



دليل عملي

دليل السلامة والأمان الرقمي

للنساء، البنات ومجتمع الميم اللي يتعرّضو للعنف الرقمي المبني على النوع الاجتماعي في تونس – ولكل شخص يحب يعاونهم.

سجّل الأدلة وخطة السلامة

شنّة تعمل كان صار

أمن حساباتك وتليفونك

وين تلقى المساعدة

في خطر توا؟

1899 الخط الأخضر المجاني للنساء ضحايا العنف · **197** الشرطة · **193** الحرس الوطني · **190** الإسعاف (SAMU)

المحتوى

3	كيفاش تستعمل الدليل هذا	1
4	نفهمو العنف الرقمي المبني على النوع الاجتماعي	2
6	أمن حساباتك	3
8	تليفونك وأجهزتك	4
10	إعدادات الخصوصية، منصة بمنصة	5
12	كان صار: أوراق التدخّل	6
15	التوثيق والحفاظ على الأدلة	7
17	خطة السلامة الشخصية متاعي	8
18	أساسيات قانونية في تونس	9
19	تهلّ في روك	10
20	وين تلقى المساعدة	11
22	قوائم تحقّق في صفحة وحدة	12

كيفاش تستعمل الدليل هذا

الدليل هذا ليك كان فما شكون يستعمل الإنترنت، التليفون ولا التطبيقات باش يأذك، يخوفك، يتحكم فيك ولا يسكتك – ولا كان تحب برك تحمي روحك خير. وهو زادة للأصحاب، للعائلة وللمختصين/ات اللي يحبوا يعاونو.

بالشوية عليك

بعض الأجزاء تنجم تكون صعبة في القراءة. خذ راحة. تنجم تطلب من شخص تثق فيه يقرأ معاك.

القرار ليك

موش لازم تبليغ على حتى شي، لحتى حد. استعمال الدليل ما يلزمكش بحتى خطوة. كل قرار يبقى ليك.

إقرأ كان اللي تحتاجو

كل فصل يتقرا وحدو. كان فما حاجة قاعدة تصير توا، أمشي طول للفصل 6، "كان صار".

شنوة باش تلقى

- **تفهم** شنوة هو العنف الرقمي المبني على النوع الاجتماعي (الفصل 2).
- **تحمي** حساباتك، تليفونك وخصوصيتك (الفصول 3 حتى 5).
- **تتصرف** كان صارت حاجة، بأوراق تدخل قصيرة (الفصل 6).
- **توثق** اللي يصير وتخطط لسلامتك، بأوراق عمل تعمّرها على الورق (الفصلين 7 و 8).
- **تعرف** حقوقك، تتهلّى في روحك وتلقى المساعدة (الفصول 9 حتى 11).
- **تثبت** في روحك بقوائم تحقق في صفحة وحدة (الفصل 12).

فما حد يراقب شاشتك ولا تليفونك؟

كان تحس إنو فما شكون يفتش تليفونك ولا الأوردي متاعك، إقرأ الدليل هذا من جهاز ما يوصلوش (تليفون صاحب/ة تثق فيه/ا، أوردي الخدمة ولا المكتبة)، ولا خبي النسخة المطبوعة في بلاصة آمنة. في موقع E-RADAR، الزر "**خروج سريع**" اللي فوق في كل صفحة – ولا كي تنزل **Esc مرتين** – يهزك طول J Google. بعدها، تنجم زادة تفسخ الموقع من تاريخ المتصفح، ولا تستعمل نافذة خاصة (incognito).

كان إنت في خطر توا

كلم 197 (الشرطة)، 193 (الحرس الوطني) ولا 190 (الإسعاف SAMU، حالة طبية مستعجلة). الخط الأخضر المجاني للنساء ضحايا العنف هو 1899.

كلمة على الكلمات: نحكيو معاك بـ"إنت" في الدليل الكل. الدليل هذا لكل النساء والبنات، ولكل مجتمع الميم، مهما كانت الهوية. أسامي القوائم في التطبيقات تتبدل برشا: كان إعداد عندو اسم مختلف شوية في تليفونك، استعمال خانة البحث اللي في إعدادات التطبيق.

نفهمو العنف الرقمي المبني على النوع الاجتماعي

العنف الرقمي المبني على النوع الاجتماعي هو كل تصرف يصير عبر الإنترنت، التليفون ولا التطبيقات، ويقصد بأذى، يخوف، يسكت ولا يتحكم في شخص على خاطرها مرا ولا بنت، ولا على خاطر هويتو الجندرية ولا ميولو الجنسية.

هو عنف حقيقي. وأثرو على صحتك النفسية، سلامتك، قرايتك، خدمتك وعلاقاتك حقيقي. برشا مرات يجي من حد قريب: شريك ولا شريك سابق، فرد من العائلة، زميل/ة في الخدمة، صاحب/ة في القرابة. وينجم زادة يجي من ناس ما تعرفهمش، ساعات منظمين في مجموعات.

علاش "مبني على النوع الاجتماعي"؟

النساء ومجتمع الميم يتعرّضو ليه بأشكال خاصة: تعليقات على الجسم، تهديد بنشر تصاور حميمية، كشف الهوية (outing) قدام العائلة، حملات تشويه سمعة. والضغط الاجتماعي والعائلي ينجم يخلي العواقب أثقل برشا — ويصعب الحكي عليها.

