نحو بيئة رقمية امنة
للمدافعات عن حقوق الانسان في العـــــراق

دليل الحماية الرقمية للمدافعات عن حقوق الانسان:

نحو فضاء رقمي آمن في العراق
بين المعرفة والممارسة لحماية أصوات النساء
في الفضاء الرقمي

الاعداد:
المحامي وليد علي عبدي | إقليم كوردستان - العراق
رايـــة شـــاربين | الأردن


SMEX
تعزيز الحقوق الرقمية
advancing digital rights


SODHR NGO
منظمة سلامتك للدفاع عن حقوق الانسان

نحو بيئة رقمية امنة للمدافعات عن حقوق الانسان في العراق

دليل الحماية الرقمية للمدافعات عن حقوق الانسان:

نحو فضاء رقمي آمن في العراق
بين المعرفة والممارسة لحماية أصوات النساء
في الفضاء الرقمي

الاعداد:

المحامي وليد علي عبدي | إقليم كوردستان - العراق

رايـــة شـــاربيـن | الأردن

اسم المشروع: **نحو بيئة رقمية امنة للمدافعات عن حقوق الانسان في العراق**

اسم الدليل: **دليل الحماية الرقمية للمدافعات عن حقوق الانسان: نحو فضاء رقمي آمن في العراق بين المعرفة والممارسة لحماية أصوات النساء في الفضاء الرقمي**

اسم المنظمة المنفذة: **منظمة سلامتك للدفاع عن حقوق الانسان | العراق**

الاعداد: **المحامي وليد علي عبدي | إقليم كوردستان-العراق**
رايـــة شـــاربين | الأردن

اسم المنظمة الشريكة (المانحة): **SMEX**
مبادرة صندوق الحقوق الرقمية لمنطقة غرب آسيا وشمال أفريقيا" (Digital Rights Fund for WANA)

الهدف الرئيسي للمشروع: **تعزيز وتمكين المدافعات عن حقوق الإنسان في العراق من خلال توفير بيئة رقمية آمنة تمكنهن من العيش والعمل بحرية وأمان في الفضاء الرقمي**

منفذ التصميم: **باور محمد صديق**
مطبعة: **Seven Points**

محتوى الدليل

٤. الحماية الرقمية: نحو بيئة رقمية امنة للمدافعات عن حقوق الانسان

القسم الأول: أدوات وتقنيات الحماية الرقمية

١. مقدمة: أساسيات الحماية الرقمية العامة: سلوك يومي يحميكِ... لا مجرد مهارة تقنية

١. الروتين اليومي للحماية الرقمية الشخصية

الروتين الأول: لنبدأ من الباب الأمامي: راجعي إعداداتكِ

الروتين الثاني: نظّفي المساحة: احذفي ما لا يُطمئنكِ

الروتين الثالث: تأكدي من أن جهازكِ «معكِ»، لا ضدكِ

الروتين الرابع: امسكي زمام الأمور: كلمات السر

الروتين الخامس: كوني واعية لما تنشرينه يوميا

الروتين السادس: راقبي الزوار غير المرئيين

الروتين السابع: خفّفي الحمل عن جهازكِ

الروتين الثامن: علبة الأدوات

الروتين التاسع: هل هناك تحديث متوفر؟ لا تؤجليه!

٢. رفيقاتك الرقميات: تطبيقات وبرامج لا غنى عنها لحمايتك الرقمية اليومية

خطوتك الأولى: هدوء في الاتصال، أمان في الهوية

خطوتك الثانية: حفظ الملفات الحساسة — لا تتركي أثركِ مكشوفاً!

خطوتك الثالثة: «حسابكِ هو هويتكِ... لا تتركي المفاتيح لأي أحد»

خطوتك الرابعة: ابحثي وتواصلي بأمان... دائماً!

خطوتك الخامسة: افتحي بريدكِ بعين الحذر... لا بعين الثقة!

خطوتكِ السادسة: واي فاي آمن... بيتكِ الرقمي يبدأ من هنا

خطوتكِ السابعة: الرفاهية الرقمية... لأن سلامتكِ النفسية جزء من الحماية

القسم الثاني: سلوكيات الحماية الرقمية في المواقف المختلفة:

أولا: الأمن الرقمي أثناء تغطية الاحتجاجات والمظاهرات السلمية

ثانيا: الحماية الرقمية داخل مؤسسات المجتمع المدني:

ثالثا: عندما يتحول الفضاء الرقمي إلى ساحة تهديد: كيف نواجه المضايقات والابتزاز الإلكتروني؟

رابعا: توثيق انتهاكات حقوق الإنسان الرقمية

خامسا: التهيئة للعمل في ظل انقطاع الإنترنت

القسم الثالث: التخطيط للطوارئ الرقمية:

خطوتكِ الأولى: إعداد خطة الاستجابة للهجمات الإلكترونية:

خطوتك الثانية: بناء شبكات دعم وتعاون مع جهات محلية ودولية لحالات الطوارئ

٥. المراجع والمصادر والموارد الإضافية

الخاتمة

شكر وتقدير

1. المقدمة

في بيئة متقلّبة سياسيًا وأمنيًا، واقتصاديًا واجتماعيًا، تواجه المدافعات عن حقوق الإنسان في العراق وإقليم كوردستان تحديات متزايدة تهدّد أمنهن الرقمي، وتُقوّض قدرتهن على الاستمرار في أداء أدوارهن الحيوية في حماية الحقوق والحريات. لم تعد الانتهاكات محصورة في المجال الواقعي فقط، بل امتدّت بقسوتها إلى الفضاء الرقمي، فأصبح الاختراق والتشهير والمراقبة والابتزاز من الأدوات الجديدة لإسكات الأصوات النسائية المدافعة، وعرقلة نضالهن من أجل العدالة.

من هذا الواقع، أطلقت منظمة سلامتك للدفاع عن حقوق الإنسان في العراق (SDHR) مشروعًا بعنوان «نحو بيئة آمنة للمدافعات عن حقوق الإنسان في العراق»، بدعم من مبادرة «صندوق الحقوق الرقمية لمنطقة غرب آسيا وشمال أفريقيا» التي تديرها منظمة SMEX. يهدف المشروع إلى تعزيز وتمكين المدافعات عن حقوق الإنسان من حماية أنفسهن، ومؤسساتهن، والمجتمعات التي يعملن معها، من المخاطر الرقمية المتزايدة، من خلال تقديم هذا الدليل الذي يجمع ما بين المعرفة، والمهارة، والسلوك، والممارسة.

لا يقدّم هذا الدليل مجرد تعليمات تقنية أو نصائح رقمية، بل يستند إلى الواقع الميداني للمدافعات، مستلهمًا تجاربهن الحقيقية من مختلف محافظات العراق، ومن سياقات عمل متنوّعة وشائكة. وقد حاولنا أن نُعيد صياغة الحماية الرقمية لا كعبء، بل كجزء أصيل من العمل الحقوقي، وكأداة تُستخدم من أجل الاستمرار، لا الانسحاب.

يوفّر هذا الدليل أدوات وقائية واستجابات طارئة، ويقدّم تطبيقات موثوقة،

وسـلوكيات روتينيـة، وخططًـا عمليـة على المسـتويين الشـخصي والمؤسسـاتي، تسـاعد المدافعـات في التعامـل مـع الهـجمات الرقميـة، وتوثيـق الانتهـاكات، ومواجهـة الابتـزاز الإلـكتروني، والعمـل في ظـلّ انقطـاع الإنترنـت، والتحـضير لحـالات الطـوارئ.

وهو مُوجّه بشكل رئيسي إلى:

- المدافعات عن حقوق الإنسان في العراق وإقليم كوردستان؛
- منظمات المجتمع المدني المحلية
- الصحفيات والمدوّنات والناشطات الإعلاميات؛
- النقابات والجمعيات التي تمثل المدافعين والمدافعات.

يطمـح هـذا العمـل إلى أن يكـون مرجعًـا عمليًـا، ورفيقًـا في الطريـق، وشـهادة تضامـن نسـجت سـطورها مـن الميـدان، لا مـن الخيـال. فالدفـاع عـن الحقـوق في العـراق لم يكـن يومًـا طريقًـا سـهلًا، لكننـا نؤمـن أن الأمـان الرقمـي هـو أحـد مفاتيـح الاسـتمرار، وأن الوعـي هـو الـدرع الأهـم في مواجهـة المخاطـر.

- **دليل الحماية الرقمية**

هـذا الدليـل أعـد خصيصًـا لـكِ، أنـتِ المدافعـة عـن حقـوق الإنسـان التـي تعملـين وسـط بيئـة مليئـة بالتحديـات والمخاطـر، والتـي تسـتخدمين الإنترنـت كوسـيلة للتعـبير، للتوثيـق، للتنظيـم، أو حتـى فقـط للتواصـل بأمـان.

سـواء كنـتِ صحفيـة، ناشـطة، محاميـة، باحثـة، أو عضـوة في منظمـة مجتمـع مـدني، فهـذا الدليـل هـو رفيقـكِ الرقمـي، الـذي يسـاعدكِ على حمايـة نفسـكِ ومَـن حولـكِ في الفضـاء الرقمـي.

الدليـل موجـه للنسـاء والفتيـات المدافعـات عـن حقـوق الإنسـان في العـراق، بمـا في ذلـك ذوات الإعاقـة أو المنتميـات إلى مجتمعـات مهمشـة أو نائيـة، واللـواتي قـد لا تصـل إليهـن دائمًـا فـرص التدريـب أو المـوارد التقنيـة اللازمـة بسـبب التحديـات الجغرافيـة أو اللغويـة أو التقنيـة.

- **ماذا يقدم لكِ هذا الدليل؟**

- يمنحكِ فهمًا عميقًا للسياق الرقمي الذي تعملين فيه، مع تسليط الضوء على التهديدات والانتهاكات التي تستهدف النساء المدافعات في العراق.
- يوضح لكِ المخاطر الرقمية الأكثر شيوعًا، ويساعدكِ على التعرف عليها مبكرًا قبل أن تتحول إلى تهديد حقيقي.
- يُزوّدكِ بإرشادات عملية ومبسطة لتأمين أدواتك الرقمية، حماية اتصالاتك، واستخدام الإنترنت بطريقة أكثر أمانًا.
- يساعدكِ في وضع خطط استجابة لحالات الطوارئ الرقمية، من الهجمات السيبرانية، إلى الابتزاز، إلى فقدان البيانات.
- يعرّفكِ على جهات دولية ومحلية يمكنكِ الرجوع إليها عند التعرض لأي انتهاك رقمي أو تهديد مباشر.
- يُشجعكِ على بناء وعي رقمي مشترك مع زميلاتكِ المدافعات، ليكون الأمن الرقمي جزءًا من عملكن اليومي لا مجرد رد فعل عند الطوارئ.

يأتي هذا الدليل استجابةً للواقع المعقد الذي تعمل فيه المدافعات، لا سيما في ظل تصاعد الانتهاكات الرقمية التي تستهدف النساء المدافعات عن حقوق الانسان والناشطات.

وتم إعداد هذا الدليل استنادًا إلى مقابلات مباشرة مع مدافعات عن حقوق الإنسان من محافظات مختلفة في العراق وإقليم كردستان، حيث شاركن بتجاربهن الشخصية، وتحدياتهن، والمخاوف التي يواجهنها في الفضاء الرقمي.

لقد استمعنا إلى أصواتهن، وحرصنا أن يكون هذا الدليل انعكاسًا لما يشعرن به فعلاً، لا لما يُفترض أن يُقال لهن. هذا الدليل بُني بناءً على احتياجاتهن، ليكون أداة حقيقية لحمايتهن، ودعماً مستمراً لجهودهن.

الدليل ليس مجرد مجموعة من النصائح، بل هو مساحة آمنة للتعلم والتفكير، صُممت بعناية لتكوني أكثر قدرة على المواصلة، والتعبير، والمواجهة، دون أن تكوني وحدكِ في هذا المسار.

2. الخلفية والسياق: التهديدات الرقمية للمدافعات عن حقوق الإنسان في العراق

خلال السنوات الأخيرة، ازدادت المخاطر الرقمية التي تواجهها المدافعات عن حقوق الإنسان في العراق، نتيجة لتفاقم الوضعين السياسي والأمني، إلى جانب انتشار التكنولوجيا واستخدامها الواسع في النشاط الحقوقي والتعبير عن الرأي. في هذا السياق المعقّد، أصبحت التهديدات الرقمية أداة فعالة للرقابة، التخويف، والتضييق، خاصة في بيئة لا تزال تفتقر إلى ضمانات حماية حقيقية في الفضاء الرقمي.

- **البيئة المتغيرة للنشاط الحقوقي الرقمي**

منذ احتجاجات تشرين عام ٢٠١٩، برزت النساء المدافعات عن حقوق الإنسان في العراق وإقليم كوردستان في مشهد الاحتجاجات، سواء عبر التوثيق، أو المشاركة، أو التنظيم الرقمي، وهو ما جعلهن عرضة مباشرة لموجة من الانتهاكات الرقمية. هذه الانتهاكات شملت اختراق الحسابات، التشهير، الابتزاز، المراقبة، والعنف اللفظي الإلكتروني. في مقابلات أُجريت مع مدافعات في بغداد، ذي قار، البصرة، النجف، واسط، بابل، الانبار، نينوى والسليمانية،

تـم التأكيـد مـراراً على أن التهديـدات الرقميـة تمثّـل اليـوم أحـد أخطـر أشـكال القمـع الـذي تتعـرض لـه الناشـطات.

"مجرد أن أكتب رأياً بسيطاً، أو أشارك في التعبير عن رأيي عن أي موضوع يتعلق بالانتهاكات التي تتعرض له النساء، أبدأ أتلقى رسائل تهديد أو تشويه سمعة. الأمر أصبح معتاداً وخطيراً في آنٍ معاً."

مدافعة من بغداد

- **الأمية الرقمية والفجوة في بناء القدرات**

رغـم انتشـار أدوات التكنولوجيـا، إلا أن الأميـة الرقميـة مـا زالـت تحـدّ مـن قـدرة الكـثير مـن المدافعـات على الحمايـة الذاتيـة. ويبرز هـذا التحـدي بشـكل خـاص في صفـوف الشـابات مـن المناطـق النائيـة أو المجتمعـات التـي تقيّـد وصـول النسـاء إلى المهـارات الرقميـة. لا تقـتصر هـذه الفجـوة على الجانـب التقني، بـل تشـمل أيضـاً غيـاب الفهـم لأسـاليب الحمايـة الرقميـة الأساسـية. هـذا الضعـف يترك المدافعـات عرضـة للاختراق والتتبـع والتشـهير، دون أدوات حقيقيـة للدفـاع.

ويُلاحظ بشـكل خـاص غيـاب البرامج المتخصصـة التي تأخـذ في الاعتبـار احتياجات النسـاء والفتيـات ذوات الإعاقـة مـن المدافعـات عـن حقـوق الانسـان. فالكـثير منهـن لا يحصلـن على فـرص تدريبيـة مخصصـة، أو مـوارد تقنيـة مـيسّرة، مـا يزيـد مـن تهميشـهن في المسـاحات الرقميـة.

على الرغـم مـن أهميـة الحمايـة الرقميـة للمدافعـات عـن حقـوق الإنسـان في العـراق، إلا أن الـبلاد تعـاني مـن ضعـف كـبير في البنيـة التحتيـة الخاصـة بهـذه الحمايـة. يرافـق ذلـك نقـص في الوعـي المجتمعـي والرسـمي بأهميـة الأمـن الرقمـي، خصوصـاً للمدافعـات اللـواتي يواجهـن تهديـدات متزايـدة عبر الفضـاء الرقمـي. مـن أبـرز التحديـات التـي تواجـه المدافعـات هـو ضعـف الدعـم القانـوني لضحايـا الجرائـم الرقميـة، حيـث تفتقـر القـوانين العراقيـة الحاليـة إلى آليـات واضحـة وفعالـة لمحاسـبة المعتديـن وحمايـة المدافعـات اللـواتي يتعرضـن لانتهـاكات رقميـة.

"عندما حاولت التبليغ عن تهديدات إلكترونية، وجدت نفسي وحيدة في مواجهة النظام... لا قانون يحمي، ولا جهة تستجيب."

مدافعة من بغداد

- **أبرز التهديدات الرقمية**

إلى كل مدافعة عن حقوق الإنسان في العراق:

نعلم أن واقعكِ في الفضاء الرقمي محفوف بالمخاطر، وأنكِ قد تكونين قد تعرضتِ أو ما زلتِ تتعرضين لأحد أشكال الانتهاكات الرقمية، أو حتى أكثر من نوع منها. هذه الانتهاكات، التي تتزايد يومًا بعد يوم، تمسّ حياتكِ الشخصية، وسمعتكِ الاجتماعية، وسلامتكِ النفسية، وقدرتكِ على الاستمرار في عملكِ الحقوقي. نضع بين يديكِ هنا أبرز أشكال الانتهاكات الرقمية التي رُصدت ميدانياً من خلال المقابلات مع المدافعات في العراق وإقليم كوردستان، والتي تم توثيقها أو التبليغ عنها، مع محاولة تسليط الضوء على تطورات جديدة ظهرت نتيجة تطور أدوات الذكاء الاصطناعي، أو التي يُتوقع أن تظهر مستقبلاً:

١. **مصيدة الروابط: التصيد الاحتيالي الذكي:** تقنيات التصيد أصبحت أكثر تعقيداً، ولم تعد تعتمد على رسائل بسيطة بل قد تأتي على شكل روابط

مـن جهـات تبـدو موثوقـة، أو حتـى باسـتخدام الـذكاء الاصطناعـي لمحـاكاة لغـة الحديـث الخاصـة بصديقاتـك أو زميلاتـك. الوقـوع في هـذه المصيـدة قـد يـؤدي لاختـراق بريـدك، حسـاباتك، أو ملفـات حساسـة لـكِ أو للضحايـا الذيـن تدافعـين عنهـم.

٢. **العيون الخفية: المراقبة الرقمية المستمرة:** تشـمل تتبـع موقعـكِ الجغـرافي، مراقبـة نشـاطكِ عـلى وسـائل التواصـل، وحتـى اعـتراض اتصالاتـكِ في بعـض الحـالات. هـذه المراقبـة قـد تتم مـن جهـات رسـمية أو مجموعات غـير معروفة، وقـد تصـل إلى التجسـس عـبر تطبيقـات مزروعـة في هاتفـك دون علمـك.

٣. **السلاح القذر: التشهير والابتزاز الرقمي:** ربمـا يكـون هـذا هـو الأخطـر عـلى الإطـلاق. يُسـتخدم فيـه محتـوى شـخصي (حقيقـي أو مفبرك) لتشـويه سـمعتكِ أو الضغـط عليـكِ للتوقـف عـن العمـل الحقوقـي. يتلاعـب هـذا النـوع مـن الانتهـاك بالعُـرف الاجتماعـي والوصمـة، ويسـتهدفكِ في أعمـق مناطـق الأمـان الشـخصي.

٤. **الغرف المظلمة:** العنـف الرقمـي اللفظـي والجسـدي المُهـدد: يشـمل التهديـد بالقتل، الاغتصاب، الإيذاء الجسـدي، أو حتى اسـتهداف عائلتكِ. هذه التهديدات غالبًـا مـا تكـون متكـررة ومنسـقة، هدفهـا الأسـاسي هـو بـث الرعـب فيـكِ وعزلـكِ عـن الفضـاء العـام.

٥. **الطرد الصامت: التمييز الرقمي ضد النساء والفتيات:** يتجسـد في تجاهـل آرائـك، إقصائـكِ مـن النقاشـات، التقليـل مـن مسـاهمتكِ، أو حتـى تحريـض الآخريـن عـلى مهاجمتـكِ بسـبب كونـكِ امـرأة. الإنترنـت هنـا يصبـح انعكاسًـا صارخًـا لواقـع اجتماعـي قائـم عـلى التمييـز.

٦. **التلاعب العميق: فبركة الصور والفيديوهات (التزييف العميق - Deepfake):** مـع تصاعـد اسـتخدام الـذكاء الاصطناعـي، بـات مـن الممكـن تركيـب صـور أو فيديوهـات لـكِ في مواقـف لم تحـدث، بهـدف النيـل مـن مصداقيتـكِ أو سـمعتكِ. هـذه التقنيـة تتطلـب وعيًـا كبـيراً، حيـث يصعـب أحيانًـا تمييـز المـواد المفبركـة مـن الحقيقيـة.

٧. **الاختناق الرقمي:** الإبلاغ الجماعي وتعطيل الحسابات: تقوم مجموعات منظمة أو أفراد بالإبلاغ المكثف عن حسابكِ، مما يؤدي إلى إغلاقه أو تقييد ظهوره، وبالتالي إسكات صوتكِ دون الحاجة إلى مواجهة مباشرة.

٨. **الاختراق العاطفي:** الاستهداف عبر العلاقات الشخصية: يتمثل في انتحال صفة صديقة أو شخص مقرب لكِ، لكسب ثقتكِ ثم سرقة معلوماتكِ أو إيذائكِ. هذا النوع من الهجوم شديد التأثير نفسيًا لأنه يستغل الثقة والعلاقات الإنسانية.

"هددوني بنشر صور خاصة بي إن لم أتوقف عن الكتابة. لم أكن أملك أي وسيلة للدفاع، وحتى المقربين مني نصحوني بالصمت."

مدافعة من بغداد

هذه الانتهاكات ليست مجرد حوادث رقمية عابرة، بل أدوات ممنهجة لقمع صوتكِ والتأثير على قراركِ. لكن الوعي بها هو الخطوة الأولى للمواجهة.

في الأقسام التالية من هذا الدليل، سنعرض كيف يمكن مواجهة كل نوع من هذه الانتهاكات، ونزودكِ بأدوات عملية للحماية الرقمية، لنواصل معًا النضال في سبيل العدالة وحقوق الإنسان بأمان وثقة.

"كلمة واحدة تم اجتزاؤها من سياقها جعلت حياتي جحيماً. الرسائل لم تتوقف لأيام. حتى عائلتي بدأت تشك."

ناشطة من كركوك

- **الإطار القانوني والاجتماعي**

رغم وجود مسودة «قانون جرائم المعلوماتية» في مجلس النواب العراقي منذ عام ٢٠١١، إلا أنه لم يُشرّع حتى اليوم. وتُثير المسودة الحالية قلقاً واسعاً بين منظمات المجتمع المدني والمدافعات عن حقوق الإنسان، نظرًا لاحتوائها على مواد فضفاضة وتمييزية قد تُستخدم لتقييد حرية التعبير بدلاً من حماية الضحايا، خصوصاً النساء والفتيات. ورغم تقديم ملاحظات

واعتراضات متعددة من جهات حقوقية محلية ودولية، لم تُعتمد تعديلات جوهرية على المسودة حتى الآن.

"نعرف التهديدات، لكننا نرفض أن نصمت. هذا الدليل هو أحد أشكال المقاومة."
مشاركة في مراجعة مسودة هذا الدليل

أما القوانين النافذة حالياً، فتقتصر غالبًا على مواد متفرقة في قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩، لا سيما المواد المتعلقة بالتشهير أو التهديد. ومع أن هذه النصوص قد تُستخدم أحياناً لملاحقة بعض الجرائم الرقمية، إلا أنها تفتقر إلى آليات إنفاذ واضحة وفعالة في السياق الرقمي.

ويُعد الإبلاغ وتقديم الشكاوى أحد أكبر التحديات التي تواجه النساء والفتيات، خاصة أن هذه الانتهاكات غالبًا ما ترتبط بموضوعات الشرف والسمعة، مما يخلق ضغطًا اجتماعيًا ونفسيًا يمنع العديد من النساء المدافعات من اللجوء إلى القضاء أو حتى الحديث عمّا تعرّضن له. كما أن عبء الإثبات يقع بشكل كامل على الضحية، ما يزيد من تعقيد الحصول على العدالة.

"الخوف من أن تُستخدم صورة أو كلمة ضدي يجعلني أتراجع عن المشاركة أحياناً، حتى لو كان هذا ضد مبادئي."
مدافعة من البصرة

لذا لا يمكن فصل التهديدات الرقمية عن البيئة السياسية والأمنية التي تعمل ضمنها المدافعات، فهي ليست مجرد تحديات تقنية، بل هي انعكاس مباشر لواقع معقد ومهدد.

