل المنصات

التحقق الثنائي وطبقات الحماية

التحقق الثنائي (2FA) يعني إضافة طبقة حماية ثانية بعد كلمة المرور. حتى لو سُرقت كلمة مرورك، لن يستطيع المخترق الدخول بدون هذه الطبقة.

اجعليه عادةً

فعّلي التحقق الثنائي على: البريد الإلكتروني، واتساب، فيسبوك، إنستغرام، حسابك البنكي أولاً.

أنواع التحقق الثنائي — من الأضعف للأقوى

النوع	مستوى الحماية
رسالة SMS	**متوسط** — يمكن اعتراضه
تطبيق المصادقة	**جيد جداً** — Google Authenticator / Authy
مفتاح أمان فيزيائي YubiKey	**الأقوى** — للعمل الحقوقي

خطوات تفعيل التحقق الثنائي على واتساب

1. **افتحي واتساب** ← الإعدادات ← الحساب ← التحقق بخطوتين
2. **اضغطي:** تفعيل
3. **أدخلي** رقم PIN من 6 أرقام (احفظيه في مكان آمن)
4. **أضيفي** بريداً إلكترونياً للاسترداد

تحذير مهم

لا تُشاركي أكواد التحقق مع أي شخص — حتى من يدّعي أنه من دعم المنصة. هذا أسلوب شائع لاختراق الحسابات.

**الحساب المحمي بتحقق ثنائي يصعب اختراقه بنسبة 99% حتي لو كانت كلمة المرور مكشوفة.

مراجعة الإعدادات الأمنية

مراجعة دورية

خصصي 15 دقيقة كل شهر **لمراجعة إعدادات الأمان** على حساباتك الرئيسية.

مراجعة إعدادات Google

- **myaccount.google.com** ← الأمان
- **مراجعة التطبيقات** المرتبطة بحسابك
- **التحقق بخطوتين** ← التأكد من تفعيله
- **النشاط الأخير** ← البحث عن أي دخول مريب

مراجعة إعدادات فيسبوك

- **الإعدادات والخصوصية** ← الإعدادات
- **الأمان وتسجيل الدخول** ← مراجعة الأجهزة المتصلة
- **الخصوصية** ← مراجعة من يرى منشوراتك
- **الجلسات النشطة** ← أنهِي الجلسات المجهولة

تنبيه أمان

إذا وجدتِ جلسة نشطة من جهاز أو موقع لا تعرفينه، أنهيها فوراً **وغيِّري كلمة المرور.**

الخصوصية على منصات التواصل الاجتماعي

إعدادات الخصوصية الأساسية على إنستغرام

- **حساب خاص (Private Account)** — من يستطيع رؤية منشوراتك؟
- **أوقفي** إمكانية إضافتك لمجموعات دون إذن
- **استخدمي** الكلمات المقيَّدة لتصفية التعليقات المسيئة
- **أوقفي** إمكانية مشاركة موقعك في القصص
- **مراجعة التطبيقات** المرتبطة بحسابك

إعدادات الخصوصية على واتساب

- **الصورة الشخصية:** جهات الاتصال فقط
- **آخر ظهور:** لا أحد أو جهات الاتصال فقط
- **مجموعات:** من يستطيع إضافتك؟ ← جهات الاتصال فقط
- **فعِّلي التحقق بخطوتين**

⚠ لا تثقي بالقائمة العامة

حتى إذا كانت منشوراتك للأصدقاء فقط، فإن الأصدقاء قد يُشاركون لقطات شاشة. كوني حذرة بشأن المحتوى الحساس.

حماية الأجهزة المحمولة

i الهاتف أكثر من مجرد هاتف

هاتفك يحمل بريدك الإلكتروني، محادثاتك، صورك، بياناتك البنكية، وموقعك. حمايته تعني حماية كل ذلك.

إعدادات الأمان الأساسية للهاتف

- **رمز قفل قوي** (6 أرقام على الأقل أو بيومتري)
- **تشفير كامل للجهاز** (مُفعَّل افتراضياً في الهواتف الحديثة)
- **فعِّلي "ابحثي عن جهازي"** (Find My Device)
- **أوقفي الاتصال التلقائي** بشبكات الواي فاي العامة

في حال فقدان أو سرقة الهاتف

1. **استخدمي** Google Find My Device لتحديد موقعه
2. **أقفلي الجهاز** عن بُعد فوراً
3. **امسحي البيانات** عن بُعد إذا لم تتمكني من استرداده
4. **غيِّري كلمات مرور حساباتك** الرئيسية من جهاز آخر
5. **أبلغي البنك** إذا كان هناك تطبيق بنكي على الجهاز

تذكري: النسخ الاحتياطي

احتفظي بنسخة احتياطية منتظمة. في حال المسح عن بعد، ستفقدين كل ما على الهاتف. النسخة الاحتياطية تضمن عدم خسارة بياناتك.

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

القسم الثالث

العنف المُيسَّر بالتكنولوجيا

التحرش — الإساءة المنسَّقة — الإباحية الانتقامية

التحرش الإلكتروني وحملات الإسكات

العنف الرقمي هو امتداد للعنف الجسدي والنفسي في الفضاء الإلكتروني — آثاره حقيقية ومؤلمة. هو ليس "مجرد كلام" على الإنترنت.

أشكال العنف الرقمي

الشكل	الوصف
التنمر الإلكتروني	رسائل مسيئة متكررة — يستهدف الأطفال والشابات
التحرش الجنسي الرقمي	إرسال محتوى جنسي غير مرغوب أو ألفاظ مبتذلة
خطاب الكراهية	محتوى يستهدف المرأة بسبب جنسها أو دينها أو رأيها
الاستهداف الممنهج	هجوم جماعي منسق من حسابات متعددة
انتحال الشخصية	إنشاء حسابات مزيفة بهوية الضحية فيسبوك، إنستغرام
التشهير الإلكتروني (Doxxing)	نشر بيانات شخصية كالعنوان ورقم الهاتف

حملات التشويه

نشطت حملات التشويه في مصر خاصةً خلال جائحة كورونا، من خلال استهداف البريد الإلكتروني ومنصات التواصل.

التحرش الإلكتروني هو نمط من السلوك العدواني المتكرر عبر الفضاء الرقمي بهدف إيذاء الضحية أو ترهيبها أو إسكاتها.