أشكال معروفة

الشكل	كيفاش بيان
التحرّش	ميساجات وتعليقات مسيئة، جنسية ولا موش مرغوب فيها، متكررة، وبرشا مرات من أكثر من حساب.
التهديد	ميساجات فيها تهديد بالعنف، بالفضيحة، ولا بأذى ليك ولا للناس القريبين منك.
الابتزاز	"أعمل هكّا، ولا راني ننشر / نقول..." — يطلب فلوس، تصاور، لقاء، ولا إنك تسكت.
الابتزاز الجنسي (sexortion)	ابتزاز بتصاور ولا فيديوهات حميمية، حقيقية ولا مزيفة.
نشر تصاور حميمية من غير موافقة	نشر، ولا التهديد بنشر، تصاور حميمية من غير موافقة — حتى التصاور اللي تصوّرت بالسرقة والـ deepfakes (تصاور مزيفة معمولة بالذكاء الاصطناعي بوجهك).
التشهير	نشر كذب ولا إشاعات باش يخسر سمعتك.
الملاحقة الإلكترونية	مراقبتك، تبيّلك ولا تتبّعك على الإنترنت ولا عبر تليفونك: ميساجات ما توفاش، تتبّع البلاصة، تطبيقات تجسس.
خطاب الكراهية	هجمات عليك على خاطرك مرا ولا من مجتمع الميم، وساعات فيها تحريض على العنف.
كشف الهوية (outing)	كشف — ولا التهديد بكشف — الميول الجنسية ولا الهوية الجندرية متاع شخص من غير موافقتو.
انتحال الشخصية	حسابات مزيفة باسمك ولا بتصاورك، ولا حد يسيطر على حسابك ويحكي في بلاصتك.
نشر المعلومات الشخصية (doxxing)	نشر معلوماتك الشخصية: العنوان، رقم التليفون، بلاصة الخدمة، تفاصيل على العائلة.

علامات تنبيه

ساعات العنف الرقمي يبدأ بحاجات صغيرة. العلامات هاذي تنجم تعاونك تسمي اللي قاعد يصير:

- تحس بالخوف ولا القلق كل ما يجيك ميساج من شخص معيّن.
 - حد يطلب منك كلمات السر متاعك، يفتش تليفونك، ولا يحب يعرف وين إنت ديما.
 - حد يعرف حاجات عمرك ما قلتها لو: وين كنت، شكون قابلت، شنو كتبت.
 - حد يهدّد ينشر تصاور، محادثات ولا معلومات عليك.
 - حد يطلب منك فلوس ولا تصاور مقابل إنو ما ينشرش حاجة.
 - تلقى حساب باسمك ولا بتصاورك ما عملتوش إنت.
 - تجيك تعليقات مسيئة على جسمك، هويتك ولا ميولك.
- كان واحدة من هاذم تشبه للي صايرلك، راهو من حقه تطلب الدعم. ما يلزمش تستنى لين يولي الوضع أخطر.

موش ذنبك. موش على خاطر وثقت في حد، موش على خاطر بعثت تصويرة، موش على خاطر
شنو تلبس، تقول ولا تنشر، موش على خاطر شكون إنت ولا شكون تحب. المسؤولية كاملة على
الشخص اللي يأذيك.

أمن حساباتك

أغلب سرقات الحسابات تصير بكلمة سر ضعيفة ولا معاودة، بكود مسروق، ولا بشخص قريب يعرف تليفونك. شوية تبديلات تعمل فرق كبير.

! كان حد قريب منك ممكن يراقب حساباتك

أعمل التبديلات من جهاز آمن ما يوصلوش. كي تسكّر عليه الباب فجأة، ينجم يفيق — كان هذا ينجم يحطّك في خطر، فكّر قبل في خطة السلامة متاعك (الفصل 8) ولا أطلب دعم.

1. أبدا بالإيميل متاعك

الإيميل هو المفتاح متاع الحسابات الكل: اللي يتحكّم فيه ينجم يبذل كلمات السر متاع الحسابات الأخرى الكل. أمّنو هو الأول، بعدها الحسابات المرتبطة برقم تليفونك، بعدها مواقع التواصل.

2. كلمات سر قوية ومختلفة

- استعمل **جملة سر**: أربعة كلمات ولا أكثر بالصدفة، ساهلة عليك تتفكّرها وصعبة على غيرك يلقاها. مثلاً: **olive-bus-cloud-river-27** (ما تستعملش هاذي!).
- **عمرك ما تعاود** نفس كلمة السر في زوز حسابات. كي موقع يتسرّب، المهاجمين يجربو كلمة السر هاذيكا في كل بلاصة.
- بحدّ على تواريخ الولادة، الأسامي، الحيوانات، أرقام التليفون — الناس القريبين منك ينجمو يلقاهاهم.
- **مدير كلمات السر** (ولا اللي موجود في تليفونك ولا المتصفح، Bitwarden تطبيق يحفظ كلمات السر الكل في خزنة مشفرة، كيما — r يسهّلك برشا. تتفكّر كان جملة سر وحدة قوية.
- ما تعطيش كلمات السر متاعك للشريك، حتى "كدليل على الثقة". كي يطلبهم، هذا ينجم يكون شكل من أشكال التحكّم.

3. فَعْل المصادقة الثنائية (2FA)

بال 2FA، الدخول من جهاز جديد يطلب كود ثاني زيادة على كلمة السر. حتى كان حد يعرف كلمة السر متاعك، ما ينجمش يدخل.

- **الأحسن**: تطبيق مصادقة (Google Authenticator، Microsoft Authenticator، Aegis...) ولا passkey.
- **مقبول**: كودات بال SMS — خير من والو، أما أضعف، خاصة كان حد ينجم يوصل لشريحة تليفونك (SIM) ولا لتليفونك.

المنصة

وين تلقاها

الإعدادات ← **مركز الحسابات (Accounts Center)** ← كلمة السر والأمان ← **المصادقة الثنائية (Two-factor authentication)** ← اختار الحساب ← تطبيق المصادقة (ينصح بيه).

فايسبوك وإنستغرام

المنصة	وين تلقاها
واتساب	الإعدادات ← الحساب ← التحقق بخطوتين (Two-step verification) ← تفعيل ← اختار PIN من 6 أرقام ما يعرفو حد ← زيد إيميل باش تنجم ترجعو.
جيميل / Google	حساب Google (myaccount.google.com) ← الأمان ← التحقق بخطوتين (2-Step Verification) ← تتبع الخطوات؛ زيد تطبيق مصادقة وكودات احتياطية.
تيك توك	البروفيل ← القائمة ≡ ← الإعدادات والخصوصية ← الأمان ← التحقق بخطوتين (2-step verification) .