"نحتاج أدوات سهلة، وناس تفهم واقعنا وتساعدنا، مو بس برامج تقنية معقدة."
ناشطة من إقليم كوردستان

في المشهد الرقمي المتطور باستمرار، يصبح من الضروري فهم أساسيات السلامة والأمن الرقمي عبر الإنترنت، مع مراعاة الإطار القانوني الوطني والدولي، والنظر إليه من خلال الممارسات والسوابق التي وضعتها السلطات المختصة في العراق.

يهدف هذا الدليل إلى توضيح أهمية الحماية الرقمية وتقديم أساليب فعالة لتحقيقها، بدءاً من تعزيز الوعي بالحقوق الرقمية ضمن السياق التشريعي الوطني والدولي، مروراً بالسلوكيات الرقمية الواجب اتباعها، وصولاً إلى استخدام الأدوات والتطبيقات الآمنة التي تتناسب مع طبيعة عمل المدافعات في العراق. ومن خلال تقديم توصيات وخطط عمل عملية، نسعى معاً لمواجهة التهديدات الرقمية والحفاظ على سلامة وأمان المدافعات في عالم الإنترنت المتزايد التعقيد.

"التمييز الرقمي هو امتداد للعنف المجتمعي العام ضد النساء والمدافعات على وجه الخصوص، حيث تُحمّل الضحية مسؤولية الهجوم، وتُوصم بالعار، بينما يفلت المعتدي من العقاب."

تعليق لمشاركة اطلعت على مسودة الدليل

- **الحاجة إلى دليل عملي وواقعي**

كل هذه العوامل تبرز الحاجة إلى دليل متخصص، مبني على واقع النساء في العراق، ويقدّم لهن:

- سُبل وقائية لحماية أنفسهن رقمياً.
- أدوات تقنية موثوقة وسهلة الاستخدام.
- فهماً للسياق القانوني والحقوقي.
- إرشادات واضحة للتصرف في حالات الابتزاز، التهديد، أو التشهير.

هذا الدليل ليس بديلاً عن المؤسسات، بل هو أداة دعم ميداني موجهة لكل امرأة عراقية تدافع عن حقوق الإنسان، لتكون أقوى، وأكثر أمناً، وأكثر

وعيـاً في فضـاء رقمـي غير متـوازن.

"ما نحتاجه ليس فقط أدوات تقنية، بل من يفهم كيف نشعر، وكيف نُهدّد، وكيف يمكن أن نخسر كل شيء بسبب صورة أو كلمة."

مشاركة في مقابلات إعداد هذا الدليل

3. المدافعات عن حقوق الانسان والحقوق الرقمية

أولا: المدافعات عن حقوق الانسان:

في العراق، حيث تواجه المرأة تحديات كبيرة في كل جانب من جوانب حياتها، يبرز دور المدافعات عن حقوق الإنسان كصوت شجاع يرفع مطالب العدالة والكرامة والمساواة. أنتِ كمدافعة عن حقوق الإنسان، تواجهي مواقف صعبة ليست فقط من المجتمع أو السلطات، بل أحيانًا من بيئة الإنترنت نفسها التي يجب أن تكون مكانًا آمنًا للتعبير والمشاركة.

هذه المقدمة تهدف إلى توضيح من أنتِ، وما يعنيه أن تكوني مدافعة عن حقوق الإنسان في بلد مليء بالتحديات السياسية والاجتماعية والأمنية، حيث تلتقين بين واجب الدفاع عن الحقوق الشخصية والمجتمعية وبين مخاطر كثيرة قد تعترض طريقك.

إن فهم هويتك كمدافعة عن حقوق الإنسان هو خطوة أولى مهمة لحمايتك وتعزيز عملك، ولأنك تعرفين حقوقك ومكانتك، يمكنك مواجهة التحديات الرقمية بكل قوة وثقة.

"المدافعات عن حقوق الإنسان يرفعن الصوت ليس فقط من أجل أنفسهن، بل من أجل مستقبل أكثر عدلاً ومساواة لكل النساء."

ملالا يوسفزاي،
ناشطة حقوقية حائزة على جائزة نوبل السلام

أ. المدافعات عن حقوق الإنسان في البيئة الرقمية

من هي المدافعة عن حقوق الإنسان؟

قد لا تملكين لقبًا رسميًا أو منصبًا في منظمة، لكنكِ مدافعة عن حقوق الإنسان حين ترفعين صوتكِ دفاعًا عن العدالة، أو تتضامنين مع امرأة تعرّضت للعنف، أو توثّقين انتهاكًا، أو تشاركين في حملة، أو تكتبين منشورًا تطالبين فيه بالحقوق. المدافعة عن حقوق الإنسان ليست فقط من تعمل في مؤسسة حقوقية، بل كل امرأة أو فتاة تنخرط بشكل سلمي في الدفاع عن كرامة الإنسان، سواء في المنزل، أو الشارع، أو المدرسة، أو الفضاء الرقمي.

في العراق، المدافعات عن حقوق الإنسان يعملن في بيئة مليئة بالتحديات، ليس فقط بسبب القيود القانونية أو المخاطر الأمنية، بل أيضًا بسبب الأعراف والتقاليد الاجتماعية التي قد تُقيّد حرية المرأة وتحمّلها أعباء إضافية عند التعبير عن رأيها أو ممارستها لدورها في المجتمع. ومع ذلك، لا تزال الكثير من النساء يواصلن العمل من أجل التغيير، ويمثلن مصدر إلهام لأخريات.

قد تكونين محامية، صحفية، ناشطة، طالبة، ممرضة، موظفة، أو حتى أمًّا تدافع عن حق أولادها في التعليم والحماية، كل هذه الأدوار تحمل في جوهرها معنى الدفاع عن الحقوق، إذا اقترنت بالإيمان بالعدالة والعمل من أجلها.

تعتبر المدافعات عن حقوق الإنسان منظمات وأفراداً يعملون على حماية حقوق الإنسان والدفاع عنها. فهن يسعين إلى ضمان الحقوق المدنية والسياسية والاقتصادية

"أنا مدافعة عن حقوق الإنسان لأنني أؤمن بأن الكرامة والحرية حق لكل إنسان. كلماتي أو أفعالي هو صوتي وهو مكمل لأصوات كل النساء ، وأنا هنا لأرفع ذلك الصوت رغم كل الصعوبات والمخاطر التي تواجهني."

مدافعة عن حقوق الانسان من بغداد

والاجتماعية والثقافية وغيرها من الحقوق بما في ذلك الحقوق والحريات الأساسية والحق في الخصوصية والأمان الرقمي، مكافحة التمييز الجنسي والعنصري والعنف الرقمي وضمان النساء والفئات الضعيفة.

"أنا لستُ مشهورة، ولا أملك منصة كبيرة، لكنني أرفض أن أرى الظلم وأسكت. هذا وحده يكفي لأن أُعرِّف نفسي كمدافعة عن حقوق الإنسان."

مشاركة شابة من البصرة،
خلال مقابلة حول تجارب المدافعات

يمكنك من خلال هذا الفيديو الذي أعدته أمنيستي (Amnesty) وبشكل بسيط فهم من هن المدافعات عن حقوق الانسان:
https://www.youtube.com/watch?v=R8oCpLJB97Q

إذا هل انت مدافعة عن حقوق الانسان؟

لإعطاء صورة أوضح، يمكننا الرجوع إلى الإعلان المتعلق بحق ومسؤوليات الافراد والجماعات وهيئات المجتمع في تعزيز وحماية حقوق الانسان والحريات الأساسية الذي اقرته الجمعية العامة للأمم المتحدة في ١٠ ديسمبر ١٩٩٨. وقد عرّفت المدافعين عن حقوق الإنسان على النحو التالي:

"١. من حق كل شخص، بمفرده وبالاشتراك مع غيره، ان يدعو ويسعى الى حماية وإعمال حقوق الانسان والحريات الأساسية على الصعيدين الدولي والوطني».

صدر هذا الإعلان لأهمية دور المدافعين عن حقوق الإنسان وضرورة حمايتهم في جميع أنحاء العالم في دعم حركة حقوق الإنسان.

وقد عرفتها منظمة فرونتلاين ديفيندرز Frontline Defenders، وهي احدى المنظمات الدولية التي تعمل على حماية المدافعين عن حقوق الانسان بأنهم «هم الأشخاص الذين يعملون، بصورة فردية أو جماعية، وبشكل سلمي، نيابة عن الآخرين من أجل تعزيز حقوق الإنسان المعترف بها دولياً والدفاع عنها».

إذا من هنّ المدافعات عن حقوق الإنسان في البيئة الرقمية؟

المدافعة عن حقوق الإنسان في البيئة الرقمية، هي كل امرأة أو فتاة تستخدم الإنترنت أو وسائل التواصل الاجتماعي أو أدوات التكنولوجيا للمطالبة بالحقوق، أو كشف الانتهاكات، أو دعم قضية إنسانية، أو نشر الوعي حول قضايا مجتمعها. قد تكتبين منشورًا، أو تنظمين حملة رقمية، أو توثقين حدثًا، أو تدافعين عن ضحية عبر الإنترنت، كل ذلك هو شكل من أشكال الدفاع الرقمي عن حقوق الإنسان.

في العراق، أصبحت البيئة الرقمية واحدة من أهم مساحات العمل الحقوقي، لكنها أيضًا من أكثر المساحات خطورة على النساء والفتيات. لأنكِ كامرأة تعبرّين عن رأيك أو تدافعين عن قضية، فقد تُستهدفين بالتشهير، المراقبة، الابتزاز، أو الهجمات اللفظية. ولهذا، فإن المدافعة الرقمية لا تحتاج فقط إلى الشجاعة، بل إلى الوعي والمعرفة بكيفية حماية نفسها في هذا الفضاء المعقّد.

أنتِ مدافعة في البيئة الرقمية عندما ترفعين صوتكِ رغم الصمت الذي يُفرض، وتتمسكين بحقكِ في التعبير رغم التهديدات، وتستعملين التكنولوجيا كأداة مقاومة لا كأداة ترهيب.

ب. ما الذي تقمن به المدافعات عن حقوق الانسان؟

قد لا تسألين نفسك يومًا هذا السؤال، لأنكِ ببساطة «تقومين بالفعل» يومًا بعد يوم. لكن في جوهره، عمل المدافعة عن حقوق الإنسان هو الدفاع عن الكرامة، والعدالة، والمساواة — سواء بصوتكِ، أو قلمكِ، أو وقوفكِ إلى جانب من لا صوت لهم.

أنتِ كامرأة مدافعة، تقومين بأدوار عديدة، تتداخل فيها القوة بالتعاطف، والمعرفة بالفعل:

- **تحمين الحقوق وتُطالبين بها:** تسعين لضمان أن يتمتع كل فرد – نساءً، رجالًا، أطفالًا – بكامل حقوقهم، في كل مكان، وخصوصًا أولئك المهمّشين أو المُستبعدين.
- **توثقين وتُظهِرين الحقيقة:** قد تجمعين شهادات، أو توثقين حالة، أو تكتبين تقريرًا، أو تنشرين عبر منصاتك ما لا يراه الآخرون. فأنتِ جسر بين الضحايا والعدالة.
- **تقفين مع الضحايا لا بجانبهم فقط:** توفّرين لهم الدعم، تُخفّفين عنهم،

تُساعدينهم في الوصول إلى العدالة، سواء عبر الدعم القانوني، أو النفسي، أو الاجتماعي، أو حتى بمجرد الاستماع الصادق لهم.

- **تعملين في كل المساحات:** من الحيّ الصغير، إلى ساحات التظاهر، إلى غرف الاجتماعات، إلى الحملات على الإنترنت. نشاطكِ قد يكون محلّيًا أو وطنيًا أو حتى دوليًا – كل هذا جزء من نضالكِ.
- **تحاولين وقف الانتهاكات، أو على الأقل الحد منها:** سواء بإطلاق نداء عاجل، أو توثيق حادثة، أو الضغط على الجهات المعنية، أو نشر قصة ضحية، فأنتِ تحاولين أن تكوني «سورًا» يحول دون استمرار الظلم.
- **تنشرين الوعي:** في المدارس، المجتمعات، على الإنترنت، أو حتى في جلسة بسيطة بين صديقاتك. ثقافة حقوق الإنسان لا تنتشر وحدها، بل عبركِ أنتِ ومن يشبهكِ.
- **تدافعين عن حق الناس في أن يعيشوا بكرامة:** وهذا يشمل دعم الحكم الرشيد، المشاركة في رسم السياسات، والدعوة لحكومة تُصغي وتستجيب.
- **تساعدين في شفاء ما يمكن شفاؤه:** عبر مبادرات للدعم النفسي، أو برامج قانونية، أو مبادرات مجتمعية تُداوي أثر الانتهاك وتعيد للضحايا الأمل.

"أن تكوني مرئية على الإنترنت كامرأة تطالب بالعدالة، يعني أنكِ تحتاجين إلى شجاعة مضاعفة. نحن لا نطالب بحقوقنا فقط، بل نحمي وجودنا أيضاً."

مدافعة من ذي قار خلال ورشة عمل حول الحماية الرقمية

ت. ما هي معايير عمل المدافعات عن حقوق الانسان؟

كونكِ مدافعة عن حقوق الإنسان لا يتعلّق فقط بما تفعلينه، بل بالطريقة التي تمضين بها في هذا الطريق، وبالقيم التي تختارين الالتزام بها، حتى في أصعب الظروف. هناك مبادئ أساسية توجّه عمل المدافعات في كل مكان، وهي ليست قوانين جامدة، بل بوصلة أخلاقية ومهنية تبقيكِ على الطريق

الصحيح، مهما كانت التحديات.

فأنتِ لا تحتاجين إلى لقب أو صفة رسمية لتكوني مدافعة عن حقوق الإنسان. يكفي أنكِ اخترتِ أن لا تقفي صامتة أمام الانتهاكات.

لكنكِ، وأنت تمضين في هذا الطريق، ستمرّين بمحطات صعبة، وتواجهين مواقف تتطلب منكِ وضوحًا وثباتًا.

"أنا لا أُغيّر العالم، لكنني أُغير شيئًا في حياة أحدهم، وهذا يكفيني كي أستمر."
مشاركة في المقابلات التي أجريت اثناء اعداد هذا الدليل

هذه بعض القيم والمبادئ التي تُبقيكِ على الطريق، وتذكّركِ دوماً لماذا بدأْتِ:

- **كل الحقوق... لكل الناس**

ما تدافعين عنه ليس امتيازاً لفئة دون أخرى، بل هو حق لكل إنسان: امرأة كانت أم رجلًا، طفلًا أو مسنًّا، من وسط المدينة أو من أقصى القرى. لا تقبلي أن يُختزل الحق أو يُجزأ.

- **لا تبرير للظلم مهما كان شكله**

أحيانًا قد تسمعين من يقول: «هي تستحق ما حصل»، أو «الظرف لا يسمح بالحريات». لكنكِ تعرفين أن أي تبرير للانتهاك، مهما بدا مقنعًا، هو خطوة نحو التطبيع مع الظلم.

- **قول الحقيقة، حتى لو بصوت منخفض**

لا تحتاجين إلى منصة كبيرة لتكوني صادقة. النزاهة لا تُقاس بالصوت العالي، بل بالنية الواضحة، والصدق في التفاصيل، والثقة التي تزرعينها في من حولك.

- **السلمية ليست ضعفًا**

حين تختارين طريق السلم، فأنتِ تختارين أن تُقاومي دون أن تؤذي، أن تُواجهي

بالقـوة الأخلاقيـة لا بالقـوة الجسـدية. هـذا قـرار شـجاع، لا يتخـذه إلا مـن يملكـن الشـجاعة الحقيقيـة.

والدفـاع عـن الحقـوق لا يعنـي حمـل العنـف، بـل يعنـي الإصرار عـلى التغيـير دون إلحـاق الـضرر. السـلمية ليسـت ضعفًـا، بـل قـوة أخلاقيـة تعطيـكِ شرعيـة في نضالـك.

- **التواضع في الفعل، والاحترام في الاختلاف**

أن تكـوني مدافعـة لا يعنـي أنـكِ تعـرفين كل شيء. بل يعنـي أن تسـتمعي، تتعلمي، وتبقـي المسـاحة مفتوحـة أمـام تجـارب الآخريـن وآرائهـم، حتـى عندمـا تختلف.

- **مدّ الجسور مع النساء الأخريات**

أنـتِ لسـتِ وحـدكِ. هنـاك أخريـات، ربمـا لم تُتـح لهـن الفرصـة للحديـث، أو خنـق الخـوف أصواتهـن. وجـودكِ لا يعنـي أن تتحـدثي بـدلاً منهـن، بـل أن تفتحـي الطريـق لهـن، وتكـوني إلى جانبهـن لا فوقهـن.

ليس من الضروري أن تكوني مثالية، ولكن من الضروري أن تبقي وفيّة لقيمك. فالمسؤولية الأخلاقية التي تحملينها لا تحتاج إلى صخب، بل إلى ثبات في الموقف، ووضوح في النية.

ث. أهمية الحماية الرقمية للمدافعات ودورها في تعزيز حرية التعبير والعمل الحقوقي

أنـتِ لا تعمـلين فقـط في الشـارع أو في المجتمـع، بـل أصبـح جـزء كـبير مـن عملـكِ مرتبطًـا بالعـالم الرقمـي: مـن توثيـق الانتهـاكات، إلى التوعيـة، وحتـى التواصـل مـع الضحايـا أو الجهـات الداعمـة.

لكـن هـذا الفضـاء، الـذي منحنـا أدوات جديـدة للتـأثير، أصبـح أيضًـا سـاحة جديـدة للتهديـدات.

- **الحماية الرقمية ليست رفاهية... بل ضرورة.**

كل رسالة، كل صورة، كل كلمة تكتبينها قد تُستخدم ضدكِ إذا لم تكنِ مستعدة. وهذا لا يعني أن تتراجعي، بل أن تتحصني. الحماية الرقمية لا تقل أهمية عن أي آلية لحمايتك في الشارع أو بيتك. هي درعكِ الخفي الذي يرافقكِ في كل لحظة عمل.

- **الحماية الرقمية تعني أنكِ تواصلين النضال... بأمان**

حين تكونين واثقة بأن بياناتكِ في مأمن، أنكِ تعرفين كيف تتعاملين مع الروابط المشبوهة، أو كيف تُؤمّنين حساباتكِ، يمكنكِ أن تركّزي على الأهم: رسالتك، صوتكِ، عملكِ. لأن الخوف من الاختراق أو الفضح أو التشهير يُربك العمل، ويكسر الإحساس بالأمان، وهو ما يُحاول الخصوم تحقيقه.

- **حرية التعبير تبدأ من الشعور بالأمان**

لا يمكن الحديث عن حرية التعبير بينما المدافعات يتعرضن للملاحقة بسبب منشور، أو للابتزاز بسبب صورة، أو للصمت بسبب رسائل تهديد.

الحماية الرقمية هنا تُصبح فعل مقاومة، حين تعرفين كيف تحمين نفسكِ، فأنتِ تُحمين صوتكِ، وتحمين الحق في التعبير، ليس فقط لكِ، بل لكل من تمثلينهن.

"أن تعرفي كيف تحمين نفسك رقمياً... هو أن تُقرري كيف تُواصلين الطريق بأمان، دون أن تدفعي الثمن من حريتكِ أو كرامتكِ."

ج. التحديات الرقمية الأساسية:

نعلم أن الطريق الذي تسلكينه كمدافعة عن حقوق الإنسان في العراق ليس سهلًا، وأن البيئة الرقمية، رغم كونها مساحة للعمل والنضال والتعبير، قد تحولت في كثير من الأحيان إلى ساحة خطر حقيقية. فبينما تفتح التكنولوجيا أبوابًا جديدة للتواصل والتضامن وتوثيق الانتهاكات، فإنها في الوقت نفسه تكشفكِ – دون حماية كافية – أمام أنظمة مراقبة متقدمة، وخطابات كراهية منظمة، وهجمات تستهدفكِ كامرأة أولًا، وكمدافعة ثانيًا.

هذه التحديات لا تأتي جميعها دفعة واحدة، لكنها تتسلل إلى حياتك الرقمية في أشكال متعددة، تبدأ برسالة غريبة، أو رابط مشبوه، أو تعليقات جارحة، وقد تصل إلى تهديدات مباشرة، وتشويه سمعة، واختراق حساباتكِ أو حتى هندسة علاقتكِ مع محيطكِ.

ولأننا ندرك أن هذه الانتهاكات ليست مجرد تجارب مؤلمة بل أدوات ممنهجة لإسكات صوتكِ وكسر إرادتكِ، سنبدأ الآن بتفكيك أبرز هذه التحديات... واحدة تلو الأخرى، بدءًا من التهديدات الرقمية الموجهة إليكِ كامرأة تناضل في فضاء مزدوج التمييز: فضاء الإنترنت، وواقع العراق الاجتماعي والسياسي.

"التهديد ما يجي دائمًا بشكل مباشر. أحيانًا يكفي تلميح بسيط عن مكان سكني أو اسم أختي على العام، حتى أحس إنهم يراقبوني بكل حركة."

مدافعة عن حقوق الإنسان

- **التهديدات الرقمية الموجهة ضد المدافعات**

في كثير من الأحيان، تبدأ الحكاية برسالة خاصة غير متوقعة، أو إشعار باختراق محاولة دخول إلى حسابكِ، أو إشاعة تم تداولها عنكِ في واحدة

مـن مجموعـات وسـائل التواصـل. هـذه ليسـت مجـرد مواقـف عابـرة – بـل نمـط ممنهـج مـن التهديـدات الرقميـة التـي تواجههـا المدافعـات في العـراق بشـكل متزايـد.

التهديـدات قـد تكـون علنيـة، مثـل تعليقـات مبـاشرة تتوعـدكِ بـالأذى، أو رسـائل تخويـف تصـل إلى بريـدكِ الشـخصي أو هاتفكِ، وقـد تكـون مبطّنة: مثل اسـتخدام كلمات تحريضيـة بحقـكِ، أو تسريـب معلومـات خاصـة بغرض التشـهير.

في إحـدى المقـابلات التـي أُجريـت ضمـن إعـداد هـذا الدليـل، قالـت إحـدى المدافعـات مـن نينـوى:

أحـد التحديـات الأعمـق أن هـذه التهديـدات تؤثـر على شـعور المدافعـة بالأمـان النـفسي، وتخلـق بيئـة قلـق دائـم. لكـن في المقابـل، أظهـرت عـدة مدافعـات مـن اللاتي شـاركن في برامـج تدريبيـة ومبـادرات للحمايـة الرقميـة، أن مجـرد تعلـم إجـراءات بسـيطة – مثـل تفعيـل المصادقـة الثنائيـة، واسـتخدام تطبيقـات مراسـلة مشـفّرة، وتصفيـة إعـدادات الخصوصيـة – أحـدث فارقًـا كـبيرًا.

هـذا لا يعنـي أن التهديـدات سـتختفي تمامًـا، لكنهـا سـتجدكِ أكثر اسـتعدادًا لهـا، وأكثر قـدرة على مواجهتهـا بثقـة ووعـي، وهـو مـا يخفّـف مـن أثرهـا النـفسي، ويمنحـكِ بيئـة رقميـة أكثر اسـتقرارًا واسـتقلالًا.

"كنت أتكلم مع صديقة عن قضيّة حساسة، وبعدها بيوم وصلتني رسالة بيها تفاصيل ما اتكلمت عنه بالضبط، لكن من رقم غريب. صرت ما أعرف بمنو أثق!"

ناشطة ميدانية

* المراقبة والرصد الرقمي: العيون التي لا تنام:

قـد لا تكونـين وحـدكِ حـين تسـتخدمين هاتفـك أو تفتحـين بريـدك الإلكـتروني. في بعـض اللحظـات، قـد تشـعرين بـأن هنـاك مـن يتتبـع خطواتـكِ الرقميـة، يقـرأ كلماتـكِ، أو حتـى يراقـب مـن تتواصلـين معهـم. هـذا الشـعور ليـس دائمًـا وهـمًا، بـل هـو واقـع تعيشـه كثـير مـن المدافعـات في العـراق اليـوم، بسـبب تنامـي

المراقبة الرقمية من جهات متعددة – سواء كانت رسمية أو غير معروفة.