لماذا ينتشر التحرش وكيف يعمل؟

- ✓ **الحسابات الوهمية:** تُتيح التحرش دون مساءلة
- ✓ **الهجمات العلنية على منصة X/تويتر** — الأكثر استخداماً في حملات الإسكات
- ✓ **الاستهداف داخل مجتمعات الألعاب الإلكترونية** — يطال الأطفال والنساء خاصةً
- ✓ **التشهير الإلكتروني (Doxxing):** نشر بريد إلكتروني أو رقم هاتف أو عنوان المنزل

التحرش الإلكتروني وحملات الإسكات

📖 كيف تعمل حملة الإسكات؟

تبدأ بمنشور أو تصريح للضحية، تنتشر عبر مجموعات واتساب أو تليغرام المغلقة لتنسيق هجوم متزامن، الهدف إغراق الضحية بالرسائل المسيئة حتى تُجبَر على حذف حسابها أو الصمت.

الاستجابة الفعلية

1. **لا تردّي** — الرد يُحفِّز المتحرش على الاستمرار
2. **وثّقي بلقطات شاشة** مع التاريخ والوقت قبل الحظر
3. **أوقفي إمكانية التعليق** على منشوراتك مؤقتاً
4. **أبلغي المنصة** عن الحساب المتحرش
5. **في مصر:** تواصلي مع مباحث الإنترنت أو منصة Speak Up (speakupeg.com)

🛡️ احتفظي بالأدلة قبل الحظر

حظر المتحرش لا يُنهي الأدلة — لكن يجب التوثيق أولاً حتي يُمكِّنك من الإبلاغ الرسمي إذا تطوّر الأمر.

الحماية القانونية في مصر

- **قانون الجرائم الإلكترونية رقم 175 لسنة 2018** — يُجرِّم اختراق الحسابات وانتهاك الخصوصية
- **قانون مكافحة التحرش رقم 64 لسنة 2021** — يُجرِّم التحرش الإلكتروني
- **للإبلاغ عن طريق Speak Up** أو مباحث الإنترنت أو المجلس القومي للمرأة

الإساءة الرقمية المنسَّقة
(الذباب الإلكتروني)

الإساءة الرقمية المنسَّقة ليست صدفة — هي استراتيجية ممنهجة لإسكات الأصوات النسائية في الفضاء العام.

آلية عمل حملة الإساءة المنسَّقة — 4 مراحل

① **الاستكشاف**	جمع معلوماتك من المنصات العامة — مكان العمل، العائلة، الصور، الموقع
② **التنسيق**	مجموعات واتساب وتليغرام مغلقة لتنسيق توقيت الهجوم
③ **الهجوم**	إغراق مفاجئ بالتعليقات المسيئة من حسابات متعددة في وقت قصير
④ **التصعيد**	نشر المعلومات الشخصية *(Doxxing)*، تهديدات، إبلاغ جماعي لتعليق الحساب

التعامل مع الإساءة المنسَّقة

1. **احفظي الأدلة:** روابط ولقطات شاشة مع التاريخ والوقت قبل أي إجراء
2. **لا تردّي علناً** — الرد يضخّم الهجوم ويمنحه مزيداً من الظهور
3. **بلغي** المنصة عن نمط الإساءة الممنهجة وليس فقط حساباً واحداً
4. **تواصلي** مع شبكة دعم موثوقة قبل اتخاذ أي إجراء
5. **فكّري** في تقليل حضورك العام مؤقتاً خلال ذروة الهجوم

الإباحية الانتقامية ونشر الصور دون موافقة

⚠ محتوى حساس

هذا القسم يتناول موضوعاً صعباً. تذكري: **لستِ مذنبة. والمسؤولية تقع كاملاً على من ارتكب ذلك.**

لا توجد إحصاءات رسمية شاملة في مصر تحدد حجم هذة الجرائم، لأن أغلب الحالات لا تُبلّغ، ولا تُوثّق، وتُدفن تحت مسمى "الستر". لكن الدراسات الميدانية والتحقيقات القانونية والطبية تكشف جانبًا من الحقيقة التي لا تظهر في الأرقام.

📖 وقائع موثَّقة

في أكتوبر 2025، تعرضت مطربة في مصر تدعى ر.م إلى نشر فيديوهات إباحية دون موافقتها، جزءاً من حملة ابتزاز شنّها زوجها لمقابل مالي. وفي 2022، أعلنت وزارة الداخلية القبض على رجل سرّب فيديو حميم لامرأة رفضت طلب الزواج منه.

ماذا تفعلين إذا تعرضتِ للتهديد؟

- **لا تدفعي الفدية أبداً** — يُشجِّع المبتزّ على الاستمرار
- **لا تحذفي الأدلة** — احتفظي بلقطات شاشة مع التاريخ والوقت
- **لا تشاركي المحتوى** حتى لإثبات أنه مُزيَّف
- **أبلغي المنصة فوراً:** "محتوى جنسي غير موافَق عليه"
- **سجِّلي في StopNCII.org** مجاناً
- **أبلغي مباحث الإنترنت** أو اطلبي دعماً قانونياً

أداة StopNCII.org — درعك الرقمي

ما هي StopNCII؟

أداة مجانية طوّرتها منظمة Revenge Porn Helpline. لا تُرفَع الصورة إلى الموقع — يُنشئ فقط بصمة رقمية (Hash) منها على جهازك ثم يشاركها مع المنصات الشريكة لمنع نشرها.

المنصات الشريكة في StopNCII

- Facebook, Instagram, Threads — Meta
- Google, YouTube
- Reddit, Snapchat, WhatsApp
- PornHub وعدد من المواقع الإباحية الكبرى

خطوات استخدام StopNCII.org

1. **افتحي** StopNCII.org من متصفحك
2. **حددي الصورة أو المقطع من على جهازك** — لن يُرفَع للموقع
3. **ينشئ الموقع بصمة رقمية** ويخزنها ويرسلها للمنصات الشريكة
4. **تتحقق المنصات الشريكة باستمرار** وتزيل أي تطابق تلقائياً
5. **احتفظي برقم القضية وPIN للمتابعة** — غير قابلَين للاسترداد
6. **راجعي حالتك دورياً** باستخدام رقم القضية

معلومات مهمة

إذا قُصَّت الصورة أو أضيفت عليها فلاتر، لن تتعرف التجزئة عليها. استخدمي دائماً الصورة الأصلية. الملف الأصغر حجماً يُجزَّأ بشكل أفضل للفيديو.

