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.