تشمل المراقبة الرقمية تتبّع موقعكِ الجغرافي، رصد منشوراتكِ، تحليل محتوى رسائلكِ، أو حتى اعتراض مكالماتكِ. وقد تكون الأدوات المستخدمة معقدة أو بدائية، لكنها في النهاية تؤدي إلى النتيجة نفسها: انتهاك خصوصيتكِ وتقويض ثقتكِ بمساحتكِ الرقمية.

قالت إحدى المدافعات من البصرة، ممن عملن في توثيق قضايا العنف المجتمعي:

الأثر النفسي للمراقبة لا يقل خطورة عن التهديد المباشر؛ إذ تشعر المدافعة بأنها مكشوفة، مراقبة، وربما مهددة في أي لحظة. كما أن وجود احتمالية المراقبة يجعل بعض المدافعات يتراجعن عن العمل أو يخشين التواصل مع الضحايا أو الصحفيات أو المحاميات، خشية تسريب معلومات حساسة.

لكن رغم ذلك، أظهرت التجربة أن تبني ممارسات الحماية الرقمية يمكنه أن يغيّر قواعد اللعبة. من خلال خطوات مثل استخدام تطبيقات تواصل مشفّرة (مثل Signal)، وتحديث الأجهزة باستمرار، وتجنّب مشاركة المعلومات الحساسة عبر قنوات غير آمنة، بدأت كثير من المدافعات باستعادة السيطرة على خصوصيتهن الرقمية.

"بعد ما بديت أستخدم أدوات تشفير، وأقفل حساباتي، حسّيت بنوع من الراحة. صار عندي إحساس إني مو مكشوفة مثل قبل."

مشاركة في ورشة تدريبية حول الحماية الرقمية، أربيل، ٢٠٢٤

* الهجمات الإلكترونية: الأبواب المفتوحة في جدرانك الالكترونية:

حين تفتحين جهازكِ في الصباح، قد لا يخطر في بالكِ أن هناك من دخل إلى ملفاتكِ، أو قرأ محادثاتكِ، أو نسخ صورًا خاصة بكِ دون علمكِ. هذا ما يحدث يوميًا لكثير من المدافعات عن حقوق الإنسان في العراق، بفعل هجمات إلكترونية تستهدف الأجهزة والحسابات، وتستخدم فيها تقنيات مختلفة – من رسائل احتيالية تبدو عادية، إلى روابط مزيفة، أو تطبيقات

خبيثـة تـزرع برمجيـات تجسـس بصمـت داخـل هاتفـكِ.

الهـجمات الإلكترونيـة قـد تأخـذ عـدة أشـكال، منهـا: الاختراق المبـاشر لحسـابات البريد أو فيسـبوك أو واتسـاب، زرع برامج خبيثة (Malware) للتجسـس على الكاميرا أو الصـوت أو حتى لوحـة المفاتيـح، القرصنـة باسـتخدام أدوات مخصصة تسـتغل ضعـف الحمايـة أو الثغـرات الأمنيـة في البرامـج.

بعـض هـذه الهـجمات تـأتي مـن جهـات مجهولـة، وبعضهـا يكـون مـن أطـراف لهـا أهـداف سياسـية أو اجتماعيـة واضحـة لإسـكات صوتـكِ أو تشـويهكِ. وقـد يصـل الأمـر إلى فقـدان السـيطرة الكاملـة على جهـازك، أو تسريـب معلومـات ضحايـا قمـتِ بتوثيـق حالاتهـن.

"كل ملف كنت أجهزه عن الانتهاكات اختفى فجأة. وبعد أيام، نُشرت معلوماته من حساب مزور فيه أكاذيب وتشويه، وكأنه أنا اللي كتبتها."

صحفية مستقلة، ٢٠٢٤

* القمع الرقمي: حين يُراقبكِ الصمت... وتُهاجمكِ الخوارزميات

أن تعـبّري عـن رأيـكِ، أن تنـشري حقيقـة، أو أن ترفعـي صوتـكِ دفاعًـا عـن ضحيـة... هـذه حقـوق أساسـية، لكـن في الفضـاء الرقمـي، قـد تُواجَـه هـذه الأفعـال بمحـاولات صامتـة لإسـكاتكِ. يُطلـق عـلى ذلـك القمـع الرقمـي – وهـو اسـتخدام الأدوات التقنيـة، والمنصـات الاجتماعيـة، وحتـى القوانـين، لتقييـد حريتـكِ في التعبـير وتقليـل وصـول صوتـكِ.

تقول إحدى المدافعات من إقليم كوردستان:

تتجسد مظاهر القمع الرقمي في العراق بعدة طرق:

- حـذف أو تقييـد المحتوى مـن قبل منصـات التواصـل، خاصة عند اسـتخدام كلـمات أو وسـوم مرتبطة بحقوق الإنسـان أو قضايا حساسـة.
- الإبـلاغ الجماعـي والمنسـق عـلى الحسـابات الحقوقيـة لإغلاقهـا أو تقليـل انتشـارها.

- استخدام قوانين فضفاضة مثل «النشر المسيء» أو «الإساءة لمؤسسات الدولة» لتجريم التغريدات أو المنشورات الحقوقية.
- الضغط من المحيط الاجتماعي لتجنب الخوض في موضوعات «لا يجوز الحديث عنها»، بحجة السمعة أو التقاليد.

"تعلمت كيف أقفل كل باب رقمي عندي، وصرت أحس بثقة أكبر وأنا أشتغل، خصوصًا لما أعرف إني عاملة نسخ احتياطي مشفر لكل شيء مهم."

ناشطة من بغداد، ٢٠٢٤

كل هذا يخلق بيئة رقمية خالية من الأمان التعبيري، وتجعل الكثير من المدافعات يعانين من الرقابة الذاتية، حيث يبدأن بحذف منشورات أو الامتناع عن الكتابة خوفًا من التبعات.

لكن هناك جانب آخر مشرق:

المدافعات اللواتي تعلمن كيفية صياغة المحتوى بذكاء قانوني وحقوقي، أو أنشأن شبكات تضامن رقمية، استطعن التفاعل مع جمهور أوسع دون أن يتعرضن للحظر أو الرقابة المباشرة.

تعلمّ بعضهن كيف يستخدمن أدوات التشفير وVPN لحماية مصادرهن، أو كيف يُنشئن منصات بديلة مستقلة توصل صوتهن دون رقابة.

في النهاية، القمع الرقمي هو محاولة لإطفاء النور، لكن الإدراك بالأدوات القانونية، والمعرفة بأساليب النشر الآمن، والدعم المتبادل بين المدافعات، كلها مفاتيح لإبقاء هذا النور مشتعلاً في كل ركن من أركان العالم الرقمي.

في البيئة الرقمية، كل باب غير محمي هو دعوة مفتوحة للمخترقين. حماية هذه الأبواب تبدأ بخطوات بسيطة لكنها فعّالة، وقد تُحدث فرقًا كبيرًا في سلامتكِ وسلامة من تعملين معهم.

- **ثانيا: الحقوق الرقمية**

أ- مفهوم الحقوق الرقمية وأهميتها.

ما هي الحقوق الرقمية؟ ولماذا تهمكِ كمدافعة عن حقوق الإنسان؟

الحقوق الرقمية هي ببساطة حقوق الإنسان نفسها... ولكن في العالم الرقمي.

فكما لكِ الحق في حرية التعبير في الشارع، لكِ أيضًا هذا الحق وأنتِ تكتبين منشورًا أو تشاركين رأيًا على الإنترنت.

وكما أن لكِ الحق في الخصوصية في بيتك، فلَكِ الحق في الحفاظ على خصوصيتكِ في هاتفك، وبريدك الإلكتروني، ومساحاتك الرقمية.

"نشرتُ تقريرًا عن اعتقال تعسفي، فتم حظر صفحتي فجأة، وكأنني اختفيت من الإنترنت. لا أحد رآني، ولا سمع صوتي بعدها."

ناشطة في حقوق العمل، ٢٠٢٤

الحقوق الرقمية تشمل:

١. الحق في الوصول إلى الإنترنت والمعلومات:

لكِ الحق في أن تكوني «مُتصلة» بالعالم — أن تستخدمي الإنترنت متى احتجتِ، دون عوائق أو رقابة مجتمعية أو سياسية. هذا يشمل وصولكِ للمواقع، المنصات، والمصادر التي تساعدكِ في عملكِ الحقوقي، أو في تطوير مهاراتكِ. في العراق، كثير من النساء في بعض المناطق لا يمتلكن إنترنت منتظم أو حواسيب شخصية، وبعضهن يُمنعن من استخدامه بسبب الأعراف.

٢. الحق في حرية الرأي والتعبير والتجمع السلمي على المنصات الرقمية:

لكِ الحق أن تعبّري عن رأيك، تدافعي عن قضية، ترفضي ظلمًا، أو تسألي سؤالًا على فيسبوك، إنستغرام، تويتر، أو أي منصة... دون أن تُهددي، أو تُخوّني، أو تُهاجمي. فالرقابة على آرائك الرقمية، سواء من جهات رسمية أو من أفراد، تمثل انتهاكًا واضحًا لحقك في التعبير.

٣- الحق في الخصوصية الرقمية وحماية بياناتكِ الشخصية:

لـكِ الحـق أن تكـوني وحـدكِ مـن تقررين مـا الـذي تريدينـه أن يُعـرف عنـكِ، ومـن يمكنـه الوصـول إليـه.

صـوركِ، رسـائلكِ، ملفاتـكِ، مكانـكِ الجغـرافي، كلهـا بيانـات خاصـة. ولا يحـق لأي جهـة، مـهما كانـت، أن تراقبـكِ أو تـخترق حسـاباتكِ أو تسرق معلوماتـكِ دون إذنكِ.

٤- الحق في الحماية من العنف الرقمي والتمييز:

التحـرش، التهديـد، الشـتم، التنمـر، أو الإقصـاء مـن النقاشـات الرقميـة بسـبب كونـكِ امـرأة أو مدافعـة... كلهـا أشـكال مـن العنف الرقمي. كذلـك فـإن التهديدات المبنيـة على الشرف أو السـمعة أو الديـن أو الخلفيـة الاجتماعيـة، تعـتبر تمييـزاً رقميًـا خـطيراً. وهـذا الحـق يعني أن لـكِ مساحة آمنـة على الإنترنـت، دون خـوف أو إسـكات.

"ما عاد صوتنا ضعيف، بس صار أذكى. نختار كلماتنا بعناية، ونبني دعمًا متبادلًا، ونتواجد بطرق تعجز الخوارزميات عن حجبها."

مشاركة في ورشة تدريب رقمي، ٢٠٢٤

لماذا هذه الحقوق مهمة لكِ؟

- لأنـكِ كمدافعـة تعملـين في بيئـة رقميـة محفوفـة بالمخاطـر. وقد تُسـتخدم التكنولوجيـا ضـدكِ، بـدلاً مـن أن تخدمـكِ، إذا لم يتـم الاعـتراف بحقوقـكِ الرقميـة أو حمايتهـا.
- مـع الأسـف، مـا زالـت الكثـير مـن القوانـين في العـراق لا تعـترف صراحـة بهـذه الحقـوق، أو لا توفـر لهـا الحمايـة الكافيـة، خاصـة عندمـا تكـون الانتهـاكات موجهـة ضـد النسـاء.
- ومـن هنـا تـأتي أهميـة أن تكـوني عـلى درايـة بهـذه الحقـوق، وأن تطالبـي بهـا، وتحميهـا بنفسـكِ، إلى أن تتوفـر بيئـة قانونيـة ومجتمعيـة تُنصفـكِ وتُوفـر لـكِ الحمايـة الفعليـة.

ب. صلة الحقوق الرقمية بحرية التعبير وحرية التنظيم والعمل الحقوقي

حين تتصلين بالإنترنت، وتشاركين رأيًا، أو توثقين انتهاكًا، أو تنظمين لقاءً، أو تتواصلين مع زميلة، فأنتِ تمارسين أحد أهم حقوقكِ: حرية التعبير وحرية التنظيم.

هذه الحريات لا تتوقف عند حدود المكان أو الزمان، بل تمتد اليوم إلى الفضاء الرقمي، حيث أصبح العمل الحقوقي أكثر اعتمادًا على التكنولوجيا، وأصبح الإنترنت ساحة نضال حقيقية.

الدستور العراقي في المادة (٣٨) يكفل حرية التعبير عن الرأي بكل الوسائل، وحرية الاجتماع، والتنظيم، وتكوين الجمعيات. هذه الحقوق تمتد لتشمل الوسائل الرقمية الحديثة، باعتبارها منابر للتعبير والتنظيم، لا تقل أهمية عن الساحات العامة.

أما على الصعيد الدولي، فقد صادق العراق على العهد الدولي الخاص بالحقوق المدنية والسياسية، الذي ينص في المادة (١٩) على الحق في حرية الرأي والتعبير، ويؤكد على أن هذا يشمل «حرية التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى آخرين، دونما اعتبار للحدود، سواء على شكل مكتوب أو مطبوع، أو في قالب فني، أو بأية وسيلة أخرى يختارها» — ما يشمل الوسائل الرقمية بشكل مباشر.

كما أن العراق طرف في اتفاقية القضاء على جميع أشكال التمييز ضد المرأة (سيداو)، التي تفرض على الدولة اتخاذ جميع التدابير المناسبة لتمكين النساء من المشاركة في الحياة العامة والسياسية، بما يشمل الوصول إلى المعلومات ووسائل التعبير والتواصل، وهي حقوق ترتبط اليوم بشكل وثيق باستخدام الإنترنت ووسائل الاتصال الحديثة.

خصوصيتكِ... ليست قابلة للتفاوض.

في العـراق، تواجـه المدافعـات عـن حقـوق الإنسـان تحديـات مضاعفـة: مـن جهـة، يطالـبن بمسـاحة للتعبـير والمنـاصرة، ومـن جهـة أخـرى، يُهاجمـن عنـد اسـتخدامهن لتلـك المسـاحة. ولذلـك فـإن حمايـة الحقـوق الرقميـة تعنـي حمايـة المسـاحة التـي تُمكنـكِ مـن:

الحديث علنًا عن قضايا النساء والعدالة والمساواة.

التنظيم الرقمي للورش، الحملات، أو الفعاليات الحقوقية.

التواصل الآمن مع الشبكات المحلية والدولية.

تبادل الملفات والمعلومات دون خوف من الاختراق أو التجسس.

حين يتـم التضييـق على حقوقـكِ الرقميـة، فـإن حريتـكِ في التعـبير والعمـل تتعـرض للاختنـاق، حتـى وإن لم يُغلـق بـاب مكتبـك أو يُمنـع صوتـك في الشـارع.

ت. نظرة على الإطار القانوني (العراقي والدولي) المتعلق بالحقوق الرقمية للنساء

قـد تبـدو القـوانين بعيـدة أو معقـدة أحيانًـا، لكـن مـن المهـم أن تعـرفي أن هنـاك نصوصًـا قانونيـة – سـواء في العـراق أو على مسـتوى العـالم – تـعترف بحقوقـكِ في اسـتخدام التكنولوجيـا والتعـبير عبر الإنترنـت بأمـان وحريـة.

الفضاء الرقمي لكِ أيضًا... لا تدعي أحدًا يطردكِ منه بصمته أو بخوفه.

على المستوى الوطني (العراقي):

- **الدستور العراقي** في المـادة (٣٨) يضمـن لـكِ حريـة التعبـير والتواصـل والمشـاركة، وهـذه تشـمل مـا تقومـين بـه في الإنترنـت ووسـائل التواصـل الاجتماعـي.

لكـن في الواقـع، لا يوجـد **قانون خاص يحمي حقوق النساء في الفضاء الرقمي** حتـى الآن. مـا زالـت **مسودة قانون جرائم المعلوماتية** معلقـة في البرلمـان منـذ ٢٠١١، ورغـم أنهـا تتحـدث عـن الجرائـم الرقميـة، فـإن فيهـا مـواد قـد تُسـتخدم لتقييـد حريـة التعبـير بـدل حمايتهـا، وقـد أبـدت منظـمات حقـوق الإنسـان اعتراضاتها عـلى ذلـك.

- القوانـين الحاليـة، مثـل **قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩**، تتعامـل مـع بعـض الجرائـم مثـل التشـهير أو التهديـد، لكنهـا لا تقـدم حمايـة كافيـة للنسـاء مـن الابتـزاز أو العنـف الإلكـتروني، ولا توضـح بوضوح كيـف يمكـن تقديـم شـكوى أو حمايـة الضحيـة، خاصـة إذا كانـت امـرأة.

على المستوى الدولي:

> في العالم الرقمي، الدفاع عن حقوقكِ يبدأ من معرفتكِ بها."

- **العهد الدولي الخاص بالحقوق المدنية والسياسية** (الـذي انضـم عليـه العـراق) يؤكـد حقـكِ في حريـة التعبـير، والحصـول عـلى المعلومـات، والاتصـال بحريـة دون رقابـة – ويشـمل هـذا كل مـا تقومـين بـه عـبر الإنترنـت.
- **اتفاقية سيداو** (التـي انضـم اليهـا عليهـا العـراق أيضًـا) تلـزم الدولـة بحمايـة النسـاء مـن كل أشـكال التمييـز، بمـا في ذلـك التمييـز والانتهـاكات التـي تحصـل في الفضـاء الرقمـي.
- يمكـن للمدافعـات التوجـه إلى آليـات الحمايـة الدوليـة، مثـل **لجنة سيداو** أو **المقررة الخاصة المعنية بحالة المدافعين عن حقوق الإنسان**، لتقديـم الشـكاوى في حـال لم يحصلـن عـلى الحمايـة محليًـا – لكـن هـذا المسـار يحتـاج دعـم قانـوني وخـبرة.

> إن حمايتكِ في الفضاء الرقمي، هي جزء من حمايتكِ في الحياة العامة، وهي حق يكفله الدستور، وتضمنه المواثيق الدولية التي التزم بها العراق.

الحقيقـة أن الفجـوة بين النـص القانـوني والواقـع مـا زالـت كـبيرة، لكـن معرفتـكِ بحقوقـكِ هـو أول خطـوة لحمايـة نفسـكِ، والمطالبـة بالتغـيير.

الإطار الدولي	الإطار الوطني (العراقي)	المحور
العهد الدولي الخاص بالحقوق المدنية والسياسية.	الدستور العراقي (مادة ٣٨) يضمن حرية التعبير بشكل عام.	الأساس القانوني
يعترف بالحق في التعبير والوصول إلى المعلومات عبر الإنترنت.	لا يوجد قانون واضح أو مفعّل يضمن الحقوق الرقمية للنساء.	حماية الحقوق الرقمية
يلتزم بحماية النساء من التمييز والانتهاكات، بما في ذلك في الفضاء الرقمي.	معالجة محدودة عبر قانون العقوبات رقم ١١١ لسنة ١٩٦٩ (مثل التشهير أو التهديد).	الجرائم الرقمية
اتفاقية «سيداو» تنص على حماية النساء من كافة أشكال العنف والتمييز، بما فيها الرقمية.	هناك مسودة قانون لجرائم المعلوماتية منذ عام ٢٠١١، لكنها غير مُشرعة حتى الآن.	قانون خاص بالإنترنت؟
توجد آليات دولية (مثل لجنة سيداو) لكن الوصول إليها يتطلب دعمًا قانونيًا متخصصًا.	لا توجد آليات فعالة وسهلة للتبليغ أو الحماية، خاصة في حالات العنف أو الابتزاز الرقمي.	الإبلاغ والحماية
تركـز الاتفاقيـات الدوليـة على تجريـم اللـوم المجتمعـي ودعم الضحايـا بالكامـل.	نظـرة مجتمعية سـلبية غالبًـا نحو الضحيـة، خاصـة في قضايا تمس السمعة أو الشرف.	الاستجابة المجتمعية

4.
الحماية الرقمية: نحو بيئة آمنة في حياة المدافعات عن حقوق الانسان

القسم الأول: أدوات وتقنيات الحماية الرقمية

١. مقدمة: أساسيات الحماية الرقمية العامة: سلوك يومي يحميكِ... لا مجرد مهارة تقنية

في عالم متصل طوال الوقت، لم تعد الحماية الرقمية رفاهية، بل ضرورة لا غنى عنها. الأمر لا يتعلق فقط بامتلاك التطبيقات الصحيحة أو تفعيل خيارات الأمان، بل يتعلق بكيفية تفكيركِ، تصرفكِ، وتفاعلكِ مع الأدوات الرقمية من حولكِ.

الحماية الرقمية هي ثقافة شخصية وسلوك جماعي، تتطلب من كل مدافعة أن تتعامل مع الهاتف، البريد الإلكتروني، كلمات المرور، والتطبيقات كجزء من مساحة خاصة لا يجب فتحها على مصراعيها للغرباء أو حتى المقرّبين، ما لم تكن الثقة محصّنة بالوعي.

"الأمان الرقمي يبدأ من قراراتي الصغيرة اليومية، لا من التكنولوجيا وحدها."
مدافعة من السليمانية

كما أنها مسؤولية جماعية. فسلامتكِ الرقمية لا تنفصل عن سلامة زميلتكِ المدافعة، أو إحدى الضحايا التي تسجلين حالتها. كل خطوة واعية منكِ تُبقي الدائرة آمنة، وكل إهمال بسيط قد يفتح الباب لانتهاك يتجاوزكِ شخصيًا.

هذه ليست خطوات تقنية فقط، بل عادات صغيرة وبسيطة تحمي حياتكِ وعملك وسلوكياتك اليومية.

ربما تتساءلين، وأنتِ تقرئين هذا القسم، عن كيفية التوفيق بين العمل اليومي المليء بالضغوط، والتزاماتك في توثيق الانتهاكات، والتواصل مع الضحايا، والمشاركة في الحملات والأنشطة الحقوقية، وبين متطلبات الحماية الرقمية التي قد تبدو في بعض الأحيان معقدة أو مرهقة.

من الطبيعي أن لا تكوني متخصصة في الأمن الرقمي، فهذا الدليل لم يُكتب بلغة تقنية ولا يفترض خلفية رقمية سابقة، بل يضعكِ أنتِ، المدافعة عن حقوق الإنسان، في قلب اهتمامه.

في الواقع، الحماية الرقمية ليست مجموعة من البرامج والتطبيقات فقط، بل هي سلوك يومي، وعادات بسيطة، وقرارات صغيرة لكنها مهمة تتخذينها باستمرار، لحماية نفسكِ ومن معكِ من شبكات الدعم والضحايا والزميلات.

حين تكونين هدفًا، فإن كل تفاعل رقمي تقومين به – رسالة، صورة، ملف، أو حتى «لايك» – يمكن أن يُستغل ضدكِ. لذلك، فإن بناء روتين حماية رقمية لا يعني فقط تفادي الاختراق أو التصيد، بل أيضًا تعزيز رفاهكِ النفسي والثقة بنفسك في الفضاء الرقمي، ومواصلة عملكِ بشجاعة ووعي.

"أصبحت أبدأ صباحي كما أراجع بريدي، أراجع إعدادات الخصوصية. كما أتحقق من قفل باب منزلي، أتحقق من من جهازي."

مشاركة في ورشة حماية رقمية للمدافعات، أبريل ٢٠٢٤

لماذا يجب أن تتحول الحماية الرقمية إلى روتين يومي؟

قد يبدو مصطلح «بيئة امنة يومية للحماية الرقمية» مبالغًا فيه، لكن

الحقيقة أن القواعد البسيطة التي نكررها كل يوم تصبح تلقائيًا خط دفاع أول. هذا الروتين لا يعني أن تكوني خبيرة أمن سيبراني، بل أن تكتسبي وعيًا عمليًا يُساعدك في اتخاذ قرارات صحيحة في لحظات سريعة، دون الحاجة إلى مراجعة دليل أو سؤال خبير.

الحماية الرقمية السليمة تبدأ من فهمكِ أن سلامتكِ الرقمية لا تخصكِ وحدك، بل تمتد إلى من تتواصلين معهن: منظمات، زميلات، ضحايا، ومجتمع محلي.

ما الذي نقترحه لكِ في هذا القسم؟

١. روتين يومي للحماية الرقمية الشخصية: خطوات بسيطة يمكن تنفيذها صباحًا أو قبل النوم، مثل مراجعة نشاط الحسابات، وتحديث كلمات المرور، أو التحقق من الأجهزة المتصلة.

٢. ممارسات أسبوعية أو عند الحاجة: مثل نسخ الملفات احتياطيًا، تحديث التطبيقات، مراجعة الصلاحيات، أو استخدام أدوات فحص الأمان.