4. خبي كودات الاسترجاع في بلاصة آمنة

كي تفعل الـ 2FA، المنصة تعطيك كودات استرجاع (احتياطية). هاذم يخليوك ترجع لحسابك كان ضاع تليفونك. أكتبهم ولا إطبعمهم وخبيهم في بلاصة آمنة ما يوصلهاش الشخص اللي يأذك. عمرك ما تبعث كود لحتى حد — حتى لواحد يقول إنو من "الدعم".

5. شوف شكون داخل لحساباتك

شوف كل مرة الجلسات والأجهزة النشطة، وأخرج من أي حاجة ما تعرفهاش:

- **فايسبوك / إنستغرام:** مركز الحسابات ← كلمة السر والأمان ← **وين إنت داخل (Where you're logged in)**.
- **واتساب:** الإعدادات ← **الأجهزة المرتبطة (Linked devices)**. أوردي مرتبط ينجم يقرأ الميساجات متاعك الكل.
- **Google:** حساب Google ← الأمان ← **أجهزتك (Your devices)**. **فحص الأمان (Security Checkup)** يمشي بيك خطوة بخطوة.
- **تيك توك:** الإعدادات والخصوصية ← الأمان ← **إدارة الأجهزة (Manage devices)**.

تبت زادة في إيميل ورقم تليفون الاسترجاع في كل حساب، وفي التطبيقات الأخرى المرتبطة بيه. فسخ أي حاجة موش متاعك.

6. ردّ بالك من الروابط و"الدعم" المزيف

عمرك ما تدخل كلمة السر في صفحة جاتك من رابط في ميساج، حتى كان تبان رسمية. حلّ التطبيق ولا أكتب العنوان بيدك. المنصات عمرها ما تطلب الكود ولا كلمة السر متاعك في ميساج.

نصيحة



أعمل حساب واحد في النهار: الإيميل الأول، بعدها واتساب، بعدها فايسبوك/إنستغرام، بعدها البقية. الخطوات الصغيرة زادة خطوات.

تليفونك وأجهزتك

تليفونك فيه الميساجات، التصاور، البلاصة والحسابات متاعك، اللي يهزّو في يدو، حتى كان دقائق، ينجم يعمل برشا. هاو كيفاش تحميه.

قفل الشاشة

- استعمل PIN من 6 أرقام على الأقل ولا كلمة سر. بقّد على الأشكال السهلة والتواريخ.
- ردّ بالك من البصمة ولا التعرّف على الوجه كان حد ينجم يغصبك ولا يستعملها وإنّ راقد/ة.
- ما تعطيش الكود متاعك لحد. كان حد يعرفو من قبل، بدّلو.
- خبّي محتوى الإشعارات في شاشة القفل، باش الميساجات والكودات ما يتقراوش من غير ما يتحلّ التليفون.

تطبيقات ما تعرفهاش

- شوف قائمة التطبيقات الكاملة (الإعدادات ← التطبيقات). بعض تطبيقات التجسس تتخبّي بأسماء عادية كيما "System service" ولا "Sync". ثبتّ زادة في:
- **Android:** الإعدادات ← الأمان ← **تطبيقات مشرف الجهاز (Device admin apps)**، والتطبيقات اللي عندها وصول لإمكانية الوصول (Accessibility)، الإشعارات ولا البلاصة. ثبتّ إنيو **Google Play Protect** مفعل.
 - **iPhone:** الإعدادات ← عام ← **VPN وإدارة الجهاز (VPN & Device Management)** (بروفيلات ما تعرفهاش). **فحص الأمان (Safety Check)** (الإعدادات ← الخصوصية والأمان) يوريك مع شكون تشارك الوصول ويخليك توقفو.

علامات تطبيق تجسس (stalkerware)

- حد يعرف ميساجاتك، محادثاتك ولا تحركاتك من غير ما تقلّو.
- البطارية تفرغ بسرعة موش عادية، ولا التليفون يسخن وإنّ ما تستعملوش.
- استهلاك الإنترنت (data) يطلع من غير سبب.
- إعدادات تبدّلت من غير ما تبدّلها إنت (البلاصة تشعلت، إعدادات الأمان تطفات).
- الشخص كان عندو تليفونك في يدو، ولا "رگبهولك".

ما تفسخش تطبيق التجسس طول

كان تشك في stalkerware، كي تفسخو الشخص ينجم يفيق والوضع ينجم يولّي أخطر. وزيد يفسخ الأدلة. أعمل قبل خطة سلامة (الفصل 8)، استعمل جهاز آخر باش تطلب المساعدة، وأطلب دعم تقني. كي يكون آمن، إعادة ضبط المصنع (factory reset) الكاملة — بعد ما تحفظ الأدلة متاعك — هي أضمن طريقة باش تنظّف التليفون.

مشاركة البلاصة

- ثبتّ كانك تشارك بلاصتك في **Google Maps** (مشاركة الموقع)، **Find My** في iPhone (مشاركة موقعي)، **Snapchat** (Ghost Mode استعمل — Snap Map)، وتطبيقات تتبّع العايلة.

- طَقّي البلاصة للتطبيقات اللي ما تحتاجهاش (الإعدادات ← الموقع / الخصوصية ← خدمات الموقع).
- ما تنشرش بلاصتك وقتها. أنشر بعد ما تخرج من البلاصة.

أجهزة التتبع

- أجهزة تتبع Bluetooth صغيرة (كيما AirTag) تنجم تتخبي في ساك، في مونطو ولا في كرهبة.
- **iPhone** يتبّك كي جهاز تتبع ما تعرفوش يتحرّك معاك ("AirTag Found Moving With You").
- **Android** فيه تنبيهات أجهزة التتبع المجهولة (**Unknown tracker alerts**) (الإعدادات ← السلامة والطوارئ) وفحص يدوي.
- كان لقيت واحد، فكّر في سلامتك قبل ما تنحّيه: الشخص ينجم يلاحظ. صوّرو، أكتب وين ووقتاش لقيتو، وأطلب دعم.