أداة StopNCII.org — درعك الرقمي

⚠ لا تدفعي الفدية

دفع الفدية للمبتزّ لا يوقف الأمر — بل يُثبت له أن الضغط يُجدي نفعاً ويُشجعه على التصعيد.

الحقوق القانونية في مصر

i قانون مكافحة التحرش رقم 64 لسنة 2021

يُجرِّم التحرش الجنسي بما في ذلك الإلكتروني. العقوبة تصل إلى 3 سنوات سجن وغرامة مالية.

Doxxing — نشر المعلومات الشخصية

⚠ ما هو Doxxing؟

هو نشر معلوماتك الخاصة (عنوان منزلك، رقم هاتفك، مكان عملك) دون إذنك بهدف تمكين آخرين من استهدافك في الواقع الفعلي.

المعلومات التي يبحث عنها المُهاجمون

- ✓ عنوان السكن ومكان العمل وأوقات الحضور
- ✓ أسماء أفراد الأسرة والحيوانات الأليفة
- ✓ الصور التي تكشف الموقع الجغرافي (بيانات EXIF)
- ✓ رقم الهاتف الشخصي

1. ابحثي عن اسمك على Google وراجعي ما يظهر
2. أزيلي معلوماتك من مواقع الكتاب الهاتفي عبر الإنترنت
3. أوقفي ظهور موقعك الجغرافي في الصور (EXIF Data)
4. لا تُشاركي عنوان منزلك أو روتينك اليومي علناً

أداة مجانية: EXIF Tool

قبل نشر أي صورة، احذفي بيانات الموقع المخفية باستخدام تطبيق Photo Metadata Remover.

**الـ Meta Data هي البيانات التي يتم أضفاتها تلقائيا على أي ملف مثل الموقع الجغرافي للصور، نوع الهاتف، الوقت الذي تم أخذ الصورة أو انشاء الملف فيه. عن طريقها يستطيع الهاتف كمثال بترتيب صورك على الهاتف، لكن بعض المهاجمين يستطيعون استعمالها للوصول إليكي.

إيقاف تسجيل الموقع الجغرافي

إيقاف تسجيل الموقع الجغرافي (EXIF Data) في الصور خطوة ضرورية لحماية خصوصيتك، وتختلف الطريقة حسب نوع هاتفك:

1. إيقاف الموقع في الصور على الآيفون (iPhone/iOS)

- افتح **الإعدادات** (Settings).
- انتقل إلى **الخصوصية والأمان** (Privacy & Security).
- اضغط على **خدمات الموقع** (Location Services).
- ابحث عن **الكاميرا** (Camera) واضغط عليها.
- اختر **أبداً** (Never) لإيقاف تسجيل الموقع نهائياً في الصور المستقبلية.

2. إيقاف الموقع في الصور على أندرويد (Android)

- افتح تطبيق **الكاميرا** (Camera).
- اضغط على **الإعدادات** (غالباً رمز الترس⚙️).
- ابحث عن خيار **علامات الموقع** (Location tags/geo tag) وقم بإيقافه.
- طريقة أخرى: انتقل إلى **إعدادات الهاتف** < **الموقع** < **أذونات التطبيقات** < **الكاميرا**، وقم بإيقاف الوصول للموقع.

3. إزالة الموقع من صور تم التقاطها بالفعل (حذف الـ EXIF)

- **على iPhone:** افتح الصورة، اضغط على **المزيد** (i)، ثم **ضبط الموقع**، واختر **لا يوجد موقع**.
- **على Android:** افتح الصورة في "صور Google"، اضغط على النقاط الثلاث، ثم **إزالة الموقع الجغرافي**.
- **باستخدام تطبيقات:** يمكن تحميل تطبيقات مثل "Exif Metadata Remover" لإزالة البيانات بالكامل قبل مشاركة الصور.

دليل الإبلاغ على المنصات الكبرى

الإبلاغ على فيسبوك

1. اضغطي على النقاط الثلاث (•••) فوق المنشور أو على الملف الشخصي
2. اختاري 'الإبلاغ'
3. حددي النوع: تحرش، عنف، محتوى جنسي، حساب مزيّف

الإبلاغ للشرطة المصرية

i الخطوات الرسمية

١. توجّهي لأقرب مركز شرطة مع لقطات الشاشة
٢. اطلبي تحرير محضر للتحرش الإلكتروني أو الابتزاز
٣. إذا رُفِض البلاغ، توجّهي للنيابة العامة
٤. يمكنك الاستعانة بمنظمة حقوقية

⚠ احتفظي بنسخ من كل التوثيق

الأدلة الرقمية تُحذَف بسرعة. احتفظي بلقطات الشاشة وعناوين URL والتواريخ في مكانين مختلفين على الأقل.

العنف الرقمي في العلاقات الحميمية

⚠ العنف الأسري الرقمي

كثيراً ما يُستخدَم التحكم الرقمي — مثل مراقبة الهاتف — كأحد أشكال العنف المنزلي. إذا كنتِ في علاقة مُسيئة، فسلامتك تأتي أولاً.

علامات التحكم الرقمي في العلاقات

✓ مطالبتك بتسليم كلمات مرورك
✓ تثبيت تطبيقات على هاتفك دون إذنك
✓ متابعة موقعك على مدار الساعة
✓ التهديد بنشر صور أو معلومات

خطوات لمساعدتك

1. استخدمي جهازاً أو شبكةً آمنة للتخطيط
2. أنشئي حساباً بريدياً سرياً لا يعرف به الشريك
3. احتفظي برقم طوارئ موثوق في مكان آمن
4. تواصلي مع خط نجدة للمرأة: 16021

⚠ احتفظي بنسخ من كل التوثيق

الأدلة الرقمية تُحذَف بسرعة. احتفظي بلقطات الشاشة وعناوين URL والتواريخ في مكانين مختلفين على الأقل.

القسم الرابع

التزييف والمعلومات المضللة

الحملات المضللة — التزييف العميق — الذكاء الاصطناعي والجريمة

الحملات المضللة الموجَّهة

الحملات المضللة أصبحت جزءاً من الحروب النفسية باستخدام التكنولوجيا — تستهدف الرأي العام والناشطات وصانعات السياسات على حدٍّ سواء.