٣. تطبيقات وأدوات ذكية تساعدكِ في المواقف التي تقل فيها قدرتكِ على التركيز أو المتابعة: فالحياة ليست دائمًا تحت السيطرة، ومن المهم أن تكون بعض أدوات الحماية تعمل لصالحكِ دون جهد كبير.

تذكير مهم:

ليس المطلوب منكِ أن تكوني مثالية في كل شيء، بل أن تتقدمي خطوة بخطوة، وتضعي أمنكِ الشخصي في مقدمة أولوياتكِ. لأنكِ حين تفعلين ذلك، فإنكِ في الحقيقة تحمين أيضًا من حولكِ، وتقودين نموذجًا جديدًا من الوعي الرقمي في سياق حقوق الإنسان.

أ. الروتين اليومي للحماية الرقمية الشخصية

خطوات بسيطة، لكنها تصنع فرقًا كبيراً في سلامتكِ الرقمية

قد لا يتطلب منكِ هذا الروتين سوى بضع دقائق يوميًا، لكنه يُشكّل خط الدفاع الأول في وجه التهديدات الرقمية، ويمنحكِ شعورًا أكبر بالسيطرة

والطمأنينة. إليكِ أبرز الخطوات التي يمكنكِ إدراجها في يومكِ مثلما تشربين قهوتكِ الصباحية أو تغلقين باب المنزل.

وربما تتساءلين:

كيف أجد الوقت والمساحة الذهنية لحماية نفسي وسط كل هذا الضغط؟

العمل الحقوقي مرهق، والتعامل مع الضحايا، والانتهاكات، والتقارير، والمجتمع، والقلق المستمر... يجعل من الصعب التركيز على حماية حساباتنا وأجهزتنا كل يوم.

لكننا هنا لا لنطلب منكِ أن تصبحي خبيرة في الأمن الرقمي.

بل لنرافقكِ — بخطوات هادئة وعملية — نحو روتين رقمي بسيط وفعّال.

تعالي نبدأ من هنا...

الروتين الأول: لنبدأ من الباب الأمامي: راجعي إعداداتكِ

كما تفعلين حينما تستيقظين من النوم، راجعي اليوم إعدادات الأمان لحساباتكِ الرئيسية.

ابدئي يومكِ بمراجعة سريعة لأهم الحسابات التي تستخدمينها (فيسبوك، واتساب، إيميلكِ الرئيسي):

- **هل تم تسجيل دخول جديد غير مألوف؟**

لمعرفة ذلك يمكنك اتباع الخطوات ادناه لكل من تطبيقات (الفيسبوك، بريد الجيميل، الواتساب)

أولًا: فيسبوك (Facebook)

- افتحي تطبيق فيسبوك أو الموقع ------> اذهبي إلى الإعدادات والخصوصية ------> الإعدادات ------> اختاري الأمان وتسجيل الدخول.
- في قسم أماكن تسجيل الدخول، سترين قائمة بكل الأجهزة التي تم

الدخـول منهـا إلى حسـابك، ومواقعهـا التقريبيـة.

- إذا لاحظـتِ جهـازًا لا تعرفينـه أو مـن موقـع غريـب ------> اضغطـي عـلى « ⋮ » (النقـاط الثـلاث) بجانـب الجهـاز ------> ثـم «تسـجيل الخـروج».

ثانيًا: جيميل (Gmail / Google Account)

- اذهبـي إلى https://myaccount.google.com/security ------> تحـت قسـم أجهزتـك (Your Devices)، سـتجدين جميـع الأجهـزة التـي دخلـت إلى حسـابك ------> اختـاري إدارة الأجهـزة (Manage Devices).

- إذا لاحظتِ جهازًا لا تعرفينه:

- اضغطـي عليـه ------> ثـم اختـاري تسـجيل الخـروج ------> راجعـي أيضًـا التنبيهـات أسـفل الصفحـة إن وُجـد تسـجيل دخـول مشـبوه.

ثالثًا: واتساب (WhatsApp)

- افتحـي تطبيـق واتسـاب عـلى هاتفـكِ ------> اضغطـي عـلى النقـاط الثـلاث في الزاويـة العليـا ------> الأجهـزة المرتبطـة (Linked Devices) ------> سـترين قائمـة بـكل الأجهـزة التـي تسـتخدم حسـابك (مثـل واتسـاب ويـب أو تطبيقـات سـطح المكتـب).

- إذا لاحظتِ جهازًا لا تعرفينه: اضغطي عليه، ثم اختاري تسجيل الخروج.

نصيحة: لا تعطـي رمـز التحقـق الـذي يصلـك لأي شـخص، حتـى لـو ادعـى أنـه مـن «واتسـاب».

تنبيه يجب الانتباه لها:

- وصـول إشـعار إلى بريـدك أو هاتفـك بعنـوان: «تـم تسـجيل دخـول جديـد إلى حسابك»

- تغيير لغة الواجهة فجأة.

- رسائل لم ترسليها، أو نشاط غير مألوف.
- استلام رموز تحقق لم تطلبيها.

"الأمان يبدأ من الوعي. كل صباح، تأكدي أن من يستخدم حساباتك هو أنتِ فقط."
مدافعة من واسط ٢٠٢٤

▪ هل توجد إشعارات غريبة أو تنبيهات أمان؟

هي رسائل تصلك من مزوّدي الخدمات (مثل فيسبوك، جوجل، واتساب...) تُنبّهك بأن شيئًا غير معتاد قد حدث. وهذه أمثلة على ذلك:

ماذا يجب أن تفعلي؟	ما الذي يعنيه؟	نوع الإشعار
افحصي الجهاز، وسجّلي الخروج فورًا منه. غيّري كلمة المرور.	قد يكون شخصًا غيرك دخل إلى الحساب.	"تم تسجيل دخول جديد إلى حسابك من جهاز غير مألوف"
استعيدي السيطرة فورًا عبر إعدادات الأمان، وقدّمي بلاغ دعم.	إذا لم تفعلي ذلك، فربما يكون حسابك مخترقًا!	"تم تغيير كلمة المرور/الإيميل الأساسي لحسابك"
فعّلي التحقق بخطوتين، وغيّري كلمة السر.	هناك من يحاول الوصول لحسابك.	"تم محاولة تسجيل الدخول، لكن كلمة السر كانت خاطئة"
تجاهلي إن كنتِ أنتِ، أو تابعي الإجراءات الأمنية إن لم تكوني.	إشارة لمحاولة اختراق.	"هناك محاولة تسجيل دخول فاشلة من موقع غير مألوف"
اذهبي لقائمة الأجهزة وقومي بتسجيل الخروج من الجهاز الغريب.	شخص ما قد يستخدم حسابك.	"تم ربط جهاز جديد أو متصفح جديد بحسابك"

أين تجدين هذه الإشعارات؟

- على بريدك الإلكتروني المرتبط بالحساب.
- في إشعارات الهاتف الخاصة بالتطبيقات (مثل إشعار واتساب أو فيسبوك).
- في صفحة الأمان الخاصة بالحساب (مثل صفحة "الأمان" في إعدادات جوجل أو فيسبوك).

ماذا تفعلين عندما تشكّين بإشعار؟

- لا تتجاهليه: حتى لو لم تكوني متأكدة.
- افتحي إعدادات الأمان لحسابك فورًا، وافحصي سجل النشاط.
- غيّري كلمة المرور فورًا إذا وجدتِ شيئًا غريبًا.
- فعّلي التحقق بخطوتين إن لم يكن مفعلًا مسبقًا. (وسيكون له تفصيل كامل في القسم الذي يليه)

لماذا هذا مهم كروتين يومي؟

لأن الكثير من محاولات الاختراق تبدأ بتنبيه بسيط، وإذا تم تجاهله، يتمكن المهاجم من الدخول والاستيلاء على الحساب أو البيانات.

كل إشعار أمان هو بمثابة جرس إنذار صغير... لا تطفئيه بصمت، بل افهمي ما يخبركِ به.

- **هل خاصية التحقق بخطوتين (Two-Factor Authentication) مفعّلة؟**

ما هي خاصية التحقق بخطوتين؟

هي خاصية تضيف خطوة أمان ثانية بعد إدخال كلمة المرور. فحتى لو كانت كلمة السر معروفة لأي شخص، لن يتمكن من الدخول إلا إذا كان يملك الوسيلة الثانية للتحقق.

ما هي الطرق الشائعة للتحقق بخطوتين؟

- رمز يُرسل إلى رقم هاتفك (SMS)
- تطبيق مصادقة مثل Google Authenticator
- مفتاح أمان فيزيائي (مثل YubiKey)
- رمز احتياطي Backup Code

كيف تتأكدي إن كانت الخاصية مفعّلة في حساباتك؟

> **"حين فعلت التحقق بخطوتين، شعرت وكأنني قمت بتركيب قفل حديدي على بابي الرقمي."**
> مدافعة من بغداد

الميزة على المنصات الأكثر شيوعًا:

أولا: الواتساب:

اذهبي إلى الإعدادات ------> الحساب ------> التحقق بخطوتين ------> تفعيل

ثانيا: الفيسبوك:

- قومي بزيارة
  https://accountscenter.facebook.com/password_and_security
- اضغطي على «المصادقة الثنائية»
- اتبعي الخطوات لتفعيل الخاصية.

ثالثا: الإنستغرام:

- قومي بزيارة
  https://accountscenter.instagram.com/password_and_security
- اضغطي على «المصادقة الثنائية»
- اتبعي الخطوات لتفعيل الخاصية.

رابعا: منصة اكس (تويتر سابقاً):

- قومي بزيارة https://x.com/settings/security
- اضغطي على «المصادقة الثنائية»
- اتبعي الخطوات لتفعيل الخاصية.

خامسا: جوجل وجيميل:

- قومي بزيارة https://accounts.google.com/security
- اضغطي على «التحقق بخطوتين»
- اتبعي الخطوات لتفعيل الخاصية.

لماذا هذه الخطوة مهمة جدًا للمدافعات؟

لأن أغلب محاولات الاختراق تبدأ بسرقة كلمة المرور، لكن التحقق بخطوتين يوقف هذا الهجوم في منتصف الطريق.

> تخيلي أن باب منزلك له مفتاح... لكنكِ تضيفين إليه قفلًا إضافيًا لا يملكه سواكِ.

نصيحة عملية:

اختاري تطبيق مصادقة (مثل Google Authenticator أو Microsoft Authenticator)، ولا تعتمدي فقط على رسائل SMS، فهي أقل أمانًا. ودوّني الأكواد الاحتياطية في مكان آمن غير متصل بالإنترنت.

نظّفي المساحة: احذفي ما لا يُطمئنكِ

تعاملي مع رسائلكِ مثل حقيبة يدكِ — أبقي فقط ما تعرفينه.

احذفي الرسائل الغريبة، والروابط غير المألوفة.

لا تضغطي، لا تردّي، لا تثقي بسرعة.

ببساطة، التحقق بخطوتين لا يحمي فقط حسابك، بل يحمي أيضًا من تراهن عليهن وتعملين من أجلهن.

الروتين الثاني: نظّفي المساحة: احذفي ما لا يُطمئنكِ

تعاملي مع رسائلكِ مثل حقيبة يدكِ — أبقي فقط ما تعرفينه.

- احذفي الرسائل الغريبة، والروابط غير المألوفة.
- لا تضغطي، لا تردّي، لا تثقي بسرعة.
- احذفي فورًا أي رسائل أو روابط لم تطلبيها، خاصة تلك التي تحتوي على عبارات غريبة أو تطلب منكِ النقر أو تحميل شيء.

الروتين الثالث: تأكدي من أن جهازكِ «معكِ»، لا ضدكِ

- هاتفكِ يجب أن يكون آمنا ويعمل لصالحكِ، لا يكون ثغرة ضدكِ.
- أعيدي تشغيله، تأكدي من قفله، ولا تتركيه بلا رقابة في الأماكن العامة.
- تأكدي أن القفل البيومتري أو كلمة المرور للهاتف مفعّلة.

الروتين الرابع: امسكي زمام الأمور: كلمات السر

- هل هذه الكلمة قوية؟ هل شاركتِها مع أحد؟
- ضعي قاعدة: عندما تشكّين، غيّري.
- خذي دقيقة واحدة يوميًا لتتذكري إن كنتِ قد شاركتِ كلمة مرورك مع أحد أو استخدمتها على جهاز غير آمن.

الروتين الخامس: كوني واعية لما تنشرينه يوميا

- فكري مرتين قبل ان تنشرين الصور، الموقع، المعلومة، وحتى التوقيت...
- تأكدي هل هذا المنشور يمكن أن يستخدم ضدكِ؟
- هل فيه ما يفتح بابًا لمن يتربص بكِ؟
- هل يمكن أن يُفهم خارج سياقه؟

"تعلمت أن أكتب وكأني سأترافع عن كل منشور في محكمة."
ناشطة من النجف

الروتين السادس: راقبي الزوار غير المرئيين

- من الذي يستخدم حساباتكِ غيركِ؟
- راجعي الأجهزة النشطة، وتخلصي من أي جهاز لا تعرفينه.
- بعض المنصات تتيح لكِ رؤية الأجهزة النشطة (مثل Gmail وFacebook). تأكدي أن الأجهزة الظاهرة هي فقط أجهزتكِ، وإن وجدتِ شيئًا غريبًا، قومي بتسجيل الخروج فورًا.

------> راجعي الروتين الاول

الروتين السابع: خفّفي الحمل عن جهازكِ

- تأكدي أن لا تتركي ملفات لا تحتاجينها.
- تأكدي ان الملفات الحساسة مكانها مؤمن.
- الصور القديمة؟ الرسائل؟ ربما حان وقت الحذف او نقلها الى أجهزة تخزين خارجية او مواقع تقدم خدمات السحابة بشكل امن ومشفر.
- لا تحتفظي بملفات حساسة مفتوحة على جهازكِ دون حاجة.
- امسحي الصور أو الملفات التي لا تستخدمينها.

الروتين الثامن: علبة الأدوات:

- لا تُكثري منها
- كلما زاد عدد التطبيقات والمنصات، زاد احتمال الثغرات.
- اسألي نفسكِ: هل أحتاج كل هذا؟
- هل يمكنني تقليل النوافذ المفتوحة على عالمي؟
- خصصي دقيقة واحدة يوميًا للتفكير: هل هناك تطبيق لا أحتاجه؟ هل يمكنني تقليل استخدامي لمنصة معينة؟

الروتين التاسع: هل هناك تحديث متوفر؟ لا تؤجليه!

"حين يُطلب منكِ تحديث تطبيق أو نظام تشغيل جهازكِ، لا ترددي. التحديثات ليست مجرد تحسين للشكل أو إضافة ميزة جديدة – بل هي في الغالب درع خفي يُغلق ثغرات يمكن أن تُستغل ضدكِ."

في كل مرة تتجاهلين فيها إشعار التحديث، تتركين بابًا مفتوحًا في جهازكِ قد تمرّ منه برامج تجسس، أو أدوات اختراق، أو برمجيات خبيثة دون أن تدري.

لذلك، اجعلي من تحديث نظام التشغيل (Windows، Android، iOS، وغيرها) وتحديث التطبيقات التي تستخدمينها بانتظام عادة أسبوعية أو كلما ورد إشعار رسمي من النظام.

- فعّلي التحديث التلقائي إن أمكن (خاصة للتطبيقات الأساسية).
- أعيدي تشغيل الجهاز بعد التحديث لتفعيل الحماية الكاملة.
- تجنبي تحميل تطبيقات من خارج المتاجر الرسمية، حتى لو بدت "مفيدة".

"التحديثات ليست عبئًا رقميًا، بل صيانة يومية لسلامتكِ الرقمية."

وأخيراً...

اجـعلي هـذا الـروتين طقسًـا شـخصيًا يُـعبرّ عـن حبـكِ لذاتـكِ واهتمامـكِ بمـن حولـكِ. ليـس عبئًـا ولا مهمـة ثقيلـة، بـل ممارسـة نابعـة مـن وعيـكِ بقيمتـكِ ودوركِ.

ضعـي فنجـان قهـوة، أو اسـتمعي لموسـيقاكِ، واجـعلي روتين الأمـان الرقمـي طقسـاً صـغيراً مـن العنايـة الذاتيـة. مثـل تسريـح الشـعر، أو ترتيـب الكتـب.

هكذا، ببساطة... تحمين نفسكِ وتحفظين صوتكِ.

"حمايتكِ الرقمية ليست رفاهية، بل مساحة للحرية — مساحة لتستمري، وتعبّري، وتكوني."
من مراجعات الدليل، الناصرية ٢٠٢٥

٢. رفيقاتك الرقميات: تطبيقات وبرامج لا غنى عنها لحمايتك الرقمية اليومية

مثـلما نختـار بعنايـة مـن نثـق بـه في حياتنـا اليوميـة، نحتـاج أيضـاً أن نختـار التطبيقـات التـي نثـق بهـا في حياتنـا الرقميـة. بعـض الأدوات لا تحمينـا فقـط، بـل تمنحنـا راحـة البـال وسـط هـذا الزحـام الإلـكتروني.

هـل تسـاءلتِ يومًـا: مـا التطبيقـات التـي يجـب أن أحتفـظ بهـا على هاتفـي أو حاسـوبي كي أكـون بأمـان؟

الحمايـة الرقميـة ليسـت رفاهيـة كما أسـلفنا ذكرهـا، وليسـت شـيئًا معقـدًا، بـل تبدأ مـن قـرارات بسـيطة — مثـل نـوع التطبيقـات التـي تسـتخدمينها كل يـوم. في هـذا القسـم، سـنزودك بمجموعـة تطبيقـات وأدوات أساسـية، صُممـت لمسـاعدتكِ على:

- تأمين الاتصالات،
- حفظ الملفات الحساسة،
- إدارة كلمات المرور،
- التحقق من التهديدات،
- وتوفير طبقة حماية إضافية لكِ ولمن حولك.

ليسـت كل التطبيقـات متشـابهة، وبعضهـا يُخفـي أكثر مما يُظهـر. لذلـك جمعنـا

لـكِ الأدوات التـي اعتمـدت عليهـا مدافعـات مـن العـراق ومـن حـول العـالم، وسنرافقـك في استكشـاف كيـف يمكـن لـكل واحـدة منهـا أن تصبـح جـزءاً مـن روتينـكِ الرقمـي الموثـوق.

خطوتك الأولى: هدوء في الاتصال، أمان في الهوية

في رحلتـكِ اليوميـة كمدافعـة عـن حقـوق الإنسـان، قـد تكـونين على تواصـل دائـم مـع ناشـطات، ضحايـا، إعلامـيين أو حتـى جهـات رسـمية. وكل هـذه الاتصـالات لا يجـب أن تكـون مكشـوفة. تـأمين طريقـة تواصلـكِ، وإخفـاء معلوماتـكِ الشـخصية أو مـا يُعـرف بـ»الهويـة الرقميـة»، ليـس فقـط لحمايتـكِ أنـتِ، بـل أيضـاً لحمايـة كل مـن يثـق بـكِ ويتعامـل معـكِ.

كيف تحققين هذه الحماية؟

> "حين أؤمن اتصالاتي، كأنني أضع حدوداً تحميني وتُشعرني أنني أتحكم بما أشاركه."
> مدافعة نسوية من الجنوب العراقي

اسـتخدمي تطبيقـات تراعـي الخصوصيـة وتوفّـر التشـفير الكامـل (مـن الطـرف إلى الطـرف). مثـل:

١. Signal: مساحة آمنة للتحدث

في عـالم مزدحـم بالمخاطـر الرقميـة، يقـدّم لـكِ هـذا التطبيـق مسـاحة آمنـة للتواصـل... فهـو لا يسـجّل بياناتـكِ، ولا يحتفـظ بصـوركِ، ولا يطّلـع على ملفاتـكِ، وكأن كل شيء يـدور بينـكِ وبين الشـخص الآخـر فقـط — وكأنـكما تتحدثـان في غرفـة مغلقـة لا يسـمعها أحـد.

سـواء كنـتِ تُنسـقين فعاليـة، أو تدعـمين ضحيـة، أو حتـى ترغـبين بالتواصـل مـع زميلاتـكِ في العمـل الحقوقـي، فـإن Signal يقـدّم لـكِ:

- مكالمات آمنة ومشفرة، حتى الجماعية منها: لا داعي للقلق من التنصت أو المراقبة، لأن كل اتصال يتم عبر تشفير من الطرف إلى الطرف، لا يمكن لأي جهة فكّه.
- لا يحتفظ بسجل محادثاتك، ولا جهات اتصالك، ولا ملفاتكِ التي ترسلينها أو تستقبلينها. فقط أنتِ من تملكين هذه البيانات.
- هو مشروع غير ربحي، مفتوح المصدر، هدفه الأساسي هو حماية حرية التعبير وتطوير أدوات اتصال آمنة لكل من يعمل في بيئات خطرة أو مقموعة.
- إخفاء رقمكِ الحقيقي واستخدام رابط خاص: إن كنتِ لا ترغبين بمشاركة رقم هاتفكِ، يمكنكِ إنشاء رابط خاص يتيح للآخرين بدء محادثة معكِ دون رؤية رقمكِ.

كيف تنشئين رابطًا خاصًا على Signal دون مشاركة رقمكِ؟

افتحي تطبيق Signal على الهاتف ------> اضغطي على صورة ملفك الشخصي في أعلى الزاوية ------> اختاري: Privacy / الخصوصية ------> فعّلي خيار: Signal PIN / رمز تعريف الإشارة — إذا لم يكن مفعلًا ------> عودي إلى الملف الشخصي واختر: Username / اسم المستخدم ------> اختاري اسم مستخدم فريد خاص بكِ (مثل: @SafeDefender_iraq) ------> بعد الحفظ، سيظهر لكِ رابط خاص لمشاركته مع من تريدين (مثل:
(https://signal.me/#p/@SafeDefender_iraq

هذا الرابط يُمكنكِ نسخه ومشاركته مع الأشخاص الذين ترغبين بالتواصل معهم دون الحاجة لمشاركة رقم هاتفكِ.

"الحديث الآمن ضرورة حين يصبح مجرد التعبير عن الرأي مخاطرة."
مدافعة من البصرة

٢. تطبيق Wire: لأن خصوصيتكِ لا تحتاج رقم هاتف

في بعض الأحيان، يكون رقم الهاتف مفتاحًا يمكن أن يُستخدم ضدكِ. سواء فُقدت شريحة الهاتف، أو تم التجسس عليها، أو أُسيء استخدامها من قِبل أطراف معيّنة، فإن ربط بياناتكِ الحساسة برقم هاتف قد يجعل خصوصيتكِ عرضة للخطر.

ولهذا، يبرز تطبيق Wire كخيار مهم للمدافعات، إذ يمنحكِ فرصة التواصل الآمن دون الحاجة إلى رقم هاتف، فقط عبر بريدك الإلكتروني، وتقدم لك:

- رسائل مشفّرة ومكالمات جماعية بالصوت والصورة: مشفّر من الطرف إلى الطرف، سواء أكنتِ تُرسلين رسالة نصية، أو تتحدثين مع مجموعة من الزميلات في اجتماع افتراضي، أو تشاركين ملفات وتقارير حساسة.
- إنشاء مجموعات آمنة للعمل أو الدعم: يمكنكِ إنشاء مجاميع صغيرة للتخطيط، التنسيق، أو تقديم الدعم النفسي أو القانوني للضحايا. كل ما يتم تداوله داخل هذه المجموعات يبقى بينكنّ فقط.
- رسائل تحذف نفسها تلقائيًا: في حال أردتِ إرسال معلومات لا يجب أن تبقى محفوظة، يمكنكِ تفعيل خاصية الرسائل ذاتية الحذف، والتي تختفي بعد فترة زمنية محددة تختارينها.
- يشبه الـ VPN في حماية التتبع: لا يكتفي فقط بالمراسلات؛ بل يحمي هويتكِ الرقمية بدرجة تشبه ما توفره بعض تطبيقات الـ VPN من خصوصية إضافية عند الاتصال بالإنترنت.

كيف تستخدمين Wire بدون رقم هاتف؟

عند فتح التطبيق، اختاري «Sign up» ------> بدلاً من استخدام رقم الهاتف، اختاري التسجيل عبر البريد الإلكتروني ------> أدخلي بريدكِ الإلكتروني، واختاري اسم مستخدم خاص، ثم أنشئي كلمة مرور قوية ------> بعد التسجيل، يمكنكِ بدء استخدام التطبيق والتواصل بأمان.

