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.