أنواع المعلومات المضللة

- تلفيق المحتوى الكاذب تماماً
- التلاعب بمحتوى حقيقي — عناوين مضلِّلة أو صور مقتطعة من سياقها
- انتحال صفة — استخدام علامة تجارية لجهة موثوقة
- محتوى دقيق مقرون بسياق مغلوط
- السخرية تُعرَض على أنها حقيقة
- الروابط الزائفة التي لا تدعم ما تدّعيه

أدوات الحملات المضللة

- **الروبوتات:** برامج آلية قادرة على الوصول لـ 10,000 مستخدم وإيهامهم بمعارضة جماعية
- **الذكاء الاصطناعي:** يُنتج محتوىً مُقنعاً ومزيفاً من نصوصاً وصوراً
- **الحسابات الوهمية (اللجان الإلكترونية):** انتحال هوية أطراف أخرى للتلاعب بالرأي العام
- **الموقع الجغرافي:** استهداف دقيق لضحايا بعينهن
- **الإغراق الإعلامي:** رسائل متشابهة لإسكات الجهات المعارضة

الحملات المضللة الموجَّهة

كيف تحمين نفسك — طريقة SIFT للتحقق السريع

الحرف	الإجراء
S — Stop	توقّفي — لا تتفاعلي فوراً
I — Investigate	تحققي من المصدر
F — Find better sources	ابحثي عن مصادر أفضل
T — Trace claims	تتبّعي مصدر الادعاء الأصلي

تتعدد أدوات التحقق من الحملات المضللة الموجهة لتشمل تقنيات الكشف عن الحسابات الوهمية، تحليل الشبكات، والتحقق من الوسائط.

أدوات التحقق المجانية

- **فتبيّنوا (fatabyyano.com)** — للمحتوى العربي
- **مسبار (misbar.com)** — تحقق من الأخبار العربية
- **Google Reverse Image** — البحث العكسي عن الصور
- **Google Alerts** — مراقبة الشائعات عن منظمتك مجاناً

التحقق من المعلومات والصور

🛡️ قبل المشاركة — توقّفي 30 ثانية
السؤال قبل المشاركة ليس شكّاً — هو مسؤولية رقمية.

أسئلة تطرحينها على كل خبر تتلقينه

- من كتب هذا الخبر؟ هل المصدر موثوق؟
- متى نُشر؟ هل هو حديث أم قديم مُعاد تداوله؟
- لماذا يُشاركني الآن؟ ما الهدف؟
- هل هناك مصادر أخرى تؤكده؟
- هل يُثير مشاعر قوية جداً؟ (الإثارة المفرطة علامة تحذير)

التحقق من الصور

- **Google Reverse Image Search** — ابحثي عن مصدر الصورة الأصلية
- **TinEye.com** — تتبع أول ظهور للصورة على الإنترنت
- **ابحثي** عن تباعد الألوان أو العلامات المائية غير الاحترافية
- **تحققي من اسم النطاق** — قد يحتوي على أخطاء مقصودة مثل: gooogle.com

التحقق من الفيديوهات

- ابحثي عن عدم تزامن حركة الشفاه مع الصوت
- راقبي حدود الوجه — التشوهات عند الأذنين والأنف
- انتبهي لأنماط الإضاءة غير المتسقة بين إطار وآخر
- استخدمي أدوات كشف التزييف مثل: Hive Moderation أو Sensity.ai

التزييف العميق — Deepfakes

⚠ تهديد مباشر للنساء

التزييف العميق يُستخدَم بصورة متزايدة لإنشاء صور وفيديوهات مُزيَّفة للنساء في سياقات إباحية أو مُهينة دون موافقتهن. 98% من فيديوهات التزييف العميق الجنسية تستهدف النساء — Security Hero 2023. واكثر من 50% من النساء المصريات تعرضن للعنف الرقمي — مرصد الأزهر 2025.

ما هو التزييف العميق؟

بدأ التزييف العميق عام 2014 حين قدّم الباحث إيان غودفيلو فكرة الشبكات التوليدية التنافسية GANs. في 2017 انتشر على Reddit. منذ 2018 أصبح أداةً للاحتيال والابتزاز.

كيف يعمل التزييف العميق؟ — الشبكات التوليدية التنافسية (GANs)

تتكوّن من شبكتين عصبيتين: المولّد يصنع المحتوى المزيف، والمميّز يحدد إذا كان حقيقياً. يتنافسان حتى ينتج المولّد مقطعاً لا يستطيع المميّز اكتشافه.

أساليب التزييف

- **تبديل الوجوه:** استبدال وجه شخص بوجه آخر في الفيديو
- **تغيير الملامح:** لون البشرة، الشعر، تعبيرات الوجه
- **محاكاة حركة الشفاه:** تركيب صوت شخص على وجه آخر
- **التوليد الكامل بالذكاء الاصطناعي:** إنشاء شخصية كاملة غير حقيقية

التزييف العميق — Deepfakes

علامات تكشفين بها التزييف

- الرمش غير طبيعي أو غائب تماماً
- الشفاه لا تتزامن مع الصوت
- تغيرات في لون البشرة من إطار لآخر
- تشوهات عند الأذنين والأنف
- إضاءة غير متسقة بين الوجه والجسد
- الشخص يرفض الالتفات أو التحرك بشكل طبيعي
- جودة مختلفة بين منطقة الوجه وبقية الصورة

📖 شركة Arup — احتيال بالتزييف العميق 2024

في مطلع 2024، خسرت شركة Arup الهندسية 25 مليون دولار بعد مكالمة فيديو مزيّفة انتحل فيها المهاجمون صفة المدير المالي وموظفين آخرين. وفي نفس العام، استُخدم تزييف صوتي لانتحال صفة الرئيس بايدن في الانتخابات التمهيدية.

الحماية من التزييف العميق

كيف تحمين نفسك؟

- قبل مشاركة أي فيديو — خذي 30 ثانية للتحقق من المصدر
- لا تشاركي محتوى يستخدم صورتك حتى لإثبات أنه مُزيَّف
- أبلغي المنصة فوراً عن أي محتوى مزيَّف يستخدم وجهك أو صوتك
- سجِّلي في StopNCII.org إذا كان المحتوى جنسياً
- استشيري محامياً أو منظمة حقوقية متخصصة

📖 المستوى المجتمعي

توصي منظمة WITNESS بخلق آليات والتزامات دولية مع الشركات للمساهمة في مساءلة إساءة استخدام الذكاء الاصطناعي وإنشاء محتوى فاضح دون موافقة، وتزويد الناشطات والصحفيات بأدوات الحماية اللازمة.