"عدم ربط بياناتي برقم هاتفي منحني شعورًا بالتحكم، وكأنني أملك حريتي الرقمية من جديد."
مدافعة من النجف

نصائح:

- اجعلي رقمكِ وهويتكِ غير مكشوفة...
- لا تستخدمي رقم هاتفكِ الأساسي في كل مكان.
- استخدمي بطاقة SIM بديلة مخصصة فقط للعمل الرقمي.

- **اخفي موقعكِ:** "خفوت في الظهور... وطمأنينة في الهوية"

لا تسمحي للتطبيقات بتحديد موقعكِ الجغرافي طوال الوقت واستخدمي أدوات الـ VPN لتغيير أو إخفاء موقعكِ عند الحاجة، خاصة عند إرسال معلومات حساسة أو فتح روابط غير موثوقة.

ليست كل حركة نخطوها على الإنترنت يجب أن تكون مرئية. كمدافعة عن حقوق الإنسان، موقعكِ الجغرافي وهويتكِ الرقمية قد يتحولان إلى مدخل خطر يهدد سلامتكِ، خاصة في البيئات التي تُراقب فيها الناشطات، أو يُساء استخدام المعلومات ضدهن.

هنا، نُرشدكِ إلى خطوات عملية لإخفاء موقعكِ، والتقليل من بصمتكِ الرقمية، حتى تظلّي أنتِ من يختار متى وأين يُعرف عنكِ.

لماذا يُعد الموقع الجغرافي قضية حساسة؟

لأن بعض التطبيقات — دون علمكِ أحيانًا — تشارك موقعكِ مع أطراف ثالثة، أو تسجله تلقائيًا في خلفية الصور والمنشورات. هذه البيانات، لو وقعت في الأيدي الخطأ، قد تكشف تحركاتكِ، أو تضعكِ في موضع خطر أثناء التغطية أو التوثيق أو حتى التواصل اليومي.

ما هي الخطوات لإخفاء موقعكِ وتأمين هويتكِ الرقمية:

١. استخدام VPN موثوق:

اختاري تطبيق VPN من المصادر الموثوقة (مثل ProtonVPN أو Mullvad) يخفي عنوان IP الحقيقي، ويمنع تتبع موقعكِ الجغرافي الحقيقي عند تصفح الإنترنت أو استخدام التطبيقات.

- **ProtonVPN:** حين تصبح خطواتكِ على الإنترنت قابلة للتتبع، يمنحكِ هذا التطبيق ممرًا سريًا تتصفحين عبره العالم بحرية، دون أن تتركي خلفكِ أثراً يدلّ عليكِ

- **Mullvad:** تخيلي أنكِ تدخلين إلى غرفة مزدحمة دون أن يضطر أحد لمعرفة اسمكِ أو وجهتكِ أو حتى سبب وجودكِ... هذا بالضبط ما يفعله.

وهو تطبيق يساعدكِ على تصفّح الإنترنت بطريقة تخفي مكانكِ وهويتكِ، من دون الحاجة لتسجيل بريد إلكتروني أو رقم هاتف. كل ما تحتاجينه هو رقم عشوائي يُمنح لكِ لتبدئي باستخدامه مباشرة.

لماذا هذه التطبيقات مهمة؟

لأنها تحميكِ من التتبع والمراقبة، خاصة في حال كنتِ تعملين على قضايا حساسة، أو تتواصلين مع ضحايا أو شبكات دعم. كما أنها مفيد جدًا إذا كنتِ في منطقة تخضع للرقابة أو الحظر الرقمي، أو تشعرين أن اتصالكِ قد يكون تحت المراقبة.

"في العمل الحقوقي، الخصوصية هي وسيلة للبقاء والاستمرارية."

٢. تعطيل خدمات الموقع على الهاتف:

اذهبي إلى إعدادات الهاتف ------> "الخصوصية" أو "الموقع" ------> أوقفي الوصول إلى الموقع لجميع التطبيقات غير الضرورية. ويمكنكِ أيضًا تفعيل خيار "السماح فقط أثناء الاستخدام" للتطبيقات التي تحتاجينها أحيانًا.

٣. احذفي البيانات الجغرافية من الصور:

الصور الملتقطة عبر الهاتف تسجّل مكان التقاطها تلقائيًا.

في الإعدادات: ------> أوقفي خيار «تضمين بيانات الموقع» في الكاميرا.

٤. استخدام أسماء مستعارة أو معرفات غير مباشرة: عند التفاعل في المساحات العامة أو المنتديات الرقمية، أو حتى إنشاء حسابات حساسة، لا تربطيها باسمكِ الكامل أو بأي معلومات قد تُشير إليكِ.

٥. راقبي التطبيقات التي تعرف مكانكِ دون علمك: بعض التطبيقات تحتفظ بصلاحيات قديمة. قومي بمراجعة دورية لقائمة التطبيقات والصلاحيات، واحذفي كل ما لا تحتاجينه فعليًا.

"أحيانًا، الحماية تعني أن تختاري الظهور فقط حين تكوني مستعدة، لا حين يُفرض عليكِ."
مدافعة من السليمانية

خطوتك الثانية: حفظ الملفات الحساسة — لا تتركي أثركِ مكشوفاً!

عزيزتي المدافعة،

في عملكِ اليومي، تمرّ بين يديكِ مستندات وتقارير وصور وتسجيلات قد تحتوي على معلومات حساسة تتعلق بضحايا، أو نشاطات ميدانية، أو حتى بحياتكِ الخاصة. ترك هذه الملفات على سطح المكتب، أو في مجلدات غير محمية، يشبه ترك باب منزلكِ مفتوحًا للجميع.

لكن لا تقلقي، فمع خطوات بسيطة، يمكنكِ جعل هذه المعلومات الحقيقية غير مرئية لمن لا يجب أن يراها.

كيف تحمين ملفاتكِ؟

إليكِ بعض الممارسات اليومية التي تساعدكِ على إبقاء ملفاتكِ الحساسة بعيداً عن الأعين غير المرغوب بها:

"حماية الملفات هي خط الدفاع الأول عن الأمان الشخصي والمجتمعي."

١. اجعلي التشفير صديقتكِ: استخدمي برامج مجانية وموثوقة لتشفير الملفات او الاقراص، مثل:

- **BitLocker:** لمايكروسوفت ويندوز (Microsoft Windows): أداة لحماية البيانات، تقوم بتشفير محركات الأقراص الويندوز للمساعدة في منع سرقة البيانات أو كشفها. يمكن اتباع هذا الرابط:

https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/install-server

لمعرفة كيفية تشفير محرك الاقراص في نظام الويندوز.

- **Veracrypt:** خزنتك الرقمية الخاصة

هل تخيّلتِ يوماً أن يكون لديكِ صندوق حديدي داخل جهازكِ، لا يمكن لأحد فتحه إلا بكلمة سر لا يعرفها سواكِ؟..هذا بالضبط ما يفعله.

هو برنامج مجاني مفتوح المصدر، يقوم بإنشاء مساحة مشفّرة (مثل خزانة سرّية) داخل جهازكِ. يمكنكِ تخزين ملفاتكِ الحساسة بداخلها، ولن يتمكن أحد من فتحها أو رؤيتها دون كلمة المرور.

كيف يعمل؟ باختصار عن طريق مشاهدة الفيديو الموجود في هذا الرابط:
https://www.youtube.com/watch?v=HEybfZXYpok&ab_channel=KMDTech
واتباع الخطوات التالية:

تنشئين "حاوية مشفّرة" – ملف مخفي يعمل كمجلد مغلق ------> تختارين كلمة مرور قوية ------> عند الحاجة، تفتحين الحاوية وتستخدمين الملفات بداخلها ------> عند الانتهاء، تغلقين الحاوية لتعود غير قابلة للفتح أو القراءة.

مثالي للمدافعات اللواتي يحتفظن ببيانات عن الضحايا، الشهادات، الصور، أو أي ملفات شخصية لا يجب أن تقع في الأيدي الخطأ.

"حين لا يمكنكِ إخفاء وجود الملفات، اجعلي فتحها مستحيلاً."

٢. رتّبي قبل أن تضعي: احـرصي عـلى تصنيـف الملفـات (مثـلاً: تقاريـر، صور، بيانات شـخصية...) وضعي كل نـوع في مجلد محمي بكلمـة مـرور. ولا تـتركي الملفـات الحساسـة في "Downloads" أو "Desktop"، بـل ضعيهـا في مجلـدات مشـفّرة. واحـذفي الملفـات التـي لم تعـودي بحاجـة إليهـا، وتأكـدي مـن إفـراغ سـلة المهمـلات نهائيـاً.

يمكنـك حـذ الملفـات بطريقـة امنـة عـن طريـق اسـتخدام تطبيـق (https://eraser.heidi.ie)، والـذي يمكنـك تحميلـه عـن طريـق هـذا الرابـط: https://eraser.heidi.ie/download

٣. التخزين الآمن:

أ. التخزين الخارجي الآمن:

احفظـي نسـخة احتياطيـة مشـفّرة مـن ملفاتـكِ عـلى وحـدة تخزيـن خارجيـة (USB أو قـرص صلـب) ولا تحتفظـي بهـا دائمـاً متصلـة بالجهـاز، مـع تشـفير القـرص الصلـب بشـكل امـن، بمكنـك اسـتخدام Bitlocker الـذي تحدثنـا عنـه في سـابقا في (اجعـلي التشـفير صديقتـك) في عمليـة التشـفير.

ب. التخزين السحابي الآمن:

حـين تكونـين كثـيرة التنقّـل، أو تحتاجـين للوصـول إلى ملفاتـكِ مـن أكـثر مـن جهـاز أو مـكان، يصبـح التخزيـن السـحابي أحـد أكـثر الحلـول مرونـة. لكـن في عـالم مـليء بالمخاطـر الرقميـة، لا يكفـي أن تُخـزني ملفاتـكِ «عـلى الإنترنـت»، بـل يجـب أن يكـون ذلـك عـلى منصّـات تحـترم خصوصيتـكِ وتحمـي معلوماتـكِ.

نضـع بـين يديـكِ ثـلاث أدوات سـحابية آمنـة، جُربـت مـن قبـل المدافعـات عـن حقـوق الإنسـان في العـراق:

"ليس كل ما يُحفظ في السحابة آمنًا... لكنكِ قادرة على جعل بياناتكِ تطير وتبقى محمية."

- **MEGA:** مساحتكِ الخاصة، المشفرة بالكامل

لماذا MEGA؟

يمنحكِ ٢٠ غيغابايت مجانًا عند التسجيل. ويستخدم تشفيراً من الطرف إلى الطرف، وهذا يعني أن لا أحد يمكنه قراءة ملفاتكِ. وواجهته بسيطة ويمكنكِ رفع الملفات وسحبها وتنظيمها بسهولة.

- رابط تنزيل التطبيق لنظام Android
- رابط تنزيل التطبيق لنظام IOS
- رابط لتنزيل التطبيق لنظام الويندوز Windows و Mac و Linux.

نصيحة إضافية:

احرصي على الاحتفاظ بنسخة من مفتاح التشفير الذي يمنحه لكِ التطبيق، لأنه ضروري في حال احتجتِ استعادة حسابكِ.

- **Proton Drive:** الأمان في خدمة ملفاتكِ

من الفريق نفسه الذي أنشأ ProtonMail و ProtonVPN، جاء Proton Drive كأداة موثوقة للمدافعات.

ما يميزه:

- لا يطلب رقم هاتف للتسجيل.
- التشفير من لحظة رفع الملف وحتى تحميله.
- يدعم اللغة العربية وواجهة سهلة الاستخدام.
- مثالي لِـ: تخزين الوثائق الحساسة، الصور، الشهادات، ملفات الصوت والفيديو المرتبطة بقضايا حقوق الإنسان.

لتنزيل التطبيق:

- رابط تنزيل التطبيق لنظام Android

- رابط تنزيل التطبيق لنظام IOS
- رابط لتنزيل التطبيق لنظام الويندوز Windows و Mac.

تذكير مهم:

رغم قوة هذه الأدوات، تذكري دائماً أن الأمان يبدأ بكِ.
لا تشاركي كلمة السر، فعّلي التحقق بخطوتين، وراجعي محتوى التخزين السحابي بشكل دوري.
فملف واحد مكشوف، قد يكون كفيلاً بكشف كل شيء.

- **Tella:** أكثر من تخزين... أداة لحماية الناشطات

ليس مجرد مساحة تخزين، بل تطبيق ثوري يُستخدم خصيصًا لتوثيق الانتهاكات، ويمنحكِ قدرة على تخزين الملفات الحساسة بشكل آمن داخل هاتفكِ أو على السحابة.

لتنزيل التطبيق:

- رابط تنزيل التطبيق لنظام Android.
- رابط تنزيل التطبيق لنظام IOS.

لماذا تختارين Tella؟

- يعمل حتى في حال انقطاع الإنترنت.
- يمكنكِ إخفاءه من شاشة التطبيقات.
- يتيح التقاط الصور وتسجيل الصوت والفيديو مباشرة من داخله وتشفيرها فوراً.
- تم تطويره لحماية الصحفيات والناشطات والعاملات في البيئات عالية الخطورة.
- "حين يتحوّل هاتفكِ إلى أداة توثيق آمنة، فإن الحقيقة تكتسب درعاً يحميها."

٤. التنقل الذكي مع الملفات:

لا تشاركي الملفات الحساسة عبر البريد الإلكتروني العادي أو واتساب. استخدمي أدوات مشاركة آمنة أو خدمات تتيح إرسال ملفات مشفّرة بكلمة مرور.

يمكنك استخدام هذه الأدوات والتطبيقات لهذه الخطوة:

يجب ان تعلمي:

انه يمكنك استخدام تطبيقات سبق ذكرها في التخزين السحابي الامن (MEGA و Proton Drive) لإرسال الملفات على شكل رابط الكتروني مشفر ومدعوم بكلمة سر أيضا، فهي تقدم اكثر من خدمة في نفس الوقت

- **Onionshare:** هي أداة مفتوحة المصدر تتيح لكِ مشاركة الملفات واستضافة مواقع الويب والدردشة مع زملائكِ باستخدام شبكة Tor بشكل آمن ومجهول الهوية.

لتنزيل التطبيق:

- تنزيل التطبيق على نظام Android
- تنزيل التطبيق على نظام IOS
- تنزيل التطبيق على أنظمة Windows و Mac و Linux.

- **Tresorit Send:** عن طريق الخدمة المجانية، شاركي الملفات السرية مع روابط المشفرة من طرف إلى طرف. يتم تشفير ملفاتكِ قبل أن تغادر جهازك ولا يتم فك تشفيرها أبداً حتى يصل إليها المستلم.

رابط الوصول الى الخدمة من هنا.

ملاحظة مهمة:

في حال كنتِ تعملين ضمن فريق أو مع شبكة من المدافعات، تأكدي من توحيد طريقة التخزين والحماية، فضعف نقطة واحدة يمكن أن يُعرض الجميع للخطر.

خطوتك الثالثة: "حسابكِ هو هويتكِ... لا تتركي المفاتيح لأي أحد"

١. حماية الحسابات وكلمات المرور

كل يـوم تفتـحين بريـدك، تتصفـحين فيسـبوك، تشـاركين ملفـات، أو تنضـمين لاجـتماع حقوقي. كل هـذه النوافـذ الرقميـة تُفتـح بكلمـة مـرور. فهـل فكـرتِ يومًـا كـم هـو سـهل على شـخص آخـر أن يدخـل مـن خلالهـا إن لم تكـن مؤمّنـة جيـدًا؟

حسـاباتكِ ليسـت فقـط وسـائل تواصلـك، بـل هـي أيضًـا مـكان يحتفـظ بمحادثاتك، صـورك، وثائقـك، وشـبكة علاقاتـكِ... لهـذا فـإنّ حمايتهـا أول خطـوة لبنـاء بيئـة رقميـة آمنـة.

كيف تحمين حساباتكِ؟ إليكِ طريقتنا،خطوة

تذكّري:

حماية ملف واحد قد تساوي حماية حياة. والأمان يبدأ بخطوة بسيطة: لا تتركي ما هو خاص في متناول من لا يجب أن يصل إليه.

بخطوة، بدون تعقيد:

أولاً: ابتكري كلمة سرّ لا تُنسى ولا تُخترق

- اجعليها طويلة (١٢ حرفًا على الأقل).
- استخدمي خليطًا من الأحرف الكبيرة والصغيرة، الرموز، والأرقام.
- لا تسـتخدمي معلومـات شـخصية (مثـل اسـمك أو اسـم أحـد أولادك أو تاريـخ ميلادك..الـخ).

مثال لكلمة مرور قوية: S!sta2025:Let'sKeepF!ghting

"كلما كانت كلمة المرور معقدة، كلما صعب اختراقكِ، وكلما زادت المسافة بينكِ وبين المتصيّدين."

ثانياً: استخدمي أحد تطبيقات كلمات المرور

تطبيق مثل: **Bitwarden**

تساعدكِ على توليد كلمات مرور قوية وتخزينها في مكان مشفّر لا يُفتح إلا بكلمة رئيسية واحدة فقط. ولا حاجة لحفظ كل كلماتكِ في رأسكِ، أو الأسوأ... في ملف على سطح المكتب.

لتنزيل التطبيق:

- تنزيل التطبيق على نظام Android.
- تنزيل التطبيق على نظام IOS
- تنزيل التطبيق على Windows و Mac و Linux.

"الهويات الرقمية مثل المفاتيح: واحدة للبيت، وأخرى للسيارة، وثالثة لصندوق الرسائل... فلا تستخدمي مفتاحاً واحداً لكل شيء."

ثالثاً: فعّلي التحقق بخطوتين (Two-Factor Authentication)، لجميع حساباتك الأساسية (جيميل، فيسبوك، إنستغرام، واتساب، Zoom...)

- **الواتساب:** اذهبي إلى الإعدادات > الحساب > التحقق بخطوتين > تفعيل
- **الفيسبوك:**

- قومي بزيارة: https://accountscenter.facebook.com/password_and_security
- اضغطي على "المصادقة الثنائية"

- **الإنستغرام:**

- قومي بزيارة https://accountscenter.instagram.com/password_and_security
- اضغطي على "المصادقة الثنائية"

- **منصة اكس (تويتر سابقاً):**

- قومي بزيارة https://x.com/settings/security
- اضغطي على "المصادقة الثنائية"

- **جوجل وجيميل:**

- قومي بزيارة https://accounts.google.com/security
- اضغطي على "التحقق بخطوتين"

تلميحة رقمية ذكية:

خصصي بريداً إلكترونياً منفصلاً للاشتراك في المواقع أو النشرات.
لا تفتحي حساباتكِ من أجهزة عامة أو شبكات غير موثوقة.
لا تستخدمي نفس كلمة السر في أكثر من حساب.
احذفي الحسابات القديمة التي لم تعودي تستخدمينها.

خطوتك الرابعة: ابحثي وتواصلي بأمان... دائمًا!

المتصفحات الآمنة والاجتماعات الرقمية الآمنة

لماذا هذه الخطوة مهمة لكِ كمدافعة عن حقوق الإنسان؟

كلّ عملية بحث تقومين بها، وكل اجتماع تشاركين فيه، قد تترك ورائها أثراً رقمياً قد يُستغل ضدكِ، أو يُعرّضكِ للاختراق أو التتبع. ولهذا، فالتحرك الذكي عبر الإنترنت يعني أن تختاري «الطريق» و«المكان» الآمن قبل أن تتكلمي. وهذا يعتمد على قرارك انت...على ماذا تعملين؟ وما هي الملفات التي تتعاملين معها؟ و هل انت في أمان مع الملفات؟

أولاً: اختاري المتصفح الذي يحميكِ... لا من يراقبكِ

المتصفحات التقليدية تجمع بيانات التصفح لديكِ، وتحفظ سجل المواقع، وتشاركها أحياناً مع جهات دعائية. وغالبا لا تمنع التتبع بشكل افتراضي.

المتصفحات الآمنة المقترحة:

١. Brave: يمنع الإعلانات والمتتبعات تلقائياً ويمنحكِ سرعة عالية وتصفحًا هادئًا.

- لتنزيل المتصفح على نظام Android.
- لتنزيل المتصفح على نظام IOS.
- لتنزيل المتصفح على نظام Windows

٢. Firefox Focus: هو متصفح الخصوصية المخصص لك مع حماية تلقائية من التتبع، ويتم تحميل صفحاتك بشكل أسرع وتبقى بياناتك خاصة. هو مخصص لأجهزة الموبايل فقط.

- لتنزيل التطبيق على نظام Android.
- لتنزيل التطبيق على نظام IOS.

٣. Tor: دافعِ عن نفسكِ ضد التعقب والمراقبة. وتحايلي على الرقابة. يقوم المتصفح بعزل كل موقع تزورينه بحيث لا تستطيع متتبعات وإعلانات الجهات الخارجية تتبعكِ. يتم مسح أي ملفات تعريف ارتباط تلقائيًا عند الانتهاء من التصفح. وكذلك سجل التصفح الخاص بكِ.

كما يمنع متصفح تور أي شخص يراقب اتصالكِ من معرفة المواقع التي تزورينها. كل ما يمكن أن يراه أي شخص يراقب عادات تصفحكِ هو أنك تستخدمين تور.

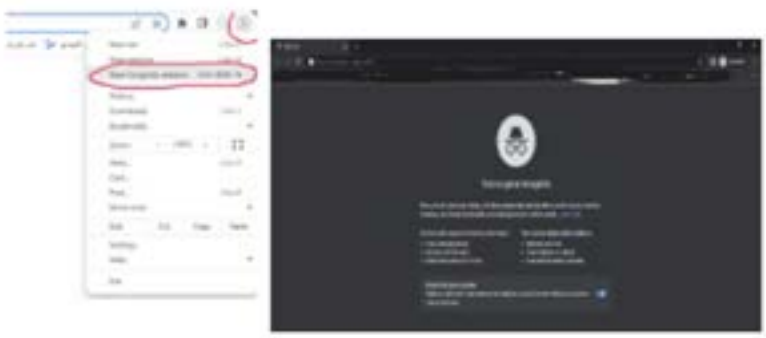
ويشير المتصفح على موقعه انهم يعملون على تعزيز حقوق الإنسان والدفاع عن خصوصيتكِ على الإنترنت من خلال البرمجيات المجانية والشبكات المفتوحة.

كيفية التنزيل:

- لتنزيل المتصفح على نظام Android.
- لتنزيل المتصفح على نظام Windows و MacOS و Linux.

٤. متصفح **Google:**

عنـد اسـتخدامك لهـذا المتصفـح يفضـل تفعيـل وفتـح المتصفـح الخقـي او الخـاص (incognito/private mode) كما هـو مـبين في هـذه الصـورة.



ثانياً: الاجتماعات الآمنة... مساحة عملكِ وصوتكِ

ما المشكلة؟

الاجتماعـات عـبر Zoom أو Google Meet قـد لا تكـون مشـفّرة مـن الطرفـين، أو قـد تُخـزّن التسـجيلات تلقائيًـا، مـا يعرّضـكِ ومَـن معـكِ للخطـر. لهـذا وحتـى نكـون عـلى قـدر كاف مـن الامـن والسـلامة سـمكن اسـتخدام تطبيقـات أخـرى تحافـظ عـلى خصوصيتـك وسريـة المعلومـات التـي لديـك عـلى أكـبر قـدر ممكـن مـن السـلامة.

أدوات موصى بها:

١. Jitsi Meet:

- مجاني ومفتوح المصدر.
- لا يتطلـب تسـجيل دخـول الا مـن خـلال الشـخص الـذي يقـوم بانشـاء الرابـط.
- يتيح لكِ تشفير المحادثة الصوتية والفيديو.
- يحتـوي التطبيـق عـلى الكثـير مـن الخيـارات والخدمـات المتوفـرة في تطبيق

Zoom لكـن بشـكل مجـاني بالكامل.

طريقة التنزيل:

- لتنزيل التطبيق على نظام Android.
- لتنزيل التطبيق على نظام IOS.

٢. Brave Talk:

يعتمـد المتصفـح على مـكالمات الفيديو الخاصـة غير المحدودة، ويتطلب الشـخص الـذي يقـوم بإنشـاء المكالمـة اسـتخدام متصفـح Brave ، ولكـن يمكـن للمشـاركين الانـضمام مـن أي متصفح.

اذا هو متصفح آمن ويوفر خدمة الاجتماعات بالصوت والصورة.