التصاور تكشف أكثر مما تتصوّر

التصاور تنجم يكون فيها معلومات مخبّية (metadata): البلاصة والوقت بالضبط وقتاش تصوّرت. طَقّي حفظ البلاصة في إعدادات الكاميرا. كي تبعت تصويرة من iPhone، أنزل على **الخيارات (Options)** وطَقّي **الموقع (Location)**؛ في Google Photos، استعمل **إزالة الموقع (Remove location)**. ثبت زادة في اللي وراك في التصويرة: لافتة شارع، طابلية مدرسة ولا اللي بيان من الشّبّاك ينجمو يكشفو وين إنت.

النسخ الاحتياطي والكلود

تصاورك وميساجاتك برشا مرات يتنسخو في **iCloud، Google Photos / Google Drive** ولا في نسخة احتياطية متاع واتساب. أي حد يعرف كلمة السر متاع الحساب هذاك ينجم يشوف كل شي، من أي جهاز. أمّن الحسابات هادي كيما في الفصل 3، وثبت شنوة الأجهزة الداخلة ليهم.

التحديثات

حدّث النظام والتطبيقات ديما. التحديثات تسكّر ثغرات أمنية يستعملوها المهاجمين.

تليفون مشترك ولا مستعمل؟



كان التليفون تعطالك، ولا حد آخر ركبّهولك، ينجم يكون مازال عندو وصول للحسابات اللي فيه. أدخل بحساب إيميل جديد متاعك إنت، وثبت في "الأجهزة المرتبطة" والأجهزة الداخلة في كل بلاصة.

إعدادات الخصوصية، منصة بمنصة

إعدادات الخصوصية هي التي تقرّر شكون ينجم يشوفك، يكلمك ويلقاك. عشرة دقائق لكل منصة تكفي.

أسامي القوائم تتبدّل من نسخة لنسخة ومن لغة للغة. كان ما لقيتش إعداد، أكتب اسمو في خانة البحث اللي في إعدادات التطبيق.

فايسبوك

- ☐ أعمل **فحص الخصوصية (Privacy Checkup)** (الإعدادات والخصوصية) – يمشي بيك خطوة بخطوة.
- ☐ خّلّي المنشورات الجاية للأصدقاء (Friends)، موش للعموم. استعمل **تحديد المنشورات القديمة (Limit past posts)** للقدام.
- ☐ خبّي قائمة أصحابك، رقم تليفونك، إيميلك وتاريخ ولادتك.
- ☐ فَعّل **مراجعة الإشارات (Tag review)** و**مراجعة البروفايل (Profile review)**، باش ما يظهر حتى شي في بروفايلك من غير موافقتك.
- ☐ حدّد شكون ينجم بيعثلك طلبات صداقة وشكون ينجم يلّقاك برقم تليفونك ولا إيميلك.
- ☐ استعمل **الحظر (Block)** للحسابات المسيئة، و**التقييد (Restrict)** كان ما تحبهمش يعرفو.

إنستغرام

- ☐ رجّع الحساب خاص (Private account).
- ☐ استعمل **التقييد (Restrict)** (ما يعرفوش) ولا **الحظر (Block)** للحسابات اللي تعمل مشاكل – حتى الحسابات الجديدة اللي ينجمو يحلّوها.
- ☐ اختار شكون ينجم بيعثلك ميساجات، يعلّق، يعمل tag ولا mention.
- ☐ فَعّل **الكلمات المخفية (Hidden Words)** باش تفلتر التعليقات وطلبات الميساجات المسيئة.
- ☐ استعمل **الحدود (Limits)** باش تخبّي مؤقتاً التعليقات والميساجات من الحسابات اللي ما يتبعوكش ولا تبعوك جديد – تنفع برشا وقت الهجوم.
- ☐ استعمل **الأصدقاء المقربين (Close Friends)** لا stories الشخصية، وخبّي حالة النشاط متاعك.

واتساب

- ☐ الإعدادات ← الخصوصية: اختار شكون يشوف آخر ظهور ومتصل (Last seen & online)، صورة البروفايل، النبذة (About) والحالة (Status).
- ☐ المجموعات: "جهات الاتصال متاعي" برك، باش الناس اللي ما تعرفهمش ما ينجموش يزيديوك.
- ☐ المكالمات ← إسكات المتصلين المجهولين (Silence unknown callers).
- ☐ ثبت في الأجهزة المرتبطة (Linked devices) كل مرة.
- ☐ فحص الخصوصية (Privacy checkup) (الإعدادات ← الخصوصية) يجمع هذا الكل في بلاصة وحدة.
- ☐ تفكر: الميساجات اللي تتفسخ وحدها و"العرض مرة وحدة" (view once) ما يمنعوش حد يصور الشاشة.

تيك توك

- ☐ رجّع الحساب خاص (Private account).
- ☐ طقي اقتراح حسابك للآخرين (Suggest your account to others) (حتى لجهات الاتصال وأصحاب فايسبوك).
- ☐ اختار شكون ينجم يعلّق، يعمل Duet، Stitch، يحمل الفيديوهات متاعك ويبعثلك ميساجات.
- ☐ استعمل فلاتر التعليقات وفلاتر الكلمات.
- ☐ خبي حالة النشاط متاعك وشكون تتبع.

أعمل "أبحث على روحك"



أبحث على اسمك، ال username متاعك ورقم تليفونك في محرّك بحث وفي كل منصة، وإنّ خارج من حسابك ولا من جهاز صاحب/ة. باش تشوف شنوة يشوفو الناس اللي ما يعرفوكش.