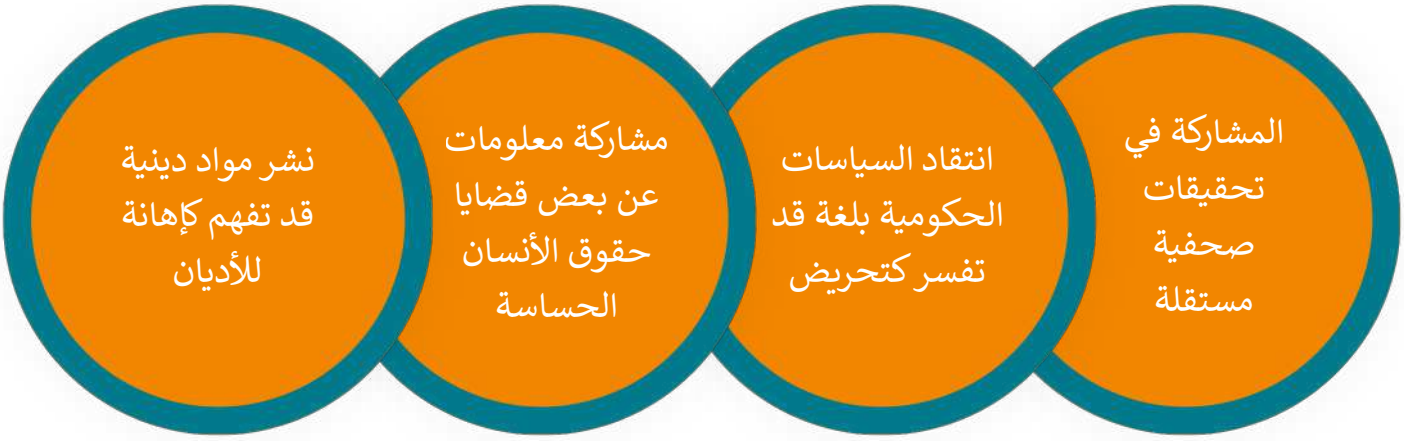
قضايا سلامة المحتوى والتعبير

متي يصبح التعبير الرقمي خطرا؟

التوازن الدقيق

حقك في التعبير عبر الانترنت مكفول قانونيا لكن بعض المحتوي يعرضك لمخاطر قانونية أو أمنية في السياق المصري. الوعي بهذا التوازن ضروري.

محتوي قد يعرضك لمخاطر



📖 **مورد مهم: دليل EFF لحرية التعبير الامنه**

تنشر منظمة EFF دليلا شاملا باللغة العربية حول كيفية ممارسة التعبير الرقمي بأمان

استراتيجيات التعبير الأمن

- ✓ استخدمي حسابات منفصلة: شخصي وعمل وناشط
- ✓ تعلمي استخدام ميزات "الاعدادات المخصصة" لكل منشور
- ✓ فكري مرتين في النشر المباشر للمعلومات الحساسة
- ✓ تواصلي مع مجموعات دعم موثوقة من نفس مجتمعك
- ✓ شاركي في تدريبات السلامة الرقمية الجماعية
- ✓ وثقي الانماط المتكررة وأبلغي المنتظمات الحقوقية
- ✓ تبادلي خبرات الحماية مع النساء الاخري

الأمان الجماعي أقوي من الفردي

بناء شبكات دعم مجتمعية تشترك في رصد التهديدات وتبادل المعلومات وتوثيق الأنماط يعزز الحماية بصورة جماعية.

الذكاء الاصطناعي والجريمة المنظَّمة

التحوّل الخطير

الذكاء الاصطناعي لم يخلق نوعًا جديدًا من الجرائم — بل جعل تنفيذها في متناول الجميع. رسالة تصيد كانت تستغرق 16 ساعة لكتابتها أصبحت تُنجَز في 5 دقائق.

أكثر من 90%
من إجمالي عمليات الاختراق الرقمي مدعومة بالذكاء الاصطناعي

88%
من هجمات التصيد تستهدف سرقة بيانات تسجيل الدخول - تحليل كاسبرسكي

أدى الاعتماد على الذكاء الاصطناعي إلى زيادة سرعة الهجمات الإلكترونية بمقدار 100 مرة

كيف يُعزِّز الذكاء الاصطناعي الهجمات؟

- يكتب رسائل تصيد مقنعة بلغة عربية سليمة خالية من الأخطاء
- يُنشئ فيديوهات وصوراً مزيّفة (التزييف العميق) لحملات الابتزاز
- يطوّر برمجيات خبيثة قادرة على تغيير سلوكها أثناء تنفيذ الهجوم
- ينتشر عبر تطبيقات مراسلة كواتساب لاستهداف المؤسسات

📖 حصان طروادة المصرفي — Trojan/Triada

فيروسات مدمجة في تطبيقات مزيفة أو أجهزة مباعة في السوق السوداء. تستهدف البيانات المصرفية وتعمل خِفية على الأندرويد. ارتفعت هجماتها على البنوك المصرية 186%، محتلةً المرتبة الثالثة في المنطقة. (Kaspersky 2026)

📖 برمجية Nexus — Android Banking Trojan

برمجية خبيثة من نوع حصان طروادة المصرفي تستهدف تطبيقات الهواتف الذكية التي تعمل بنظام الأندرويد لسرقة بيانات الدخول والمعلومات المالية. تنبيه: لا تخلطي بينها وبين عمليات حرب المعلومات الروسية-الأوكرانية — فهي أداة مختلفة تماماً.

الحماية من الجريمة الرقمية المُدعَّمة بالذكاء الاصطناعي

مؤشرات التهديد الناشئة 2026

- **التصيد بالذكاء الاصطناعي:** رسائل مخصَّصة تستخدم معلوماتك الشخصية الفعلية
- **تزييف المكالمات الصوتية:** انتحال صوت شخص تعرفينه لطلب المساعدة أو المال
- **هجمات NFC:** استهداف المحافظ الإلكترونية عبر تقنية الاتصال القريب
- **السوق السوداء:** هواتف أندرويد مباعة تحمل فيروسات مثبَّتة مسبقاً

⚠ هواتف الأندرويد المباعة مسبقاً

رُصد بيع هواتف أندرويد في السوق السوداء تحمل فيروسات مثبَّتة مسبقاً. اشتري دائماً من متاجر موثوقة وتحققي من خلوّ الجهاز من التطبيقات المشبوهة عند الشراء.