◊ خطوات سريعة لحماية الاجتماعات:

- لا تشاركي الرابط إلا مع من تثقين بهن/م.
- غطّي الكاميرا عندما لا تكون قيد الاستخدام.
- احرصي أن يكون الاجتماع من جهازك الشخصي، أو من بيئة محمية.

"كل رسالة مجهولة... قد تكون فخاً رقمياً ينتظر لحظة ضعف منكِ."

خطوتك الخامسة: افتحي بريدكِ بعين الحذر... لا بعين الثقة!

البريد الإلكتروني الآمن والروابط المشبوهة

لماذا هذه الخطوة مهمة لكِ كمدافعة عن حقوق الإنسان؟

كـثير مـن التهديـدات الرقميـة تبـدأ مـن مجـرد «رسـالة بسـيطة» تصـل إلى بريـدكِ. لكنهـا تخفـي وراءهـا برامـج خبيثـة، أو روابـط تـؤدي لاختراق جهـازكِ، أو حتـى انتحـال شـخصية زميلـة لـكِ. فالبريـد الإلـكتروني ليـس فقـط وسـيلة للتواصـل،

بـل هـو بوابـة دخـول إلى عالمـكِ الرقمـي بالكامـل.

أولاً: اختاري البريد الإلكتروني الذي يحميكِ

بريـدكِ العـادي (Gmail أو Yahoo أو Hotmail)، جيـد لكنـه ليـس الأفضـل مـن حيـث الخصوصيـة، حيـث تحتفـظ هـذه الشركات بنسـخة مـن كل رسـائلكِ على خوادمهـا، وغالبـاً مـا تكـون محميـة ولكـن ليسـت مشـفّرة مـن الطـرفين.

البدائل الآمنة المقترحة:

١. ProtonMail:

بريـد مشـفّر بالكامـل (End-to-End Encryption)، ولا يتطلـب رقـم هاتفـكِ للتسـجيل، ويعمـل مـن خلال واجهـة سـهلة أو تطبيـق.

هذه روابط تنزيل التطبيق:

- تنزيل التطبيق على نظام Android.
- تنزيل التطبيق على نظام IOS.
- تنزيل التطبيق على نظام Windows و Mac و Linux.

٢. Tutanota:

يوفـر التشـفير مـن طـرف إلى طـرف يضمـن خصوصيتـكِ، كـما تحمـي بياناتـك إلى أقـصى حـد باسـتخدام تشـفير آمـن كميًـا.

لتسـطيعين الحصـول عـلى حسـاب مـن خـلال الدخـول الى الموقـع الرئيـسي لهـم. ولتنزيـل التطبيـق يمكنـك ذلـك مـن خـلال الروابـط التاليـة:

- تنزيل التطبيق على نظام Android.
- تنزيل التطبيق على نظام IOS.
- تنزيل التطبيق على نظام Windows و Mac و Linux.

٣. Desktop - Thunderbird:

إذا كنتِ تعملين داخل منظمة مجتمع مدني، وتتعاملين يوميًا مع عشرات الرسائل الحساسة من الزملاء أو الضحايا أو الشركاء، فإن استخدام البريد الإلكتروني من خلال المتصفح لم يعد كافيًا — بل قد يكون خطيراً أحيانًا.

هنا يأتي دور Thunderbird.

هو برنامج مجاني ومفتوح المصدر من تطوير Mozilla (نفس الشركة التي طوّرت متصفح Firefox)، يمكنكِ تثبيته على جهازكِ المكتبي أو المحمول، وربطه ببريدكِ الإلكتروني (Tutanota، ProtonMail Bridge، Gmail، وغيرها من المواقع الخاصة بالمنظمة والتي من الممكن ان ترتبط ايميلاتها مع الموقع الرئيسي لهم).

لماذا ننصحكِ به؟

واجهة واحدة لكل حساباتكِ: يمكنكِ إدارة عدة عناوين بريد إلكتروني من مكان واحد، دون الحاجة إلى فتح عشرات النوافذ. والوضع غير المتصل (Offline): يمكنكِ قراءة وإعداد الرسائل دون اتصال، ثم إرسالها لاحقًا عند توفر الإنترنت.

يمكن الحصول على التطبيق من خلال هذا الرابط
https://www.thunderbird.net/en-US/thunderbird/all/
والمتواجد فيه طريق تنزيل التطبيق لكل الأجهزة.

ثانياً: الروابط المشبوهة... أفخاخ رقمية في ثوب ودّي

كيف تتعرفين على الرابط المشبوه؟ يُرسل من عنوان لا تعرفينه، أو فيه اسم غريب، وقد يحتوي على أخطاء إملائية أو لغوية غريبة. أو يدّعي أنه من مؤسسة معروفة، لكن عنوان الإرسال مزيف، أو يطلب منكِ تسجيل الدخول إلى حسابكِ في موقع بطريقة مستعجلة أو مخيفة.

ما العمل؟

- لا تضغطي أبداً على روابط لا تعرفين مصدرها.
- حـرّكي الفـأرة فـوق الرابـط دون الضغـط عليـه... وانظـري هـل الرابـط الحقيقـي يتطابـق مـع النـص؟
- افتحـي الرابـط في أحـد المتصفحـات التـي اقترحناهـا عليـكي او في وضـع التصفـح الآمـن أو في متصفـح ثانـوي إذا اضطُـررتِ لذلـك.

"كل رابط تضغطين عليه، إما أن يكون سلماً للثقة... أو باباً يُفتح على المجهول."

بالإمـكان اسـتخدام أدوات للتحقـق مـن الروابـط المشـبوهة او الملفـات التـي تصلـك، وأبـرز هـذه الأدوات هـي:

١. Virustotal:

في زحمـة الرسـائل اليوميـة والروابـط المرسـلة مـن مصـادر معروفـة أو مجهولـة، مـن السـهل أن تنقـري عـلى شيء قـد يبـدو بريئًـا... لكنـه في الحقيقـة بوابـة للاخـتراق.

هنـا يـأتي دور VirusTotal — أداة مجانيـة عـبر الإنترنـت تسـمح لكِ بفحـص الملفات أو الروابـط قبـل فتحهـا، باسـتخدام عـشرات برامـج الحمايـة في آنٍ واحـد. أي أنـكِ في لحظـات، تحصلـين عـلى «رأي جماعـي» مـن أقـوى محـركات مكافحـة الفيروسـات في العـالم.

نصيحة مهمة:

بعد فك الرابط، يمكنكِ نسخه ثم فحصه عبر VirusTotal للحصول على طبقة إضافية من الحماية.

٢. CheckShortURL:

في كثـير مـن الأحيـان، تصلـكِ روابـط مختـصرة مثـل:(bit.ly/3abcXyz أو tinyurl.

com/xyz123)، ورغم أنها تبدو بسيطة، إلا أنها قد تخفي وراءها مواقع ضارة، أو صفحات تصيّد، أو ملفات تجسسية.

CheckShortURL يساعدكِ على رؤية الوجه الحقيقي لهذه الروابط قبل أن تنقري عليها، فهو يكشف لكِ ما هو العنوان الكامل الذي تم إخفاؤه، ويعطيكِ فكرة مبدئية عمّا إذا كان الرابط يبدو آمناً أم لا.

كيف تستخدمينه؟

انسخي أي رابط مختصر مشكوك فيه، والصقيه في موقع checkshorturl.com. سترين فورًا العنوان الكامل، ووجهة الرابط، وأحيانًا حتى معاينة للموقع.

"الروابط المختصرة قد تخفي أكثر من مجرد عنوان... أحياناً قد تخفي تهديداً لصوتكِ ومساحتكِ الرقمية."

خطوتكِ السادسة: واي فاي آمن... بيتكِ الرقمي يبدأ من هنا

شبكة الإنترنت التي تستخدمينها كل يوم هي بوابتكِ إلى العالم الرقمي، لكنها قد تكون أيضًا مدخلاً للآخرين إلى خصوصيتكِ دون علمكِ. في المنزل، في المكتب، في مقهى عام أو فندق... الاتصال بشبكة Wi-Fi غير آمنة أو مجهولة قد يعرّضكِ لاختراقات صامتة لا تترك أثراً ظاهراً.

لهذا السبب، من المهم جدًا أن تتحققي من أمان الشبكة التي تستخدمينها، وتتأكدي أن لا أحد يشاركِ الاتصال دون علمكِ، أو يتجسّس على نشاطكِ.

"أنتِ لا ترين من معكِ على الشبكة، لكن من على الشبكة قد يرى كل شيء تفعلينه."

Fing: عينكِ على شبكة الواي فاي

هو تطبيق مجاني يمكنكِ استخدامه على هاتفكِ او جهاز اللابتوب لديكِ لفحص شبكة Wi-Fi التي تتصلين بها، سواء في المنزل أو المكتب أو في الأماكن العامة.

ماذا يفعل Fing؟

- يُظهـر لـكِ جميـع الأجهـزة المتصلـة بالشـبكة (حتـى تلـك التـي لا ترينهـا عـادة).
- يساعدكِ على كشف الأجهزة الغريبة التي لا تعرفينها.
- ينبهكِ في حال وجود نشاط غير معتاد على الشبكة.
- يعطيكِ فكرة عن مدى أمان الشبكة (هل هي مشفرة؟ من يديرها؟).

لتنزيل التطبيق:

- تنزيل التطبيق على نظام Android.
- تنزيل التطبيق على نظام IOS.
- تنزيل التطبيق على نظام Windows.
- تنزيل التطبيق على نظام MacOS.

"عندما تؤمنين شبكتكِ، تؤمنين بيتكِ الرقمي وصوتكِ ومساحة عملكِ وخصوصيتكِ... كلها تبدأ من نقطة اتصال واحدة."

نصائح يومية لاستخدام آمن لشبكات Wi-Fi:

- **في المنزل والمكتب:**

- غيّري اسم الشبكة وكلمة المرور الافتراضية التي تأتي مع جهاز الراوتر.
- فعّلي ميزة التشفير (WPA٢ أو WPA٣) من إعدادات الراوتر.
- افصلي شبكة الضيوف عن شبكتكِ الأساسية إن أمكن.

- **في الأماكن العامة:**

- تجنبي الشبكات المفتوحة بدون كلمة مرور.
- لا تشاركي معلومات حساسة أثناء الاتصال بشبكة غير موثوقة.

- استخدمي تطبيق VPN عند الضرورة، لتشفير الاتصال بالكامل.

"الحماية الرقمية ليست فقط كلمات مرور وتشفير واتصالات مشفّرة، بل هي أيضاً مساحة نفسية هادئة، تمنحكِ القدرة على الاستمرار، دون أن تنهكي."

خطوتكِ السابعة: الرفاهية الرقمية... لأن سلامتكِ النفسية جزء من الحمايةَ

في خضـمّ العمـل الحقوقـي، وسـط التهديـدات الرقميـة، والضغـوط النفسـية، والانشـغال اليومـي برصـد الانتهـاكات، قـد تنـسين شـيئًا مـهمًا جـدًا: **أنتِ نفسكِ**.

عندما تتعاملين يوميًا مع القضايا الصعبة، وتتواصلين مع الضحايا، وتتعرضين للمراقبة أو المضايقة الرقمية، فإن الأثر لا يكون تقنيًا فقط، بل عاطفي ونفسي أيضًا. لذلك فإن جزءًا لا يتجزأ من الحماية الرقمية هو الرفاهية الرقمية.

ما المقصود بالرفاهية الرقمية؟

هي الممارسات التي توازن بين استخدامكِ للتكنولوجيا وحاجتكِ للراحة النفسية والأمان العقلي، حتى لا يتحوّل العالم الرقمي إلى عبء مستمر ينهككِ جسديًا وذهنيًا.

إليكِ بعض الخطوات العملية التي يمكن أن تُحدث فرقًا كبيراً:

- امنحي نفسكِ فترات راحة رقمية قصيرة: حدّدي أوقاتًا في اليوم أو في الأسبوع لا تتعاملين فيها مع الشاشات أو البريد الإلكتروني أو التطبيقات الحساسة.
- ضعي تذكيرات أسبوعية بسيطة لمراجعة إعدادات الأمان، مثل التحقق من كلمات المرور أو تحديث التطبيقات أو إعادة تقييم صلاحيات الوصول في هاتفكِ. لا حاجة أن تفعلي كل شيء كل يوم.
- أنشئي "دائرة دعم رقمية" صغيرة من زميلاتكِ، لتتشاركن الخبرات، وتساعدن بعضكن على المراجعة والتذكير، أو ببساطة تبادل الدعم

العاطفي.

- مارسي "التأمل الرقمي": اسألي نفسكِ من وقت لآخر — هل هذا الاستخدام يعزز سلامتي؟ هل ما أفعله الآن يساعدني على مواصلة الطريق أم يستنزفني؟ هل هناك شيء يمكنني تغييره اليوم ليكون أكثر راحة وأمانًا لي؟

"المدافعة التي تعتني بنفسها، تعتني بقضيتها... لأن الحماية تبدأ من الداخل."
مدافعة شاركت بمراجعة الدليل من بغداد

ختامًا...

الحماية الرقمية ليست ترفًا، وليست عبئًا إضافيًا في زحمة المهام، بل هي حق وأداة بيدكِ، تمنحكِ مساحة أكثر أمانًا للتنفس، للتفكير، وللاستمرار.

خطوات بسيطة، يومية، تنمو معكِ وتتحول إلى درع، تحميكِ وتحمي من تثقين بهن ويثقن بكِ.

ليس المطلوب أن تكوني خبيرة، بل أن تكوني يقِظة، واعية، ومطمئنة بأنكِ لستِ وحدكِ.

القسم الثاني: سلوكيات الحماية الرقمية في المواقف المختلفة:

في العمل الحقوقي، لا يكفي أن نمتلك الأدوات... الأهم هو أن نعرف متى نستخدمها، وكيف نُطبّقها، وماذا نفعل في لحظة التوتر أو القرار السريع.

السلوك الرقمي الآمن ليس مجموعة تعليمات جامدة، بل هو انعكاس لعلاقتكِ بجهازك، بمعلوماتكِ، وبالناس من حولك. وكل موقف تمرين به، يضيف طبقة جديدة من الوعي، والخبرة، والقدرة على التصرّف بثقة. إن تشكيل سلوك رقمي واعٍ يبدأ من التجربة - من اللحظات التي شعرتِ فيها أنكِ كنتِ معرضة للخطر، ومن الخطوات التي ستقررين أخذها حتى لا تتكرر هذه التجربة معكِ أو مع غيركِ.

وما تحدثنا عنه سابقًا في تعريف المدافعات عن حقوق الإنسان، والمعايير التي تشكل جوهر عملهن، والمسؤوليات التي يحملنها، ليس مجرّد خلفية نظرية، بل هو جزء أساسي من الإعداد لهذه المواقف التي قد تضعكِ في مواجهة مباشرة مع المخاطر الرقمية. هذه المبادئ هي ما يمنحكِ البوصلة في الميدان، لتعرفي من أين تبدأين، وكيف تحمين نفسكِ والآخرين.

ولأنكِ تعملين في بيئة متغيرة، تتنقّلين بين ميادين الواقع وفضاءات العالم الرقمي، فإن هذا القسم من الدليل يسير معكِ في مواقف متعددة، من تغطية الاحتجاجات، إلى كتابة التقارير، إلى التفاعل مع الضحايا، وكل لحظة قد تحمل معها احتمالاً للخطر أو فرصة للأمان.

أولا: الأمن الرقمي أثناء تغطية الاحتجاجات والمظاهرات السلمية

عندما تختارين أن تكوني صوتًا في الشارع، وأن تُوثّقي، أو تعبّري، أو ترفعي كاميرتكِ في وجه العنف، فإنكِ لا تواجهين فقط واقعًا ميدانيًا صعبًا، بل أيضًا شبكة من التهديدات الرقمية التي قد تبدأ من هاتفكِ الصغير.

وفي هذا السياق، من المهم التأكيد على أن المشاركة في الاحتجاجات أو توثيقها ينبغي أن تستند دائمًا إلى مبدأ السلمية، واحترام القوانين والتشريعات النافذة في العراق وإقليم كوردستان. فالسلوك السلمي لا يحمي فقط المشاركين، بل يضفي أيضًا الشرعية الأخلاقية والقانونية على مطالبهم، ويمنح العمل الحقوقي قوته واستمراريته.

عند تغطيتكِ للاحتجاجات السلمية، تذكّري أن فقدان هاتفكِ – سواء من خلال السرقة أو المصادرة – قد يفتح الباب أمام من يحاول الوصول إلى كل شيء يخصكِ.

> **"كل خطوة رقمية واعية، تبعدكِ خطوة عن الخطر، وتقربكِ من بيئة أكثر أماناً لنا جميعاً."**
> من مراجعة جماعية للمدافعات على مسودة هذا الدليل

من خلال أدوات اختراق متوفرة، يمكن الوصول إلى رسائلكِ، صوركِ، ملفاتكِ،

وحتى كلمات المرور الخاصة بكِ. والأسوأ من ذلك، قد يعيدون تثبيت التطبيقات التي حذفتِها مؤخرًا أو يستخدمون بريدكِ الإلكتروني للدخول إلى حساباتكِ الأخرى.

لهذا، لا تتركي حماية جهازكِ وحساباتكِ لآخر لحظة. فالهاتف ليس فقط وسيلة اتصال، بل هو مساحة خاصة تحمل الكثير عنكِ وعن من تعملين معهم.

وحين تقررين النزول إلى الشارع لتوثيق، أو التعبير، أو المراقبة، فإن استعدادك الرقمي يوازي أهمية شعورك بالشجاعة. لأن الهاتف يمكن أن يكون درعكِ... أو نقطة ضعفكِ.

في مثل هذه اللحظات، تتحول الحماية الرقمية إلى حليفٍ حقيقي، يحرس خطواتكِ، ويمنحكِ مساحة إضافية من الأمان.

لذلك، نُقسم معكِ هذا القسم من الدليل إلى ثلاث مراحل:

١. قبل المشاركة في التظاهرة — استعدادك هو مفتاح الأمان

- خصصي هاتفًا منفصلًا إن أمكن، واستخدمي جهازًا لا يحتوي على بياناتكِ الشخصية أو حساباتكِ الخاصة، حتى لو تمت مصادرته، لن يكون فيه ما يُعرضكِ أو من تعملين معهمِ للخطر.
- فعّلي التشفير الكامل للهاتف، من إعدادات جهازكِ، يمكنكِ تشغيل خاصية Encryption لحماية الملفات داخليًا.
- احذفي أي مواد حساسة قبل الخروج، صور، تقارير، أسماء، محادثات... أي ملف قد يتحول إلى تهديد في حال الوصول إليه. يمكنك استخدام تطبيق Secure Eraser للقيام بذاك.
- تأكدي من تسجيل الخروج من الحسابات غير الضرورية، لا تتركي سوى الحسابات التي تحتاجينها بالفعل. كل حساب مفتوح هو باب محتمل للمتسللين.
- أوقفي خدمات الموقع الجغرافي (GPS)، خصوصًا إذا لم يكن ضروريًا.

تقليـل تتبـع موقعـكِ يعنـي تقليـل المخاطـر.

- احتفظي بنسخة احتياطية مشفّرة للمواد الهامة، ضعي المحتوى المهم على Proton Drive أو MEGA، واحذفي النسخ من الهاتف.
- فعّلي خاصية الحذف عن بُعد، في حال فُقد هاتفكِ، يمكنكِ مسحه فوراً:
  - للأجهزة التي تعمل على نظام IOS: https://www.icloud.com/find
  - للأجهزة التي على نظام الاندرويد: https://www.android.com/find
- ضعي خطة للهروب الرقمي، هل لديكِ بريد طوارئ؟ أو حساب بديل؟ فكري بخطة سريعة لحذف بياناتكِ من أي مكان.
- يوصى بتعطيل خاصية التعرف على الوجه ورمز مرور البصمة الإصبع (مثل Face ID وTouch ID)، مع ترك رمز مرور يدوي فقط. في حال مصادرة هاتفك أو أخذه، لا يُمكن استخدام وجهك أو إصبعك لفتح قفل جهازك دون موافقتك.

"أدركت لاحقًا أن الاحتجاجات لا تبدأ في الشارع، بل تبدأ من إعداد الهاتف."
مدافعة من الناصرية

٢. أثناء التظاهرة — سلوكيات وقرارات في لحظات الضغط

- تواصلي فقط عبر تطبيقات مشفّرة، مثل Signal أو Wire لتأمين محادثاتكِ ومكالماتكِ.
- تجنّبي مشاركة الصور أو الفيديوهات فورًا، احذفي البيانات التعريفية (Metadata) أو استخدمي تطبيقات تحذفها تلقائيًا.
- استخدمي تطبيقات توثيق آمنة، مثل Tella الذي يتيح التوثيق المشفر، الحذف الفوري، وعدم ربط المواد بهويتكِ.

- افعّـلي الرسـائل ذاتيـة الاختفـاء، خاصـة في WhatsApp وSignal، لتُمحـى المحادثـات تلقائيًـا.
- ابـقِ عـلى تواصـل مسـتمر مـع زميلتـك أو فريقـك، حتـى لـو برسـالة كل سـاعة، فقـط لتأكيـد أنـكِ بخـير.
- استخدمي متصفحًا لا يحتفظ بسجل التصفح، مثل Firefox Focus أو Brave.
- فعّـلي وضـع الطـوارئ عـلى هاتفـكِ، لإرسـال إشـعار وموقعـكِ لصديقـة موثوقـة إذا شـعرتِ بالخطـر.

٣. بعد التظاهرة — استرجعي السيطرة على بياناتكِ

- راجعـي محتـوى الهاتـف واحـذفي مـا لم يعـد ضروريًـا، تأكـدي أن مـا تبقّـى لا يمكـن اسـتخدامه ضـدكِ أو ضـد الآخريـن.
- انقـلي الملفـات المهمـة إلى تخزيـن آمـن، إلى قـرص خارجـي مشـفّر أو مسـاحة سـحابية موثوقـة مثـل Mega او Proton Drive.
- تأكـدي مـن إيقـاف الوصول المؤقـت للتطبيقـات المسـتخدمة أثنـاء التغطية، إن أمكـن، أزيـلي التطبيقـات الحساسـة أو عطّلي صلاحياتهـا مؤقتًا.
- أعيـدي تفعيـل خدمـات الموقـع إذا كانـت موقوفـة، لكـن فقـط بعـد التأكـد مـن أنـكِ بأمـان.

التحديات الرقمية أثناء تغطية المظاهرات:

عندمـا تتواجديـن في الشـارع لتغطيـة احتجـاج سـلمي، لا يكـون التحـدي فقـط في مواجهـة الخطـر الميـداني، بـل أيضـاً في مـا لا ترينـه — ذلـك الـذي يحـدث خلـف الشاشـات، في البُنـى الرقمية، على مسـتوى المراقبـة والاسـتهداف والاختراق.

التقنيـات التـي نحملهـا معنـا يمكـن أن تكـون وسـيلة للتمـكين، أو أداة للتهديـد. ولهـذا، مـن الضروري أن تكـوني على درايـة بالتحديـات الرقميـة التـي قـد تواجهـكِ، حتـى تكـوني مسـتعدة لهـا وواعيـة لطـرق التعامـل معهـا:

- المراقبة الحكومية:

في كـثير مـن الحـالات، تقـوم السـلطات بمراقبـة نشـاطات التحشـيد والتنظيـم على وسـائل التواصـل، أو التنصـت على المـكالمات وتتبـع المواقـع الجغرافيـة. هـذه المراقبـة قـد تبـدأ قبـل التظاهـرة، وتشـتد في ذروتهـا.

- الهجمات الإلكترونية:

قـد تتعـرض أجهزتـكِ لهـجمات اختراق أو لبرمجيـات خبيثـة تُـزرع مـن خلال روابـط وهميـة أو تطبيقـات مزيفـة، ما يـؤدي إلى تسريـب بياناتـكِ أو السـيطرة على هاتفكِ.

- الاستهداف عبر وسائل التواصل الاجتماعي:

تشـمل حـملات تشـهير، أو تصيّد يسـتغل تغطيتكِ للتظاهـرات للطعـن بمصداقيتكِ أو تخويفـكِ. هـذه الهـجمات قـد تكون مـن أفـراد أو مجموعـات منظمة.