كان صار: أوراق التدخل

أوراق قصيرة وعملية للحالات الأكثر انتشاراً. اقرأ اللي تحتاجها. في كل الحالات: موش ذنبك، تنجم توثق قبل ما تبلوكي، وتنجم تطلب دعم في أي خطوة.

6.1 حسابي تهكّر

العلامات: ميساجات ما بعثتهمش، كلمة سر تبدّلت، ما عادش تنجم تدخل.

- 1 **حاول ترجعو** بالأدوات الرسمية: فايسبوك facebook.com/hacked · إنستغرام instagram.com/hacked · جيميل g.co/recover · واتساب: عاود سجّل رقمك على تليفونك، هكّا تخرّج الشخص الآخر، بعدها فَعّل التحقق بخطوتين.
- 2 **كي ترجع تدخل:** حظّ كلمة سر جديدة وقوية، بدّل كلمة سر الإيميل زادة، أخرج من كل الجلسات اللي ما تعرفهاش، فَعّل الـ 2FA، ثبّت في إيميل/تليفون الاسترجاع والتطبيقات المرتبطة.
- 3 **حدّر جهات الاتصال متاعك** باش ما يجاوبوش على ميساجات تطلب فلوس، تصاور ولا كودات.
- 4 **وثّق:** captures للميساجات اللي تبعثت باسمك وللتبديلات في الحساب.

كان الشخص اللي دخل قريب منك وعندو وصول لتليفونك، أعمل هذا الكل من جهاز آخر آمن.

6.2 فما شكون يهدّد في

- 1 **قيّم الخطر.** الشخص يعرف وين تسكن، تخدم ولا تقرا؟ التهديدات فيها أذى جسدي؟ قاعدة تزيد؟ كان "إي" على وحدة منهم، خوذ الأمر بجديّة: كلّّم 1899، ولا الشرطة 197 كان الخطر قريب.
- 2 **ما تجاوبش وما تستفزّش.** الجواب ينجم يزيد يشعل الوضع.
- 3 **وثّق كل شي** (الفصل 7) — خَلّي الميساجات الأصلية حتى بعد ما تبلوكي.
- 4 **بلوكي وبلّغ** للمنصة بعد ما تحفظ الأدلة.
- 5 **حظّ لسلامتك:** قول لشخص تثق فيه، بدّل الطريق والأوقات كان الشخص يعرفهم، طقّي مشاركة البلاصة.

6.3 فما شكون يبتزّ في ولا يبتزّني جنسياً

اللي صار موش غلطتك. المسؤولية كاملة على الشخص اللي يبتزّ فيك.

- 1 **ما تخلصش وما تبعثش تصاور أخرى.** الخلاص نادراً ما يوقّف الابتزاز؛ وبرشا مرات يجيب طلبات أكثر.
- 2 **ما تفسخش المحادثة.** أعمل captures فيهم اسم الحساب، الرابط متاعو والتاريخ.
- 3 **وقّف التواصل** بعد ما توثق. ما تتفاوضش. تنجم تسكّر حسابك مؤقتاً في بلاصة ما تفسخو.
- 4 **أمن حساباتك:** بدّل كلمات السر، فَعّل الـ 2FA، رجّع البروفيلات خاصة، خبّي قوائم الأصدقاء والمتابعين.

5 **بلّغ على الحساب للمنصة** – عندهم إجراءات خاصة بالتصاور الحميمية.

6 **إحمي تصاورك** بـ StopNCII.org ولا Take It Down (شوف 6.4).

7 **أحكي مع حد** تثق فيه، وأطلب دعم.

6.4 تصاوري الحميمية تنشرت (ولا ممكن تنتشر)

كان بعثت تصويرة بثقة، ولا تصوّرت من غير ما تعرف، ولا عملت تصويرة مزيفة بالذكاء الاصطناعي – في كل الحالات، موش ذنبك.

1 **وثّق وين تظهر** (الرابط، الحساب، التاريخ) من غير ما تعاود تنشرها.

2 **بلّغ للمنصة** بالخانة الخاصة بالتصاور الحميمية المنشورة من غير موافقة. المنصات تعطي البلاغات هاذي أولوية.

3 **StopNCII.org** (كان كان عمرك 18 عام ولا أكثر في التصويرة): يعمل "بصمة" رقمية (hash) لتصاورك على جهازك إنت – التصويرة بيدها عمرها ما تتبعث – باش المنصات الشريكة تنجم تبلوكيها.

4 **Take It Down** (takeitdown.ncmec.org): نفس الطريقة كان كنت تحت 18 عام في التصويرة.

5 **محركات البحث:** Google عندو استمارة رسمية باش تطلب نحّي التصاور الحميمية المنشورة من غير موافقة من نتائج البحث.

6 **أطلب دعم،** نفسي وقانوني. ماكش وحدك.

! **عمرك ما تبعث التصاور**

ما تبعث تصاور حميمية لحتى حد باش "تثبت" اللي صار – لا لينا، لا لحتى حد. وصف ورابط المنشور يكفيو.

6.5 كشف الهوية (outing)، ولا التهديد بيه

هويتك متاعك. إنت وحدك اللي تقرّر شكون يعرف، ووقتاش.

في تونس، كشف الهوية ينجم يجيب رفض العايلة، فقدان السكن ولا الخدمة، عنف جسدي، ولا مشاكل قانونية. نعتبرو الوضع هذا ممكن يكون خطير.

كان حد يهدّد يكشف هويتك

1 **ما تخلّصش وما تبعثش حتى شي.** هذا ابتزاز؛ والخلص ما يوقفوش.

2 **وثّق** التهديد وخبّي الأدلة في بلاصة آمنة – موش في تليفون مشترك.

3 **قلّص المعلومات اللي تنجم تتلقّى عليك:** نظّف حساباتك، خبّي قوائم الأصدقاء، فسخ التصاور اللي ممكن تُستعمل، وثبّت في الحسابات الأخرى (تطبيقات التعارف، بروفيلات قديمة، مجموعات الدردشة).