خطوات الحماية العملية

1. **استخدمي برنامج مكافحة فيروسات على هاتفك** — Bitdefender أو Kaspersky (نسخة مجانية)
2. **لا تثبتي تطبيقات خارج** Google Play أو App Store
3. **تحققي من الروابط** قبل النقر عبر virustotal.com
4. **لا تدفعي أموالاً بناءً على مكالمة صوتية** — حتى لو كانت لشخص تعرفينه
5. **لا تصدِّقي أي عرض وظيفي يبدو مثالياً جداً** — احتيال وظيفي شائع

للإبلاغ في مصر

- **مباحث الإنترنت** — للبلاغات الرسمية
  *يجب تقديم البلاغ في أسرع وقت، ويفضل ألا يتجاوز ثلاثة أشهر من تاريخ الواقع
- **Speak Up** — دعم شامل للعنف الرقمي
- **SMEX** — دعم السلامة الرقمية للناشطات والمدافعات
- **Access Now Helpline** — دعم السلامة الرقمية للناشطات والمدافعات

القسم الخامس

الحماية والاستجابة

المعرفة وحدها لا تكفي — نحتاج إلى خطط عمل واضحة وأدوات فعلية.

خطة السلامة الرقمية الشخصية

ما هي خطة السلامة الرقمية؟

هي وثيقة حية تُحدِّدين فيها: ما الذي تريدين حمايته؟ من قد يستهدفك؟ ما الإجراءات التي ستتخذينها؟ وما مصادر الدعم المتاحة لك؟

لا توجد خطة سلامة نموذجية واحدة تناسب الجميع. تُبنى الخطة من نموذج تهديدك الشخصي الذي طّورناه في القسم الأول.

خطوات بناء خطتك الشخصية

1. **حدِّدي أصولك الرقمية:** ما الحسابات والملفات والأجهزة التي تحتاجين لحمايتها؟
2. **قيِّمي مستوى خطرك** بصدق بناءً على نموذج التهديد (القسم الأول).
3. **طبِّقي الحماية الأساسية:** كلمات مرور قوية وتحقق ثنائي.
4. **وثِّقي ما يجب فعله عند الطوارئ:** من تتصلين به؟ كيف تبلِّغين؟
5. **راجعي الخطة** كل 3 أشهر وحدِّثيها.
6. **خذي نسخة احتياطية** بانتظام.
7. **احتفظي بنسخة من مستنداتك المهمة** على جهاز تخزين خارجي آمن أو خدمة سحابية مشفرة. ستحتاجين إليها إذا فقدِت الوصول إلى أجهزتك.

إجراءات الطوارئ الرقمية

- **من تتصلين به أولاً؟** (شبكة الدعم الشخصية)
- **كيف تُوثِّقين الأدلة بسرعة؟** (لقطات شاشة وروابط وتاريخ ووقت)
- **كيف تُبلِّغين عن الحادثة؟** (من خلال المنصة والجهات المختصة)
- **أرقام الطوارئ:** المجلس القومي للمرأة 15115
  speakupeg.com | accessnow.org/help

🛡️ بناء شبكة دعم

حددي شخصاً أو أكثر تثقين بهم تتصلين بهم عند الأزمات. لستِ مضطرة لمواجهة أي شيء وحدك.

أدوات الحماية والتشفير

التشفير يعني تحويل بياناتك إلى صيغة لا يمكن قراءتها إلا من يملك المفتاح الصحيح. كثير من الأدوات المجانية توفر تشفيراً قوياً.

أدوات موصى بها — مجانية

الأداة	الاستخدام
Signal	مراسلة مشفَّرة كاملة
ProtonVPN	VPN مجاني بلا حدود — سويسري
ProtonMail	بريد إلكتروني مشفَّر
Bitwarden	إدارة كلمات المرور
Malwarebytes	مكافحة برامج التجسس والفيروسات
Brave Browser	متصفح يحجب التتبع تلقائياً

تشفير الملفات

- **VeraCrypt:** لتشفير الملفات والمجلدات الحساسة على الكمبيوتر
- **Cryptomator:** لتشفير الملفات على التخزين السحابي
- **Signal Note to Self:** لتخزين الملاحظات الحساسة على الهاتف

الاستجابة للحوادث الأمنية

ما معنى الحادثة الأمنية؟

هي أي حدث يُعرِّض حساباتك أو بياناتك أو سلامتك الرقمية للخطر — من اختراق حساب إلى تهديد أو نشر محتوى مسيء.

خطوات الاستجابة الفورية

1. **وثِّقي أولاً:** لقطات شاشة مع التاريخ والوقت — قبل أي إجراء آخر
2. **إذا اختُرق حسابك:** غيِّري كلمة المرور فوراً من جهاز آخر آمن
3. **أنهي جميع الجلسات النشطة** على الحساب المخترق
4. **أبلغي المنصة عن الحادثة**
5. **أبلغي الجهات المختصة:** مباحث الإنترنت / SMEX / Access Now / Speak Up
6. **أبلغي الأشخاص المتضررين** إذا كانت الحادثة تخصهم

الاستجابة حسب نوع الحادثة

الحادثة	الاستجابة الفورية
اختراق حساب	غيِّري المرور + أنهي الجلسات + 2FA
تهديد أو ابتزاز	لا تدفعي + وثِّقي + أبلغي
برنامج تجسس	لا تناقشي على الجهاز + Malwarebytes
صور بلا موافقة	StopNCII.org + أبلغي المنصة + محامية

الرعاية النفسية الرقمية

التعرض للعنف الرقمي والتهديدات الرقمية يُلحق أذىً نفسياً حقيقياً. الاعتناء بنفسك ليس كمالياً — هو ضروري لاستمرار عملك وحياتك.

ردود الفعل الطبيعية بعد العنف الرقمي

- **الصدمة والإنكار:** مشاعر طبيعية جداً في البداية
- **القلق والخوف** من استخدام الإنترنت
- **الإحساس بالعزلة** والوصم الداخلي
- **انخفاض احترام الذات** والإنتاجية

⚠ تذكري

لستِ مذنبة. العار ليس عليك — المسؤولية تقع كاملاً على من ارتكب ذلك.