- مصادرة أو تلف الأجهزة:

احـتمال فقـدان هاتفـكِ أو حاسـوبكِ أثنـاء التظاهـرة — سـواء بالمصـادرة أو التلـف — يعنـي فقـدان كل المـواد التـي وثّقتِهـا، أو تعريـض أصحابهـا للخطـر إذا لم تكـن محميـة بشـكل كافٍ.

"أقوى أدوات الأمان ليست التطبيقات، بل الهدوء الداخلي والقدرة على اتخاذ قرار واعٍ."

مدافعة من السليمانية

لا تنسي رفاهيتكِ الرقمية في خضم كل ذلك:

- بـين التحقـق مـن أمـان الهاتـف، والقلـق مـن الاخـتراق، والانشـغال بتوثيـق الانتهـاكات، قـد تنسـين أهـم عنـصر في المعادلـة: أنـتِ.
- الرفاهيـة الرقميـة لا تعنـي فقـط أن تكـون أجهزتـكِ آمنـة، بـل أن تبقـي أنـتِ أيضًـا متوازنـة، واعيـة، ومرتاحـة مـع أدواتـكِ الرقميـة.

- الضغـوط المسـتمرة، والخـوف مـن الاسـتهداف، والمعلومـات المتدفقـة، كلهـا عوامـل ترهـق الذهـن وتسـتنزف الطاقـة. لهـذا:

- خصـصي وقتًـا أسـبوعيًا لمراجعـة إعـدادات الأمـان بهـدوء، وليـس فقـط عنـد الطـوارئ
- لا تستخدمي التطبيقات الحساسة في لحظات التوتر أو التعب الذهني.
- نظّمـي مسـاحة هاتفـكِ وبريـدكِ حتـى لا تتحولـين إلى مراقِبـة لنفسـك أكـثر مـما تعملـين عـلى حمايتهـا.
- تذكّـري: أخـذ اسـتراحة رقميـة قصـيرة لا يُقلّـل مـن التزامـكِ، بـل يحمـي استمراريتكِ.

"الجهة التي استهدفتنا لم تخترق موظفة في المؤسسة شخصيا، بل اخترقت حاسوب المنظمة لديها، ووجدت ما يكفي لإسكات صوت المؤسسة وابتزازاها."

مدافعة من بغداد

ثانيا: الحماية الرقمية داخل مؤسسات المجتمع المدني:

في العـراق، تواجـه المدافعـات عـن حقـوق الإنسـان تحديـات لا تتوقـف عنـد الشـارع أو الحسـابات الشـخصية، بـل تمتـد إلى أماكـن العمـل التـي ينتـمين إليهـا، وغالبًـا مـا تكـون هـذه المؤسسـات خـط الدفـاع الأول عـن الضحايـا، والملاذ الآمـن للمسـتضعفين.

لكن ماذا لو كان هذا «الملاذ» نفسه غير محمي؟

مـاذا لـو أن جهـازًا غير مؤمَّـن أو ملفًـا غير مشـفَّر أدى إلى تسريـب بيانـات ضحيـة عنـف، أو كشـف هويـة شـاهدة، أو تعريـض ناشـطة للخطـر؟

مؤسسـات المجتمـع المـدني، خاصـة تلـك التـي تقودهـا نسـاء أو تعمـل مـع فئـات مهـددة (ناجيـات مـن العنـف، أقليـات دينيـة، مدافعـات شـابات)، هـي هـدف مبـاشر لانتهـاكات رقميـة قـد تتخـذ أشـكالًا متعـددة:

- اختراق بريد رسمي
- تسريب تقارير داخلية
- تعقُّب نشاطات المنظمة
- مراقبة اجتماعات الاونلاين.
- أو حتى هندسة اجتماعية لاستدراج إحدى الموظفات

ولأن هـذه المؤسسـات تعمـل غالبًـا بمـوارد محـدودة، وتحـت ضغـط مسـتمر، فـإن الحمايـة الرقميـة لا تكـون أولويـة، رغـم أنهـا يجـب أن تكـون الأسـاس.

هنـا لا يكفـي أن تكـوني عـلى درايـة بكيفيـة حمايـة نفسـك فقـط، بـل أن تسـاهمي أيضًـا في بنـاء ثقافـة حمايـة داخـل مؤسسـتك: كيـف نرسـل الإيميـلات؟، أيـن نخـزن الملفـات؟، مـن يملـك كلـمات المـرور؟، هـل اجتماعاتنـا عـبر تطبيـق آمـن؟، مـن يسـتطيع الدخـول إلى حسـابات المؤسسـة؟.

هذا القسم سيساعدك على فهم:

نصيحة:
لا تستخدمي بريدك الشخصي لأي نشاط حقوقي مؤسسي. واحرصي على تفعيل التحقق بخطوتين (2FA) دائمًا.

مفاتيح الأمان الرقمي لمؤسستك: خطوات بسيطة لحماية كبيرة

لا تحتـاج المؤسسـة التـي تعمـلين فيهـا إلى ميزانيـة كـبيرة أو قسـم تقنيـة متطـور كي تصبـح بيئـة رقميـة آمنـة. في الواقـع، معظـم الهـجمات تبـدأ مـن سـلوك فـردي غير مقصـود، مثـل فتـح رابـط مشـبوه، أو اسـتخدام كلمـة مـرور ضعيفـة، أو مشـاركة ملـف دون تشـفير.

فـيما يلي مجموعـة مـن الإرشـادات الأساسـية والتطبيقـات المجانيـة أو مفتوحـة المصـدر، التـي ستسـاعدك في بنـاء ثقافـة حمايـة رقميـة داخـل المؤسسـة خطـوة بخطـوة:

نصيحة:

لا ترسلي ملفات عبر البريد أو واتساب دون تشفير، ولا تحفظي ملفات الضحايا على الحاسوب أو الموبايل دون حمايتها بكلمة مرور قوية.

١. تأمين البريد الإلكتروني الرسمي

استخدمي بريدًا آمنًا لإرسال واستلام التقارير والوثائق الحقوقية، اشرنا اليها سابقا في الروتين الذي من الممكن ان تتبعيه مثل:

- ProtonMail: بريد إلكتروني مشفّر بالكامل وسهل الاستخدام.
- Tutanota: بديل ممتاز ويدعم التشفير بين الأطراف.
- Thunderbird (سطح المكتب): لإدارة بريدك الإلكتروني عبر بروتوكولات أكثر أمانًا، خاصة داخل مكاتب المؤسسات.

٢. تخزين ومشاركة الملفات الحساسة

استخدمي أنظمة تخزين مشفّرة ومخصصة لحفظ وثائق الضحايا، التقارير، الصور، أو الشهادات:

- Veracrypt: لتشفير الأقراص الصلبة والملفات محليًا.
- ProtonDrive أو MEGA: تخزين سحابي آمن بتشفير شامل.
- Tella: لتوثيق الانتهاكات بهوية مجهولة وتشفير عالي، مناسب للعاملات ميدانيًا.

نصيحة:

ابتعدي عن إرسال كلمات المرور عبر البريد أو الرسائل، وراجعي كلمات المرور كل 3 أشهر على الأقل.

٣. إدارة كلمات المرور

استخدمي تطبيقًا لإدارة كلمات المرور لتفادي تكرارها أو نسيانها مثل تطبيق Bitwarden

٤. المتصفحات الآمنة والروابط المشبوهة

- استخدمي متصفحات تضمن الخصوصية ولا تحتفظ بسجلاتك مثل Brave أو Firefox Focus: لحماية التصفح اليومي.
- افحصي الروابط الغريبة قبل النقر عليها:
  - CheckShortURL: يكشف مصدر الروابط المختصرة.
  - VirusTotal: يفحص الروابط والملفات قبل فتحها أو تحميلها.

٥. بيئة عمل محمية

- حدّدي من يمكنه الدخول إلى أجهزة المؤسسة أو حساباتها.
- خصّصي بريدًا رسميًا لكل مدافعة/موظفة بدلاً من مشاركة الحسابات.
- حدّدي صلاحيات الوصول إلى الملفات، وخاصة الحساسة.
- أوقفي تثبيت التطبيقات العشوائية على الأجهزة المؤسسية.

٦. شبكات الواي فاي الآمنة

- لا تستخدمي شبكة مفتوحة لإرسال تقارير أو تحميل ملفات.
- في المكتب أو المنزل، راقبي الأجهزة المتصلة بالشبكة:
  - Fing: تطبيق يساعدك في معرفة الأجهزة المجهولة المتصلة بشبكتك.

٧. اجتماعات وتدريبات رقمية محمية

نصيحة:

تأكدي دائمًا من عنوان الرابط قبل النقر، خاصة في الرسائل المفاجئة أو العروض الغريبة.

- لا تشاركي روابط الاجتماعات في مجموعات عامة.
- استخدمي تطبيقات مشفّرة للاجتماعات:
- Jitsi Meet: مجاني ومفتوح المصدر دون حاجة لتسجيل دخول.
- Zoom (مع إعدادات أمان مفعّلة): فعّلي الانتظار والتسجيل المسبق.

٨. ثقافة حماية داخل الفريق

- خصصي وقتًا شهريًا لمراجعة إعدادات الأمان.
- درّبي زميلاتكِ على كشف الروابط الخبيثة أو التهديدات الرقمية.
- حدّدي منسقة داخل الفريق لمتابعة شؤون الحماية الرقمية وتحديث الأدوات.
- اتفقي على خطة طوارئ إذا تم اختراق أحد الحسابات أو الأجهزة.

نصيحة:

دوّني ملاحظات الاجتماعات في ملفات مشفّرة، وامسحي التسجيلات إذا لم يكن الاحتفاظ بها ضروريًا.

وأخيرًا:

لا تنتظري الهجوم لتبني دفاعك.

كل خطوة تأخذينها لحماية ملفاتك، بريدك، وأدواتك، هي خطوة لحماية الضحايا، الشهود، وزميلاتكِ في العمل.

ثالثا: عندما يتحول الفضاء الرقمي إلى ساحة تهديد: كيف نواجه المضايقات والابتزاز الإلكتروني؟

في عالم الإنترنت، لا يكفي أن نكون حاضرات بأصواتنا، بل يجب أن نكون واعيات بالتهديدات التي قد تواجهنا. واحدة من أخطر هذه التهديدات هي المضايقات والابتزاز الإلكتروني، التي تستهدفكِ كامرأة أولاً، وكمدافعة عن

حقـوق الإنسـان ثانيـاً. هـذه ليسـت مجـرد إزعاجـات عابـرة، بـل هـجمات مقصـودة هدفهـا إسـكاتكِ، زعزعـة ثقتـكِ، أو حتـى دفعـكِ للتوقـف عـن نشـاطكِ الحقوقـي.

لكـن لا تـنسي: لسـتِ وحـدكِ، وهنـاك خطـوات عمليـة يمكنـكِ اتخاذهـا للتقليـل مـن الأثـر وحمايـة نفسـكِ ومـن حولـكِ.

ماذا نقصد بالمضايقات والابتزاز الإلكتروني؟

المضايقات الإلكترونية: رسـائل متكـررة مزعجـة أو مهينـة، تعليقـات مسـيئة، أو تهديـدات علنيـة أو خاصـة.

الابتزاز الرقمي: محاولـة اسـتغلال معلومـات أو صـور شـخصية للضغـط عليـكِ، مقابـل مطالـب مثـل حـذف منشـورات، التوقـف عـن النشـاط، أو حتـى دفـع مبالـغ ماليـة.

"أول مرة وصلتني رسالة تهديد كانت بعد منشور بسيط عن حقوق المعتقلين... شعرت بالخوف، لكن بعدها قررت ألا أكون فريسة سهلة."

مدافعة من الانبار

كيف نواجه هذه التهديدات بخطوات ذكية وعملية؟

١. لا تردّي فوراً... ولكن لا تتجاهلي:

خـذي نفسـاً عميقـاً. الـرد العاطفـي قـد يـؤدي إلى التصعيـد. سـجّلي، وثّقـي، واحفظـي الرسـائل أو الصـور، ولا تحذفيهـا فـوراً — فقـد تكـون دلـيلاً لاحقـاً.

٢. فعّلي خاصية الحظر والتبليغ

في فيسـبوك، إنسـتغرام، تـويتر، تيليغـرام وغيرهـا، اسـتخدمي أدوات الحظـر والتبليـغ فـوراً. لا تترددي، فهـذه منصـات عامـة ولديـكِ الحـق الكامـل في الشـعور بالأمـان.

٣. احتفظي بالأدلة

قومي بتوثيق كل شيء: خذي لقطات شاشة (screenshot)، سجّلي الوقت والتاريخ، واحتفظي بالمحتوى الأصلي في مجلد مؤمن، سواء على جهاز مشفّر أو في تخزين سحابي آمن (مثل Proton Drive أو MEGA).

٤. استخدمي تطبيقات توثيق آمن مثل Tella

هذا التطبيق مصمم لتوثيق الانتهاكات بسرية وفعالية، حيث يمكنه إخفاء نفسه على الجهاز، وتشفير كل محتوى يتم توثيقه.

٥. غيّري إعدادات الخصوصية في حساباتك، واجعلي قائمة الأصدقاء/المتابعين محدودة، أوقفي ظهور حسابك في نتائج البحث، ولا تسمحي بتلقي رسائل من غير الأصدقاء/المتابعين الموثوقين.

٦. لا تتفاوضي مع المبتز

مهما كان الضغط كبيراً، لا تقعي في فخ الاستجابة. الابتزاز لا يتوقف غالباً بعد المرة الأولى.

٧. استعيني بدعم قانوني أو مؤسسي

ابحثي عن منظمات تقدم الدعم القانوني أو التقني. كثير من المؤسسات الحقوقية أو المختصين الرقميين يمكنهم مساعدتك في تقديم شكوى، أو التعامل مع المنصة أو الجهة الرسمية.

٨. أبلغي عن الابتزاز عبر المنصات أو السلطات

العديد من الدول، ومنها العراق وإقليم كوردستان، بدأت في تخصيص أقسام للجرائم الإلكترونية والابتزاز والتهديد والمضايقات الالكترونية. بإمكانكِ، إن توفرت حماية كافية، تقديم بلاغ رسمي. أو قد تكتفين بالتبليغ للمنصة

نصيحة من مدافعة:

المضايقة على الإنترنت كانت محاولة لكسر إرادتي، لكن التحصين الرقمي، والتوثيق، والدعم من زميلاتي، خلاني أرجع أقوى.

مدافعة من البصرة

فقـط حسـب الموقـف.

مساحة دعم: تذكري أنكِ لستِ السبب

أي فعـل عنفـي ضـدكِ، سـواء كان في الشـارع أو في الفضـاء الرقمـي، لا يُبرَّر أبـداً. المعتـدي هـو المخطئ، لا أنـتِ. تواصلي مـع صديقتـكِ، شـبكتكِ، منظمـة موثوقة، او السـلطات الأمنيـة والقضـاء في منطقتـك، ولا تعـتبري المواجهـة عبئـاً فردياً.

وقـد تبـدو اللحظـة التـي تتعـرضين فيهـا لابتـزاز أو مضايقـة رقميـة كأنهـا نقطـة انهيـار، خاصـة إن كنـتِ وحـدكِ أو لا تملـكين الدعـم الـكافي. لكـن الحقيقـة أن هنـاك شـبكات تضامـن، وخطـوط دعـم، ومنصـات حمايـة يمكـن أن تقـف معـكِ. لا ترددي في الحديـث مـع مـن تثـقين بهـن، سـواء مـن زميلاتـكِ، أو منـظمات المجتمـع المـدني، أو جهـات قانونيـة مؤمّنـة.

وأخيراً، الحمايـة الرقميـة ليسـت مجـرد مجموعـة مـن الأدوات، بـل هـي فعـل مسـتمر مـن العنايـة بالنفس، ومـن يسـتهدفكِ يعـرف جيـدًا تـأثيركِ... فلا تجعليهم

> "التهديد الرقمي لا يعني نهاية الطريق... بل بداية وعي جديد بكيفية الحماية، وبمن حولكِ من شبكات دعم وأمان."

يربحـون.

رابعا: توثيق انتهاكات حقوق الإنسان الرقمية

لأن الذاكرة لا تُخترق... بل تُقاوَم بالتوثيق

في كل مـرة تتعـرضين فيهـا لانتهـاك رقمـي، فـإن توثيـق مـا حـدث ليـس مجـرد إجـراء إداري أو خطـوة قانونيـة... بـل هـو فعـل مقاومـة، وأداة للعدالـة، ووسـيلة لحمايـة نفسـكِ والضحايـا المسـتهدفين مـن بعـدك.

في السـياق العراقـي، حيـث الإفلات مـن العقـاب شـائع في العـالم الرقمـي، يصبـح التوثيـق الرقمـي أداة قـوة، لكنـه يتطلـب دقـة، أمانـاً، وسـلوكاً واعيـاً في

جمـع الأدلـة.

لماذا يجب أن نوثّق؟

- لحماية نفسكِ وتثبيت حقوقكِ أمام الجهات المختصة.
- لدعم ضحايا آخرين قد يواجهون نفس النوع من الانتهاك.
- للمسـاهمة في بنـاء ملـف حقوقـي يُسـتخدم في حمـلات المنـاصرة أو التحقيقـات.
- لتوثيق التاريخ الرقمي للانتهاكات وعدم تركها تُمحى أو تُنكر.

ما الذي يجب توثيقه؟

عنـد تعرضـكِ (أو تعـرض أي زميلـة أو ضحيـة) لانتهـاك رقمـي، احـرصي على توثيـق الآتي:

- تاريخ ووقت الانتهاك بدقة.
- نوع الانتهاك (تهديد، اختراق، تشهير، ابتزاز...إلخ).
- المنصة أو التطبيق الذي تم عبره الانتهاك.
- الرسائل أو الروابط أو الصور أو أي مواد أُرسلت إليكِ.
- عنوان المرسل أو حسابه، إن أمكن.
- ردود فعلـكِ والإجـراءات التـي قمـتِ بهـا (تسـجيل خـروج، إبـلاغ، حـذف... إلخ).
- أي أضرار لاحقة (نفسية، قانونية، مهنية).

أدوات تساعدكِ في التوثيق الآمن:

- تطبيـق Tella: يوفـر مسـاحة آمنـة لتوثيـق الانتهـاكات بالصـور أو الفيديـو أو الملاحظـات، مـع خاصيـة التشـفير والإخفـاء والحـذف الآمـن.
- Proton Drive أو MEGA: لرفع وتخزين الأدلة بشكل مشفّر على السحابة.

- Screenshot مـع توقيـت الهاتـف: احـرصي عـلى أن تكـون لقطـة الشاشـة واضحـة وتُظهـر التاريـخ والوقـت.
- ملـف Word أو PDF موثّـق: اكتبـي فيـه تفاصيـل الانتهـاك واحتفظـي بـه في مـكان آمـن (يفضـل أن يكـون مشـفراً)

نصائح للسلامة أثناء التوثيق:

- لا تُشاركي الأدلة فورًا إلا مع جهات موثوقة.
- لا تحتفظي بالأدلة على الهاتف لفترة طويلة.

"حين وثّقت أول انتهاك تعرّضت له، شعرت أنني أستعيد شيئاً من قوتي."
مدافعة عن حقوق الإنسان من البصرة

- احرصي على التحقق من أن الجهاز الذي تستخدمينه آمن ومحدّث.
- حـاولي الفصـل بـين حسـاباتك الشـخصية وتلـك المخصصـة للتوثيـق أو المراسـلات الحقوقيـة.

التحقق من الأدلة الرقمية: أدوات موثوقة تحميكِ وتحمي الحقيقة

عندمـا تصلـكِ صـورة أو فيديـو يوثّـق انتهـاكًا مـا، قـد تشـعرين برغبـة فوريـة في مشـاركته أو اسـتخدامه. لكـن قبـل أي خطـوة، توقفـي للحظـة.

اسألي نفسك:

هـل هـذا المحتـوى موثـوق؟ هـل تـم التقاطـه مـن مـكان الحـدث فعـلًا؟ هـل يعـرض أحـدًا للخطـر؟

التحقـق مـن الأدلـة الرقميـة ليـس عمـلاً معقـدًا أو حكـرًا عـلى الخـبراء. بـل هـو مهـارة أساسـية لـكل مدافعـة عـن حقـوق الإنسـان، يمكنـكِ اكتسـابها تدريجيًـا، وهـي جـزء مهـم مـن حمايـة نفسـكِ ومـن توثقـين لهـم.

كيف أبدأ؟ إليكِ بعض الخطوات والأدوات البسيطة:

- ابدئي بالتفكير النقدي: من أرسل هذا؟ هل يتطابق مع روايات شهود آخرين؟ هل سبق أن رأيتِ هذا المحتوى في سياق مختلف؟
- تفقدي البيانات الخفية (metadata): بعض الصور والفيديوهات تحتفظ بمعلومات مثل الموقع الجغرافي ووقت التصوير. هذه البيانات قد تساعدكِ على التحقق، لكنها قد تكون خطيرة إن كشفت هوية المصدر. استخدميها بحذر.
- احذري من الصور أو الفيديوهات المفبركة: يمكنكِ استخدام أداة InVID (إضافة للمتصفح) أو خدمة Google Reverse Image Search للبحث عن النسخ الأصلية للمحتوى ومكان ظهوره لأول مرة. هذا يساعدكِ على كشف أي تزوير أو إعادة استخدام لمحتوى قديم في سياق جديد.
- استخدمي أدوات تحقق موثوقة:
  - YouVerify: أداة أطلقتها منظمة العفو الدولية تساعدكِ خطوة بخطوة في تحليل الصور والفيديوهات. مصممة خصيصًا لمساعدة المدافعين والمدافعات.
  - Tella: تطبيق آمن مفتوح المصدر، يتيح لكِ توثيق الانتهاكات (صور، فيديو، ملاحظات) بشكل مشفّر، دون كشف موقعكِ أو هويتكِ، ويمكنكِ إخفاؤه أو حذف محتواه بضغطة واحدة.
  - CheckShortURL: يساعدكِ على كشف الروابط المختصرة، لتعرفي ما الذي ستفتحينه قبل النقر عليه.
  - VirusTotal: موقع يمكنكِ من خلاله فحص أي ملف أو رابط قبل فتحه، للتأكد من خلوه من البرمجيات الخبيثة.

ملاحظات مهمة:

- لا تشاركي أي محتوى يمكن أن يعرّض الضحية للخطر أو يكشف موقعها أو هويتها، خاصة إذا لم تكن لديكِ موافقتها.
- يُفضّل دائمًا حفظ الأدلة الرقمية المشفّرة على تطبيقات مثل Proton

Drive أو MEGA أو ذاكـرة خارجيـة مشـفّرة باسـتخدام أدوات مثـل VeraCrypt.

- ضعـي حـدودًا لمـا تحتفظـين بـه عـلى هاتفـكِ؛ فالهاتـف قـد يُصـادر أو يتعـرض للاخـتراق.
- "التحقـق ليـس تشـكيكًا، بـل حمايـة... لـكل مـن التقـط الصـورة، ولـكل مـن سيسـتخدمها لاحقًـا."

بهـذه الخطـوات البسـيطة، سـتملكين أساسًـا متينًـا للتعامـل مـع الأدلـة الرقميـة. قـد لا تكـوني خـبيرة في التكنولوجيـا، لكنـكِ تملـكين الفطنـة والوعي—وهـذا يكفـي لتبـدأي في خلـق بيئـة رقميـة أكثر أمانًـا واحترافيـة في العمـل الحقوقـي.

خامسا: التهيئة للعمل في ظل انقطاع الإنترنت

في العـراق، قـد يحـدث انقطـاع الإنترنـت لأسـباب متعـددة: تقنيـة، أمنيـة، أو تنظيميـة، خاصـة خلال الفعاليـات الـكبرى أو فترات التوتـر. هـذا الانقطـاع يؤثـر على المدافعـات عـن حقـوق الإنسـان، ليـس فقـط خلال التظاهـرات او المواقـف الأخـرى التـي تتطلـب توثيـق وخاصـة التوثيـق الرقمـي، بـل أيضـاً أثنـاء توثيـق الانتهـاكات التـي تمـس النسـاء، والفتيـات، والأشـخاص مـن الفئـات المهمشـة في المجتمـع.