4 **أعمل خطة سلامة:** وين تنجم تمشي كان الوضع تعقّد في الدار؟ شكون تنجم تكلم؟ شنوّة تهزّ معاك؟ (الفصل

(8)

5 **أطلب دعم** من ناس وجمعيات تحترم مجتمع الميم. E-RADAR ينجم يعاونك تلقاهم.

كان هويتك تكشف

- سلامتك الجسدية قبل كل شي. كان إنت في خطر، كَلِّم 197 ولا 193، ولا أمشي لشخص ولا بلاصة آمن/ة.
- بلِّغ على المنشورات: كشف الميول ولا الهوية متاع شخص ممنوع في قواعد أغلب المنصات.
- الدعم النفسي مهم برشا في الفترة هاذي. ماكش وحدك.

قبل ما تفكر تتوجه للسلطات، أطلب دعم قانوني يعاونك تفهم المخاطر والخيارات متاعك.

6.6 حملة كراهية ضدي على الإنترنت

شتم ولا سخرية على جنسك، جسمك، هويتك ولا ميولك؛ تحريض على العنف؛ برشا حسابات يهجمو في نفس الوقت باش يسكتوك.

- 1 **ما تقرأش كل شي وحدك.** أطلب من حد تثق فيه يفرز ويوثق في بلاصتك.
- 2 **وثق** المنشورات والحسابات، خاصة اللي فيها تهديد، تحريض ولا معلوماتك الشخصية.
- 3 **استعمل أدوات المنصة:** فلاتر الكلمات، تحديد التعليقات، التقييد ولا الحظر، "الحدود" (Limits) في إنستغرام.
- 4 **بلِّغ:** المنصات تمنع خطاب الكراهية المبني على الجنس، الهوية والميول.
- 5 **خوذ استراحة:** رجّع حسابك خاص ولا سكرو مؤقتاً حتى يهدى الوضع.

كان الهجوم فيه تهديدات ولا العنوان متاعك، تبّع زادة الورقة 6.2.

الكراهية تقول على اللي يكتبها، موش عليك.

6.7 فما شكون يلاحق فيّ على الإنترنت

العلامات: ميساجات ولا مكالمات متكررة بعد ما قتلو يوقف؛ حسابات جديدة كل ما تبلوكيه؛ يعرف وين كنت ولا مع شكون؛ هدايا ولا ميساجات توصلك للبلايص اللي تمثيلها.

كيفاش ينجم يعرف وين إنت: مشاركة البلاصة في تطبيق، stalkerware في تليفونك، جهاز تتبّع في حوايجك ولا كرهبتك، ولا البلاصة تبان في منشوراتك ولا منشورات أصحابك.

- 1 **وثق كل حادثة** في السجلّ متاعك (الفصل 7): التاريخ، الوقت، شنّوة صار.
- 2 **ثبّت في مشاركة البلاصة وطقّيها** (الفصل 4).
- 3 **كان تشك في تطبيق تجسس، ما تفسخوش طول** — الشخص ينجم يلاحظ. أطلب دعم تقني قبل.
- 4 **قول لحد تثق فيه** وأعمل خطة سلامة.

! الملاحظة تنجم تولّي خطر جسدي

كان تحس روحك في خطر، كَلِّم 197 (الشرطة)، 193 (الحرس الوطني) ولا 1899.

التوثيق والحفاظ على الأدلة

التوثيق ما يلزمكش بحتى شي. أما كان نهار تحب تبّغ ولا تشكي، تكون الأدلة موجودة.

شنّوة تحفظ

- ☐ Captures متاع الميساجات، التعليقات ولا المنشورات، **يبان فيهم التاريخ والوقت.**
- ☐ **اسم الحساب والرابط متاعو** (رابط البروفايل ولا الـ @username) — موش الاسم الظاهر برك، خاطرو ينجم يتبدّل.
- ☐ روابط المنشورات، الفيديوهات ولا الصفحات.
- ☐ سجلّ المكالمات والـ SMS.
- ☐ الإيميلات، مع عنوان اللي بعث.
- ☐ ملخص قصير: شنّوة صار، وقتاش، وين، شكون شاف.

كيفاش تعمل captures مليحة

- ثبتّ إنو الـ capture يبان فيها اسم الحساب، التاريخ/الوقت والميساج كامل.
- للبروفيل، صوّر الصفحة والرابط متاعها باين (في الأوردي، خانة العنوان).
- لمحادثة طويلة، أعمل برشا captures فيهم جزء مشترك، بالترتيب.
- في واتساب، تنجم زادة **تصدّر المحادثة** (المحادثة ← المزيد ← تصدير المحادثة (Export chat)) — خلّي الملف المصدّر.
- بعض المنصات تخليّك **تحمل المعطيات متاعك** (فايسبوك، إنستغرام، Google Takeout)، وفيها الميساجات.

كيفاش تحافظ على الأدلة بأمان

- خبّيهم في بلاصة ما يوصلهاش الشخص اللي يأذيك — موش في تليفون مشترك ولا حساب كلاود مشترك.
- خلّي **نسخة ثانية** في بلاصة آمنة أخرى (حساب إيميل منفصل تعرفو إنت برك، شخص تثق فيه، clé USB).
- ما تبدّلش، ما تقصّش وما تكتبش على الملفات الأصلية. أعمل نسخ كان تحتاج.
- عطي الملفات أسامي واضحة: `instagram_@account_tahdid.png_14-03-2026`.

التصاور الحميمة

ما تبغتش تصاور حميمة لحتى حد كدليل. أكتب الرابط ووصف؛ المختصين/ات باش يقولوك كيفاش تكمل بأمان.

التوثيق ينجم يوجع

كي تعاود تشوف المحتوى المسيء، صعب. تنجم تطلب من شخص تثق فيه يعملو معاك ولا في بلاصتك. خوذ راحة.