استراتيجيات الرعاية الذاتية

- ضعي حدوداً زمنية لاستخدام التواصل الاجتماعي
- أوقفي الإشعارات خلال أوقات الراحة والنوم
- تواصلي مع أصدقاء حقيقيين وشبكة دعم موثوقة
- وثّقي الحوادث ثم ابتعدي عنها نفسياً
- اطلبي دعماً نفسياً متخصصاً عند الحاجة

موارد الدعم النفسي في مصر

- **المجلس القومي للمرأة:** 16021
- Access Now Helpline: accessnow.org/help — للناشطات

الإرهاق الرقمي للناشطات
Activist Burnout

📖 ما هو الإرهاق الرقمي للناشطات؟

حالة من الاستنزاف العاطفي والجسدي الناتجة عن التعرض المستمر لمحتوي مؤلم أو تهديدات متكررة. يصيب الناشطات والصحفيات والمدافعات عن حقوق الأنسان بصورة خاصة

1. اعترفي بالإرهاق - عدم الشعور بالذنب
2. خذي إجازة رقمية حقيقية (يوم أو أكثر)
3. شاركي الأعباء مع فريقك أو شبكتك
4. مارسي نشاط رياضي بشكل منتظم
5. تواصلي مع معالج نفسي متخصص في الصدمات

⚠ لا تعملي في عزلة

أذا كنت تعانين من أفكار إيذاء الذات أو الاكتئاب الشديد بعد تجربة رقمية مؤلمة تواصلي فورا مع خط دعم الصحة النفسية أو طوارئ المستشفي. **صحتك أهم من أي شئ.**

الاعتناء بنفسك في العمل الرقمي

بناء مجتمع دعم متماسك هو أحد أقوى أدوات الحماية الرقمية

⚠ لستِ وحدك

العمل في الفضاء الرقمي — خاصةً في المجال الحقوقي — يُعرِّضك لضغوط متراكمة. طلب المساعدة شجاعة، لا ضعف فيها.

للمنظمات — الرعاية المؤسسية

- اعتمدي سياسة أمان رقمي واضحة للفريق
- خصصي وقتاً دورياً لمراجعة الأمان الجماعي
- أنشئي بروتوكولاً للاستجابة للحوادث يعرفه كل الفريق
- ادعمي زميلاتك اللواتي تعرضن لحوادث رقمية بدون وصمة

المسرد — مصطلحات السلامة الرقمية

التحقق الثنائي (2FA)

طبقة حماية ثانية تُضاف لكلمة المرور عبر كود يُرسَل للهاتف أو يُنتَج بتطبيق مصادقة.

التزييف العميق (Deepfake)

محتوى مرئي أو صوتي مُزيَّف بالذكاء الاصطناعي يُمثِّل شخصاً حقيقياً في موقف لم يحدث.

التصيد الاحتيالي (Phishing)

أسلوب خداع إلكتروني لسرقة البيانات عبر رسائل أو مواقع مُزيَّفة. يُمثِّل 15% من حوادث الأمن السيبراني.

برامج التجسس المخفية (Stalkerware)

تطبيقات تُثبَّت سراً على الهاتف لمراقبة الرسائل والموقع والكاميرا دون علم الضحية. تُستخدَم كثيراً في العنف الأسري.

التشفير (Encryption)

تحويل البيانات إلى صيغة مُشفَّرة لا يمكن قراءتها إلا من يملك المفتاح الصحيح.

VPN (شبكة افتراضية خاصة)

تقنية تُخفي هويتك الرقمية وتُشفِّر اتصالاتك عبر الإنترنت.

المسرد — مصطلحات السلامة الرقمية

الهندسة الاجتماعية (Social Engineering)

التلاعب النفسي بشخص لدفعه لإفصاح معلومات حساسة أو اتخاذ إجراء ضار.

التصيد بـ QR — Quishing

أسلوب تصيد يعتمد على رموز QR مزيّفة توجّه الضحية لمواقع تسرق بياناتها أو بيانات دفعها.

الصور الحميمة بلا موافقة — NCII

نشر أو تداول صور حميمة دون موافقة صاحبها. شكل من العنف الرقمي الجنساني.

OAuth — بروتوكول التفويض

بروتوكول مشروع يُتيح لتطبيق الوصول لحساب المستخدم دون معرفة كلمة المرور. يُساء استخدامه عبر تطبيقات خبيثة.

الشبكات التوليدية التنافسية — GANs

نموذج ذكاء اصطناعي: مولّد للمحتوى المزيف ومميّز للكشف عنه. الأساس التقني للتزييف العميق. (إيان غودفيلو، 2014)

DPI — فحص الحزم العميق

تقنية تستخدمها شركات الاتصالات للفحص المفصَّل لحركة البيانات. وثَّقت AFTE استخدامه في مصر لأغراض مراقبة 2018.

المسرد — مصطلحات السلامة الرقمية

التصيد الصوتي — Vishing

تصيد عبر المكالمات الهاتفية لانتحال صفة بنك أو جهة رسمية.
ارتفع 260% بين 2022 و2023.

NFC — الاتصال القريب

تقنية اتصال لاسلكي قصير المدى تُستخدَم في المدفوعات الإلكترونية.
تستهدفها هجمات جديدة لاختراق المحافظ الرقمية.

حصان طروادة / تريادا (Trojan/Triada)

فيروس يتخفى في شكل تطبيق مشروع لاختراق البيانات المصرفية. نشط على الأندرويد. ارتفعت هجماته على البنوك المصرية 186%. (Kaspersky 2026)

Nexus — Android Banking Trojan

برمجية خبيثة من نوع حصان طروادة المصرفي تستهدف هواتف الأندرويد لسرقة بيانات الدخول والمعلومات المالية.

الذباب الإلكتروني / اللجان الإلكترونية

حسابات وهمية منسَّقة تشنّ هجمات جماعية ضد شخص أو جهة بهدف إسكاتها أو تشويه سمعتها.

الأصول الرقمية

الرسائل والبريد الإلكتروني وسجلات المكالمات والصور والهواتف والأجهزة المتصلة بالإنترنت.