سجلّ الحوادث

عَمِّر سطر لكل حادثة. خَبِّي الورقة هاذي في بلاصة آمنة. أعمل منها قَدِّ ما تحتاج نسخ.

التاريخ	الوقت	المنصة	الحساب / الرابط	شَنُوة صار	capture محفوظة وين؟	الشهود

مثال: 14/03 · 22:10 · إنستغرام · @example_account (instagram.com/example_account) · هَدِّد بيعث تصاوري لخويا · clé USB، دوسي "مارس" · صاحيتي س. شافت الميساج.

خطة السلامة الشخصية متاعي

خطة السلامة هي مجموعة قرارات تأخذها بالهدوء، من قبل، باش تعرف شنوّة تعمل كان الوضع تخيّب. عمّرها على الورق، وحدك ولا مع شخص تثق فيه. خبّيها، ولا خليها في راسك.

! خبّي الخطة هادي في بلاصة آمنة

كان الشخص اللي يأذك ساكن معاك ولا يفتّش حوايجك، ما تخلّيش الصفحة هادي في بلاصة ينجم يلقاها. تنجم تعطي نسخة لشخص تثق فيه.

الناس اللي تثق فيهم

اللي نجم نكلّمهم ولا نمشيهم، في أي وقت

بلايص آمنة

وين نجم نمشي كان لازمني نخرج بالزربة

كلمة السر بيناتنا

كلمة ولا emoji تفهّم الناس اللي تثق فيهم
"نحتاج مساعدة، كلّموني / إيجيو توا"

جهاز آمن

تليفون ولا أوردي ما يوصلّوش الشخص

حسابات آمنة

حساب إيميل نعرفو أنا برك، للمساعدة وللأدلة

وين مخبّية الأدلة متاعي

وشكون عندو نسخة ثانية

الحوايج اللي نهزّهم

كان لازمني نخرج

أرقام الطوارئ

□ بطاقة التعريف / الباسبور □ التليفون والشارجور □ فلوس / كارطة بنكية
□ المفاتيح □ الدواء □ الأوراق المهمة □ الخطة هادي وكودات الاسترجاع
□ متاعي □ حاجة تريّحني

1899 الخط الأخضر المجاني للنساء ضحايا العنف · 197 الشرطة · 193 الحرس
الوطني · 190 الإسعاف (SAMU)

أساسيات قانونية في تونس

الفصل هذا يعطيك معلومات عامة باش تفهم حقوقك. موش استشارة قانونية وما يعوّضش استشارة مع محامي/ة ولا مختص/ة في القانون.

القانون الأساسي عدد 58 لسنة 2017 المتعلق بالقضاء على العنف ضد المرأة

القانون هذا يعترف بأشكال مختلفة من العنف ضد المرأة – الجسدي، المعنوي (النفسي)، الجنسي، الاقتصادي والسياسي. ويعطي الضحايا الحق في الحماية، المعلومة والإرشاد، والمرافقة القانونية والنفسية.

القانون الأساسي عدد 63 لسنة 2004 المتعلق بحماية المعطيات الشخصية

القانون هذا يحمي المعطيات الشخصية متاعك. نشر معلوماتك ولا تصاورك من غير موافقتك ينجم يكون مخالف للقانون.

وين تنجم تمشي

قبل ما تقرّر

- الخط الأخضر المجاني 1899 للنساء ضحايا العنف.
- وثق قبل (الفصل 7): الأدلة المليحة تعاون في أي إجراء.
- الوحدات المختصة بالبحث في جرائم العنف ضد المرأة في الشرطة والحرس الوطني.
- تنجم تمشي مع شخص تثق فيه ولا مع مختص/ة في القانون.
- جمعيات تقدّم دعم ومرافقة قانونية مجانية.
- إسأل شنّوة باش يصير بعد، شكون باش يعرف، وكيفاش باش تتحمى المعلومات متاعك.

كلمة بصراحة



نعرفو إنو بعض الناس – خاصة من مجتمع الميم – ينجمو يخافو يتوجّهو للسلطات، وإنو الخوف هذا ينجم يكون في بلاصتو. التوجّه للشرطة ولا للمحكمة ديما اختيارك إنت. الدعم القانوني يعاونك تفهم المخاطر والخيارات قبل ما تقرّر، وبعض الخطوات (التوثيق، التبليغ للمنصات، حماية تصاورك) ما تحتاج حتى إجراء رسمي.

تنبيه: المعلومات في الفصل هذا عامة وتنجم تتبدّل. موش استشارة قانونية. على حسب وضعك، إستشير محامي/ة ولا خدمة دعم قانوني. جمعية Intersection ما تنجمش تكون مسؤولة على قرارات تاخذت على أساس الدليل هذا برك.

تهلّ في روحك

العنف الرقمي ما يقعدش في الشاشة. يآثر على النوم، المزاج، التركيز والعلاقات. كي تهلّ في روحك، راك قاعد تحمي في روحك.

ردود فعل طبيعية

بعد العنف الرقمي، برشا ناس يحسّو بـ: خوف كل ما یرنّ التليفون، حشمة ولا لوم للنفس، قلق، صعوبة في النوم، رغبة في الانعزال، ولا غضب. وفما شكون يحس روحو مخدّر. هاذي ردود فعل طبيعية على وضع موش طبيعي.

حاجات صغيرة تعاون

إشعارات أقل

طقي الإشعارات من التطبيقات اللي تجيبك الضغط، ولا سكّت بعض الكلمات والحسابات.

شاشة أقل

قلّص الوقت اللي تقضيه تقرا التعليقات ولا الميساجات. خلّي شخص تثق فيه يشوفهم في بلاصتك.

حد تحكي معاه

أحكي مع شخص تثق فيه. موش لازم تحكي كل شي.

روتين بسيط

نوم، مأكلة، شوية حركة. الحاجات الصغيرة والمنتظمة ترجّعلك الإحساس إنك متحكّم/ة.

فكر في اللي يعطيك الأمان: بلاصة، شخص، نشاط، موسيقى. أكتبو في خطة السلامة متاعك.

كان إنت تعاون في حد

- صدّقو. قول: "موش ذنبك."
- إسمع أكثر مما تنصح. خليه هو يقرّر.
- ما تنشرش الحكاية متاعو ولا التصاور متاعو، حتى باش "تعاون".
- إقترح مساعدة عملية: التوثيق، تقعد معاه وهو يبّلع، تلّوج على المعلومات.
- تهلّ في روحك إنت زادة.

شنّوة يصير في الدعم النفسي

- شخص مختص/ة يسمعك من غير ما يحكم عليك.
- إنت تختار شنّوة تحكي، وبالسرعة اللي تريحك.
- يعاونك تفهم اللي تحس بيه وتلقى طرق تتعامل بيها مع الضغط.
- كل شي سري، بموافقتك.

تنجم تطلب دعم نفسي عبر E-RADAR:

[/radar.intersection.uno/support](https://radar.intersection.uno/support)

! كان عندك أفكار إنك تأذي روحك

عيشك أحكي مع حد توا: شخص تثق فيه، ولا كلّ الإسعاف (SAMU) على 190. إنت تستاهل المساعدة والدعم.

وين تلقى المساعدة

ماكش وحدك! أحنا معاك. هاو شكون تنجم تكلم.

190

الإسعاف (SAMU) — حالة
طبية مستعجلة

193

الحرس الوطني

197

الشرطة

1899

الخط الأخضر المجاني
للنساء ضحايا العنف

E-RADAR — e-radar.intersection.uno

منصة سرية من جمعية Intersection، بالدارجة، بالفرنسية وبالإنجليزية.

بَلِّغْ على حادثة

أحكي شئوة صار، من غير اسم كان تحب. [/report/](#)

أطلب مساعدة

دعم نفسي، قانوني ولا تقني. [/support/](#)

تابع بالكود متاعك

بعد ما تبعث، تاخذ كود متابعة، ختبه في بلاصة آمنة: يخليك تتابع البلاغ متاعك من غير ما
تعطي اسمك. [/track/](#)

في خطر توا؟

شئوة تعمل طول. [/danger/](#)

الموارد

أدلة قصيرة على كل موضوع في الدليل هذا. [/resources/](#)

ضيّعت كود المتابعة؟ ما ينجمش يرجع، أما تنجم ديما تبعث بلاغ ولا طلب جديد.

صفحات المساعدة متاع المنصات

- الحسابات المهكّرة: facebook.com/hacked · instagram.com/hacked · g.co/recover
- التصاور الحميمة: StopNCII.org · takeitdown.ncmec.org

جهات نثق فيها قريبة مني

تتعمر من Intersection ولا منك إنت: جمعيات، خدمات وناس تنجم تتوجّهلهم في منطقتك.

الاسم	شئوة يقدمو	كيفاش نتواصل

قوائم تحقق في صفحة وحدة

حظ علامة كل ما تكمل حاجة. موش لازم تعمل كل شي مرة وحدة.

أمان الحسابات

☐ الإيميل متاعي عندو جملة سر قوية وما تتعاودش، و2FA.

☐ كل حساب مهم عندو كلمة السر متاعو (ولا نستعمل password manager).

☐ ال 2FA مفعلة: فايسبوك/إنستغرام، واتساب (PIN)، Google، تيك توك.

☐ كودات الاسترجاع متاعي مكتوبة ومخبية في بلاصة آمنة.

☐ ثبتت في الجلسات النشطة وخرجت الأجهزة اللي ما نعرفهاش.

☐ إيميل ورقم تليفون الاسترجاع متاعي ومحدثين.

☐ فسخت التطبيقات المرتبطة اللي ما نستعملهاش.

☐ حتى حد ما يعرف كلمات السر ولا الكودات متاعي.

تليفوني

☐ قفل الشاشة بـ PIN من 6 أرقام ولا أكثر ما يعرفو حد.

☐ محتوى الإشعارات مخبّي في شاشة القفل.

☐ راجعت التطبيقات متاعي والصلاحيات متاعها (البلاصة، الميكرو، إمكانية الوصول).

☐ مشاركة البلاصة مطفية وين ما نحتاجهاش (Maps، Find My، Snap Map).

☐ حفظ البلاصة في الكاميرا مطفي.

☐ حساب الكلاود متاعي (iCloud / Google) مأمّن ونعرف شنوّة الأجهزة الداخلة ليه.

☐ ثبّيت في "الأجهزة المرتبطة" في واتساب.

☐ النظام والتطبيقات محدّثين.

كان فما شكون يبتزّ فيّ

ما نخلّصش وما نبعث حتى شي آخر. ☐

ما نفسخس المحادثة. ☐

عملت captures فيهم اسم الحساب، الرابط والتاريخ. ☐

وقّفت نجاوب بعد ما وثّقت. ☐

بدّلت كلمات السر متاعي وفعلت الـ 2FA. ☐

رجّعت حساباتي خاصة وخيّت قوائم الأصدقاء/المتابعين. ☐

بلّغت على الحساب للمنصة. ☐

استعملت StopNCII.org / Take It Down كان فما تصاور. ☐

حكيت مع شخص نثق فيه. ☐

نعرف الأرقام: 1899 · 197 · 193 · 190. ☐

موش ذنبك. ماكش وحدك.



ماكش وحدك! أحنا معاك.

E-RADAR منصة سرية من جمعية Intersection للنساء، البنات ومجتمع الميم اللي يتعرّضو للعنف الرقمي المبني على النوع الاجتماعي في تونس.

e-radar.intersection.uno

190 · 193 · 197 · 1899

الدليل هذا يعطي معلومات عامة. موش استشارة قانونية، طبية ولا تقنية لوضعك بالذات. أسامي القوائم في التطبيقات تتبدّل مع الوقت. نسخة 2026.