الموارد والمراجع في مصر

منظمات الدعم في مصر

الجهة	نوع الدعم والتواصل
المجلس القومي للمرأة	16021 — دعم شامل للمرأة
مبادرة Speak Up المصرية	speakupeg.com — العنف الرقمي
مؤسسة حرية الفكر والتعبير (AFTE)	الحقوق الرقمية في مصر
Access Now Helpline	accessnow.org/help — للناشطات دولياً
منصة SMEX للسالمة الرقمية	org.smex —استشارات وأدوات حماية رقمية
مباحث الأنترنت	108 — مخصص لجرائم الانترنت والابتزاز

أدوات رقمية مجانية

- **virustotal.com** — فحص الروابط والملفات المشبوهة
- **StopNCII.org** — منع انتشار الصور الحميمة غير الموافَق عليها
- **fatabyyano.com / misbar.com** — التحقق من المعلومات العربية
- **Signal / ProtonVPN / ProtonMail / Bitwarden** — أدوات الحماية المجانية
- **Cyber Civil Rights Initiative** دعم ضحايا العنف الرقمي

نموذج توثيق الحادثة الأمنية

لماذا التوثيق مهم؟

التوثيق المنهجي يُقوِّي موقفك القانوني ويساعد المنظمات الداعمة على فهم ما حدث والتصرف بفعالية.

- تاريخ الحادثة ووقتها:
- نوع الحادثة (تحرش / ابتزاز / اختراق / أخرى):
- المنصة أو القناة التي حدثت عليها الحادثة:
- وصف مختصر لما حدث:
- هل حفظتِ الأدلة؟ (لقطات شاشة / روابط):
- هل أبلغتِ المنصة؟ ورقم البلاغ إن وجد:
- هل أبلغتِ الجهات الرسمية؟ ورقم البلاغ:
- الشهود أو الأشخاص الذين علموا بالحادثة:
- الإجراءات التي اتخذتِها حتى الآن:
- الدعم الذي تحتاجينه:

أسئلة متكررة حول السلامة الرقمية

- **هل واتساب آمن لمشاركة المعلومات الحساسة؟**

واتساب يوفر تشفيراً من الطرفين للمحادثات، لكنه يجمع بيانات وصفية (من اتصلت بهن، متى، وكم مدة المكالمة). للمعلومات الحساسة جداً، استخدمي Signal — تشفير أقوى وجمع بيانات أقل.

- **هل VPN يحميني تماماً؟**

VPN يُخفي نشاطك عن مزود خدمة الإنترنت ويحميك على الشبكات العامة، لكنه لا يجعلك مجهولة الهوية تماماً. يظل مزوّد VPN يرى نشاطك — لذا اختاري مزوّداً موثوقاً مثل ProtonVPN.

- **ما الفرق بين الاختراق والتصيد؟**

الاختراق يعني دخول غير مصرح به للنظام أو الحساب عبر استغلال ثغرة تقنية. التصيد هو خداعك أنتِ لتقدِّمي البيانات طوعاً. معظم الاختراقات الناجحة تبدأ بتصيد ناجح.

- **كيف أعرف إذا كان هاتفي مخترقاً؟**

العلامات: البطارية تفرغ بسرعة، الهاتف يسخن باستمرار، ارتفاع بيانات الإنترنت، تطبيقات مجهولة. افحصي هاتفك بـ Malwarebytes for Android مجاناً.

- **هل يمكنني استعادة حساب مسروق؟**

نعم في أغلب الأحيان. تواصلي مع دعم المنصة عبر بريد إلكتروني احتياطي أو رقم هاتف مسجَّل. إذا فقدتِ الوصول لكليهما، يصعب الاسترداد — لذا احرصي على تسجيل بيانات استرداد مسبقاً.

دليل الإجراءات الفورية — بطاقة مرجعية

إذا تعرضتِ لحادثة رقمية — هذه هي خطواتك:

نوع الحادثة	
⚠ تهديد أو ابتزاز 1. لا تستجيبي ولا تدفعي 2. وثّقي كل الأدلة فوراً 3. بلغي الشرطة أو Speak Up	⚡ اختراق حساب 1. غيّري كلمة المرور فوراً من جهاز آخر 2. أنهي جميع الجلسات النشطة 3. فعّلي التحقق الثنائي 4. بلغي المنصة
📸 صور بلا موافقة 1. لا تشاركي المحتوى 2. سجّلي في StopNCII.org 3. أبلغي المنصة فوراً 4. استشيري محامية	🔒 برنامج تجسس 1. لا تناقشي الأمر على الجهاز المشتبه به 2. استخدمي جهازاً آخر للتواصل 3. افحصي بـ Malwarebytes 4. Access Now: accessnow.org/help

الطوارئ في مصر

المجلس القومي للمرأة: 16021

منصة SMEX للسلامة الرقمية: smex.org

Speak Up: speakupeg.com

Access Now: accessnow.org/help

ينصح بقراءتها من متون

كبسولة تأمين الدخول (كلمات المرور والتحقق المتعدد)

كبسولة التخزين الآمن للملفات

هل التطبيقات عدوة للنساء؟

دليلك لحماية صورك الحميمية من النشر دون رغبتك

كيف تصبح فريسة للتصيد الاحتيالي

دليل السلامة الرقمية
للنســاء

التغيير الحقيقي يبدأ بالمعرفة. بقراءتك لهذا الدليل، خطوِت خطوتك الأولى نحو فضاء رقمي أكثر أمانا.

في نهاية هذا الدليل، نود التذكير بأن الهدف ليس إثارة الخوف — بل بناء قدرة حقيقية على الفهم والتصرف والحماية.

السلامة الرقمية ليست رفاهية ولا حكرًا على المتخصصين التقنيين. هي حق لكل امرأة، وخاصَّة لمن تواجه تهديدات مضاعفة بسبب هويتها الدينية أو نشاطها الحقوقي.

نأمل أن يكون هذا الدليل بداية رحلة — رحلة تعلم مستمر، وبناء علاقات دعم متينة، وممارسة سالمة رقمية يومية تصبح عادَة لا جهدًا.

يُعبِّر فريق منظمة متون عن عميق امتنانه لجميع النساء اللواتي شاركن تجاربهن، والمنظمات الشريكة التي دعمت هذا العمل.

كيفية الاستفادة من هذا الدليل

يمكن قراءته من البداية للنهاية للحصول على صورة شاملة، أو الانتقال مباشرةً إلى القسم المتعلق بالتهديد الذي تواجهينه.