الاسـتعداد لهـذا الانقطـاع لا يعنـي مخالفـة القانـون أو تجـاوز المؤسسـات، بـل هـو جـزء مـن جهـود الحمايـة، والرصـد، والدفـاع عـن الحقـوق، وفقًـا لما تتيحـه القـوانين الوطنيـة والمعـايير الدوليـة التـي انضـم اليهـا العـراق، ومنهـا العهـد الـدولي الخـاص بالحقـوق المدنيـة والسياسـية، واتفاقيـة القضـاء على جميـع أشـكال التمييـز ضـد المـرأة (سـيداو).

كيف نستعد بطريقة آمنة ومسؤولة؟

- التخطيط المسبق:

حـمّلي الوثائـق، الـنماذج، والبيانـات التـي قـد تحتاجينهـا دون اتصـال، بمـا فيهـا أرقـام الجهـات الموثوقـة، مثـل فـرق الدعـم القانـوني أو المنـظمات التـي تقـدم خدمـات طـوارئ للمدافعـات عـن حقـوق الانسـان.

- استخدام أدوات مصممة لأغراض الحماية:

- تطبيق مثل Tella لا يُستخدم للتخفي، بل لحفظ الأدلة المتعلقة بالانتهاكات بشكل آمن ومسؤول، ويُشجَّع استخدامه في برامج حقوق الإنسان المدعومة من الأمم المتحدة والمنظمات الدولية.

- Bridgefy: في أوقات الطوارئ أو انقطاع الإنترنت، قد تحتاجين إلى وسيلة تواصل سريعة وآمنة مع فريقك أو زميلاتك المدافعات دون الاعتماد على الشبكة. هنا يأتي دور تطبيق Bridgefy، الذي يتيح إرسال الرسائل ونقل الملفات القصيرة حتى في حال غياب الإنترنت، باستخدام تقنية البلوتوث أو Wi-Fi المباشر.

بمعنى آخر:

- هاتفكِ يتصل مباشرة بهاتف شخص آخر قريب منك (حتى مسافة 100 متر تقريبًا)،
- ومن خلال سلسلة من الهواتف القريبة (شبكة Mesh)، يمكن للرسالة أن تنتقل لمسافات أبعد.

لماذا قد يفيدكِ هذا التطبيق؟

- يمكنكِ تنسيق تحركاتكِ أثناء التظاهرات أو الاجتماعات دون الحاجة للإنترنت.
- إرسال تنبيهات أو مشاركة ملفات صغيرة وصور مع الفريق في نفس الموقع.
- يعمل على أنظمة Android و iOS ولا يتطلب بيانات هاتف أو واي فاي عام.
- مثالي لتعزيز الأمان الجماعي في حالة الطوارئ.

ملاحظة: تأكدي دائمًا من تحميل التطبيق وتفعيله مسبقًا، لأن تحميل التطبيقات يحتاج إلى الاتصال بالإنترنت.

- إتاحة الوصول دون إنترنت:

- تطبيقـات مثـل Google Docs (مـع تفعيـل الوضـع غـير المتصـل)، أو تخزيـن الملفـات المشـفرة في أدوات مثـل Proton Drive أو MEGA تسـهّل اسـتمرار العمـل دون انقطـاع.
- وجود بدائل آمنة للاتصال الداخلي:

الاتفـاق على خطـة تواصـل بديلـة (مثـل إرسـال رسـالة قـصيرة أو اسـتخدام شريحـة هاتـف مـن شركـة ثانيـة) في حـال انقطـاع الإنترنـت.

لماذا كل ذلك؟

رصـد الانتهـاكات لا يعنـي دائمـا الاتهـام، بـل يعنـي العمـل بشـفافية، لتـوفير بيانـات دقيقـة يمكـن اسـتخدامها في المنـاصرة، الإبلاغ، وتطويـر سياسـات تحمـي الفئـات الأضعـف، خصوصًـا النسـاء والفتيـات، وتعزيـز وحمايـة حقـوق الانسـان الـذي هـو أسـاس عمـل المدافعـات عـن حقـوق الانسـان.

القسم الثالث: التخطيط للطوارئ الرقمية:

"عندما لا يكون الخطر «مفاجئًا"

في بيئـات العمـل التـي تسـودها المخاطـر، قد لا نلاحـظ دائمًـا التـغيرات التدريجية التـي تجعـل الوضـع أكثر خطـورة. الأمـر يشـبه الضفدعـة التـي إذا وُضعـت في مـاء يـغلي قفـزت فـورًا، لكنهـا إن وُضعـت في مـاء دافـئ يسـخن تدريجيًـا، قـد لا تـدرك الخطـر حتـى يفـوت الأوان. كذلـك نحـن، إن لم نقـم بتقييـم المخاطـر بشـكل دوري، فقـد نجـد أنفسـنا في محيـط لم يعـد آمنًـا دون أن ننتبـه لذلـك في الوقـت المناسـب

وفي العمـل الحقوقـي، وخاصـة في بيئـة كالتـي تعملـين فيهـا في العـراق أو إقليـم كوردسـتان، لا يكـون التهديـد الرقمـي شـيئًا عابـرًا أو اسـتثنائيًا، بـل واقعًـا متكـرّرًا. فقـد يحـدث أن تُفاجئـي برسـالة "تـم تغـيير كلمـة المـرور"، أو تجـدي نفسـك خـارج حسـابك فجـأة، أو يصـل إليـك رابـط مشـبوه في لحظـة انشـغال. وفي لحظـة واحـدة، كل شيء يصبـح مهـدداً: ملفاتـك، خصوصيتـك، وحتـى الأشـخاص الذيـن تعمـلين معهـم.

لكن ماذا لو كنتِ مستعدة؟

مـاذا لـو كانـت لديـكِ خطـة بسـيطة، مرنـة، تعـرفين كيـف تـتصرفين مـن خلالهـا عنـد وقـوع أي طـارئ رقمـي؟

إن **التخطيط للطوارئ الرقمية** لا يعني بالـضرورة امتـلاك معرفـة تقنيـة عاليـة، بـل يتعلّـق أكـثر بامتـلاك رؤيـة واضحـة وسـلوك وقـائي، يمكّنـكِ مـن تقليـل الـضرر، وحمايـة نفسـكِ ومـن حولـكِ، واسـتعادة نشـاطكِ بسرعـة.

"علّمتنا التجربة أن ردّ الفعل في اللحظات الحرجة لا يُبنى في اللحظة نفسها، بل قبلها بكثير."

مدافعة من بغداد

سـواء كنـتِ تعمـلين بمفـردكِ أو ضمـن فريـق أو منظمـة، هـذا القسـم مـن الدليـل سـيمنحك الأدوات الأساسـية لتكويـن خطـة طـوارئ رقميـة تكـون بمثابـة "درع خفـي" وقـت الأزمـات.

خطوتكِ الأولى: إعداد خطة الاستجابة للهجمات الإلكترونية:

لماذا نحتاج إلى خطة استجابة للهجمات الإلكترونية؟

الاختراق ليـس مجـرد احـتمال... بـل واقـع يتكـرر، وبتنـا نـراه يُصيـب زميلـةً هنـا، ومؤسسـةً هنـاك. لا أحـد في مأمـن تـام. لكـن الفـرق بين مـن ينهـار تحـت أول صدمـة، ومـن يسـتطيع الوقـوف مـن جديـد، غالبًـا مـا يكـون شـيئًا بسـيطًا: وجـود خطـة.

خطة الاستجابة للهجمات الإلكترونية ليست ترفًا تقنيًا، وليست شيئًا «للمتخصصين فقـط». هـي خارطـة طريـق بسـيطة، لكنهـا تنقـذك في لحظـة ارتبـاك. تُسـاعدك على حمايـة نفسـكِ، ومـن تعمـلين لأجلهـم، وتحافـظ على مصداقيتـكِ وثقتـكِ في وقـت تكـون فيـه أعصابـكِ تحـت ضغـط كـبير.

في سـياق العمـل الحقوقـي في العـراق، حيـث تتداخـل الانتهـاكات الرقميـة مـع محـاولات التخويـف والتشـويه، فـإن وجـود خطـة اسـتجابة يُعـدّ أحـد أشـكال التمـكين الـذاتي. هـو فعـل دفـاع، ووعـي، واسـتعداد... لا مـن أجلـكِ فقـط، بـل

مـن أجـل الضحايـا والمجتمـع الـذي تدافـعين عنـه.

أحيانًا لا يكـون السـؤال "هل سـأتعرض لهجـوم إلـكتروني؟"، بل "متى سـيحدث؟"، وكيف سـأتصرف عندمـا يحدث؟

"حين تتعرضين لهجوم رقمي، يكون أسوأ ما قد يحدث هو أن تبدأي من الصفر، بلا خطة، بلا نسخة احتياطية، بلا شبكة أمان."

مدافعة من البصرة

لذلك، لا بدّ من خطة استجابة يتم تجهيزها مسبقًا، لا بعد وقوع الحادث.

لكـن قبـل ذلـك .. يجـب ان تـدركي المخاطـر الرقميـة والية تحليـل هـذه المخاطـر والتهديدات.

تحليل المخاطر الرقمية: بوابة الفهم والاستعداد

لا يمكننـا مواجهـة مـا لا نفهمـه. والتحليـل الجيـد للمخاطـر الرقميـة هـو بمثابـة الخريطـة التـي تُظهـر لنـا مكامـن الضعـف والتهديـد، وتكشـف قدراتنـا ومـا ينقصنـا مـن أدوات ومهـارات. لـكل مدافعـة عـن حقـوق الإنسـان، ولـكل مؤسسـة تعمـل في هـذا المجـال، تحليـل المخاطـر الرقميـة هـو نقطـة الانـطلاق نحـو بنـاء حمايـة رقميـة واقعيـة وفعّالـة.

ما هو تحليل المخاطر الرقمية؟

تحليـل المخاطـر هـو أداة بسـيطة لكنهـا فعّالـة تسـاعدكِ على تقييـم وضعـكِ الرقمـي مـن حيـث:

- ما هي التهديدات المباشرة او المحتملة التي قد تواجهينها؟

"عندما بدأتُ أفكر في من قد يستهدفني، وكيف، وبأي وسيلة... بدأتُ أفهم ما الذي يجب أن أتعلمه، وأين أركز جهودي."

مدافعة من بغداد

- ما هي نقاط الضعف في أجهزتكِ، حساباتكِ، أو سلوككِ الرقمي؟
- ما هي قدراتكِ أو قدرات مؤسستكِ على مواجهة هذه التهديدات؟

هـذا التقييـم والاجابـة على هـذه الأسـئلة الـثلاث سـتعطيك الإجابـة على اهـم سـؤال وهـو **(ما هي الاحتياجات التي يجب العمل عليها والتي انا في حاجة اليها على المستوى القريب او البعيد؟)**

المخاطر	نقاط الضعف	القدرات المتاحة	القدرات التي يتعين الحصول عليها

أدوات بسيطة تساعدكِ في تحليل المخاطر:

- اسـتمارة تقييـم ذاتي: تتضمـن أسـئلة مثـل المذكـورة أعـلاه، وتُراجعهـا المدافعـة كل ٦ أشـهر.
- هـذا نمـوذج بسـيط للاسـتمارة التـي مـن الممكـن الاعتـماد عليهـا حتـى بالنسـبة للتقييـم المؤسسـاتي

المخاطر	نقاط الضعف	القدرات المتاحة	القدرات التي يتعين الحصول عليها
فقدان المعلومات الخاصـة بعمـل المنظمة و نشـا طا تها	عـدم المعرفـة والالمام بمواضيـع الحمايـة الرقميـة	لا توجد	تدريـب الموظـفين على الحمايـة الرقميـة
	وجـود المعلومـات المتعلقـة بالمنظمـة ومشـاريعها وكل المعلومـات عـن المسـتفيدين في حواسـيب غير امنـة		شراء أجهـزة خاصـة بحفـظ المعلومـات غير مرتبطـة بالأنترنـت

وعـلى أسـاس ان الاحتيـاج هـو الأسـاس الـذي مـن الممكـن ان نبنـي عليـه ايـة خطـة فقـد يمكـن ان يسـتوحى ممـن هـذا الجـدول المعادلـة التاليـة:

الاحتياجات بالنسبة للمخاطر = نقاط الضعف – القدرات المتاحة

وهذا نموذج للاستمارة يمكن الاستفادة منه في اعتماد التحليل:

- جلسـة جماعيـة مـع الفريـق: لمراجعـة سـيناريوهات الهجـمات وتحديـث الإجـراءات.
- مصفوفـة بسـيطة (اختيـاري): تقومـي بتصنيـف التهديـدات حسـب «درجـة الخطـورة» و»مـدى التكـرار».
- التحليـل ليـس مهمـة لمـرة واحـدة. هـو ممارسـة يجـب تكرارهـا دوريًـا لتبقـى الحمايـة مسـتجيبة للتغـيرات.

لماذا هذا التحليل مهم؟

لأنـه يجنّبـكِ اتبـاع إجـراءات حمايـة غير ملائمـة لحالتـكِ، ويوفـر الوقـت والطاقـة لتطويـر مـا هـو فـعلاً ضروري لـكِ. كما أنـه يسـاعدكِ على طلـب الدعـم مـن الآخريـن (مـدربين، منـظمات، مانـحين) بنـاءً على احتياجـات حقيقيـة وليـس افتراضـات عامـة.

في هذا القسـم، سنرشـدكِ، خطـوة بخطـوة، لوضع خطة اسـتجابة على مسـتويين: شـخصي ومؤسسـاتي. وسـنقدّم لـكِ أدوات وممارسـات وتجـارب حقيقيـة تُظهـر أن الوقايـة ليسـت صعبـة، بـل تبـدأ مـن وعـي صـغير يمكـن أن يُحـدث فرقًـا كـبيراً.

أولًا: على المستوى الشخصي:

لا يجـب أن تكـون الخطـة معقـدة، بـل بسـيطة، مكتوبـة، ويمكـن الوصـول إليهـا عنـد الحاجـة.

ماذا يجب أن تتضمن خطتكِ الشخصية؟

فكّري في أكثر ما قد تتعرضين له، واعملي على أساسه ما يلي:

١. قائمة سريعة بالأشياء التي يجب فعلها فورًا:

- تغيير كلمات المرور (ابدئي بالحسابات الحساسة: Gmail، فيسبوك، Telegram...).
- تفعيل التحقق بخطوتين (إذا لم تكن مفعّلة سابقًا).
- إعلام المؤسسة او أي منظمة متخصصة ضمن شبكة علاقاتك او صديقة موثوقة أو زميلة حقوقية بأنك تعرضت لهجوم.
- استخدام جهاز نظيف (لم يُخترق) لإدارة الأزمة.

٢. خط اتصال بديل في حالة الطوارئ:

- جهزي بريدًا إلكترونيًا احتياطيًا وهاتفًا بديلًا أو حتى حسابًا ثانويًا لتواصلكِ مع فريقكِ عند الطوارئ.

٣. خطة لاسترجاع الحسابات:

- خزّني أسئلة الاستعادة وكلمات السر الاحتياطية في تطبيق آمن مثل Bitwarden.
- احتفظي بنسخة مشفرة لكلمات المرور الأساسية في Veracrypt أو عبر Proton Drive او Mega.

٤. تطبيقات مهمة تساعدكِ عند الاستجابة السريعة:

- Have I Been Pwned: لفحص ما إذا تم تسريب بريدك الإلكتروني أو كلمة المرور.

"أول مرة تم اختراق حسابي كنت في حالة صدمة، لم أعرف من أين أبدأ. الآن لديّ خطة أرجع لها مباشرة، وأعرف كيف أتصرف."

مدافعة من النجف

- VirusTotal: لفحص الروابط أو الملفات المشبوهة.
- Signal: لتواصلكِ الآمن مع الأشخاص الموثوقين أثناء الهجوم.
- Tella: لتوثيق الهجوم إن كان يستهدفكِ كمدافعة أو ناشطة.

ثانيًا: على المستوى المؤسساتي:

"حين وقع الاختراق، لم نكن نعرف كيف نرد. الآن، لدينا ملف بسيط ومكتوب، نطبّقه فورًا. ونعرف من نتصل به."
مدافعة في منظمة من السليمانية

حتى المؤسسة الصغيرة، أو الفريق التطوعي، يحتاج إلى خطة. لأنه حين يتم اختراق البريد الرسمي، أو سرقة بيانات المستفيدات، فإن الضرر قد يشمل الجميع.

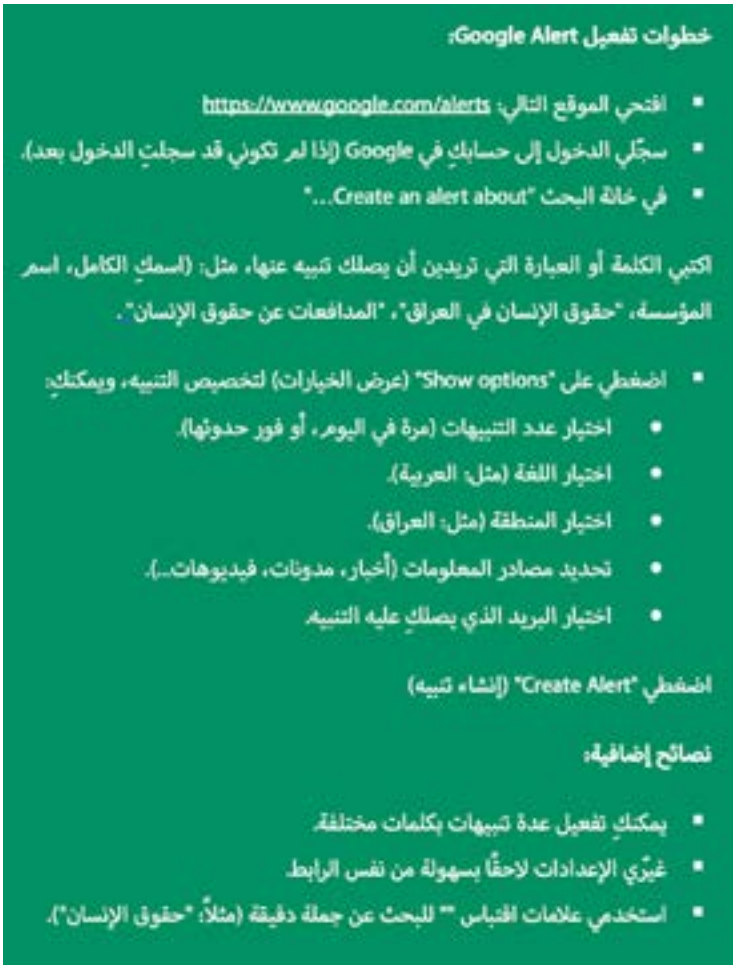
عناصر أساسية في خطة استجابة مؤسسية:

١. وضع سياسة للمنظمة تختص بتحليل والاستجابة للمخاطر الرقمية تكون معتمدة من قبلها وتقوم بتحديثها بمراحل دورية.

٢. فريق الطوارئ الرقمي داخل المؤسسة:

حددي شخصًا مسؤولًا عن الأمن الرقمي، أو شكّلي فريقًا مصغرًا (حتى لو من متطوعين) يتولى التصرف فورًا عند وقوع حادث.

٣. قائمة بالأدوات والبريد البديل:



- حساب بديل للطوارئ لاستخدامه عند تعطل الحسابات الرسمية.
- تفعيل أدوات مثل Google Alert لمراقبة ذكر اسم المؤسسة في أي سياق غير اعتيادي.
- إعداد Bitwarden Teams أو أي مدير كلمات مرور مؤسسي.

٤. خطة إعلامية داخلية:

- كيف ستتواصل المؤسسة داخليًا عند حدوث هجوم؟
- استخدام قناة مشفرة مثل Wire أو Signal Group مغلق للطوارئ.

- تحديد ناطق رسمي داخلي للإبلاغ عن الوضع.

٥. خطة حماية للبيانات الحساسة:

- تخزين البيانات على Proton Drive أو Mega مشفر.
- نسخ احتياطي تلقائي كل أسبوع.
- تقييد الوصول للبيانات بحسب الدور الوظيفي.

٦. تدريب دوري على الاستجابة للهجمات:

- نظّمي «محاكاة» كل ٣-٦ أشهر مع فريقكِ:
  - ماذا لو تم اختراق حساب المؤسسة؟
  - ماذا لو تم تسريب ملف يحتوي بيانات حساسة؟

الهدف من المحاكاة هو اكتساب الثقة والسرعة في التعامل.

٧. تحديد الجهات التي يمكن طلب الدعم منها:

- منظمات داعمة مثل Access Now (خدمة الطوارئ)، Front Line Defenders، أو Digital First Aid Kit.

"حينما تعرضتُ لحملة تشهير بعد تغطيتي لمظاهرة في البصرة، كان منقذي الأول رسالة سريعة إلى إحدى الصديقات في منظمة دولية. لم تحلّ كل شيء، لكنها منعت الأسوأ."

مدافعة من البصرة

- خبراء محليون أو شبكات أمان رقمية داعمة في العراق أو الإقليم.

ويمكنك الاطلاع على القسم الأخير من الدليل المتعلق ب (مراجع وموارد إضافية فيها اهم المنظمات الدولية والمحلية التي تقدم الخدمات للمدافعات عن حقوق الانسان في حالات الطوارئ)

خطوتك الثانية: بناء شبكات دعم وتعاون مع جهات محلية ودولية لحالات

الطوارئ

لا يمكـن أن تخـوض المدافعـة عـن حقـوق الإنسـان معركتهـا الرقميـة بمفردهـا. في بيئـة عاليـة المخاطـر، يصبـح وجـود شـبكة دعـم موثوقـة أحـد أهـم أدوات الحمايـة.

في حـالات الطـوارئ الرقميـة، مثـل التعـرض لاختراق، ابتـزاز، تسريـب معلومـات حساسـة، أو حـملات تشـهير واسـعة، فـإن سرعـة الـردّ واتسـاع نطـاق الدعـم

تذكّري:

لا تنتظري وقوع الأزمة لبناء الشبكة، فالوقت في الأزمات الرقمية ثمين.
أعدّي قائمة بالأشخاص أو الجهات الذين يمكن الوثوق بهم، وحدثيها دوريًا.
لا تشاركي معلومات حساسة عن نفسكِ أو غيركِ إلا بعد التأكد من هوية الجهة وتدابير الأمان المتبعة.

يمكـن أن يصنعـا الفـارق بين الأزمـة والكارثـة.

لذلـك، مـن الضروري العمـل على بنـاء شـبكة مسـاندة تتنـوع مـا بين الدعـم التقنـي والقانـوني والنـفسي، وتتضمـن أفـرادًا ومؤسسـات محليـة واقليميـة و ودوليـة يمكـن التواصـل معهـم في الأزمـات.

كيف تبنين شبكة دعم فعّالة؟

- حددي جهات الدعم المحلية:

ابحثـي عـن منظـمات مجتمـع مـدني، فـرق الدعـم الرقمـي، أو مجموعـات نسـوية تقنيـة داخـل العـراق تسـتطيعين التواصـل معهـا في حـال وقـوع تهديـد أو اختـراق. تأكـدي مـن موثوقيتهـا، والتزمـي بالحفاظ عـلى خصوصية المعلومـات المتبادلـة. مثـل

- ابنـي علاقـات مـع منظـمات دوليـة وإقليميـة متخصصـة: مثـل ، SMEX Front Line Defenders ، Access Now ، Digital Defenders Partnership (DDP))، والتـي تقـدّم دعـمًا تقنيًـا وأمنيًـا وقانونيًـا للمدافعـين/ات في حـالات الطـوارئ. بعـض هـذه الجهـات توفـر نمـاذج تدخـل سريعـة يمكـن تعبئتهـا عنـد وقـوع حـادث. وسـوف نوردهـا كلهـا في القسـم الأخـير مـن الدليـل.

- تواصلي مع شبكات نسوية عابرة للحدود: مثل شبكة «Urgent Action Fund» أو «AWID»، فهذه الجهات لا تقدم فقط الدعم العاجل، بل تتيح أيضًا مساحة للتضامن والتعلّم من تجارب الأخريات.

- اعملي على مأسسة الدعم داخل مؤسستك: من خلال تعيين «نقطة اتصال طوارئ رقمية»، وتوثيق جهات الاتصال، وخطوات الاستجابة الأولية، وتدريب الفريق على كيفية طلب الدعم الخارجي في حال عدم توفر الإمكانيات داخليًا.

- فكري بمن يمكنه رفع صوتكِ دوليًا: من الممكن أن تتعرضي لانتهاك يحتاج إلى «تدويل» القضية كوسيلة ضغط وحماية. لذلك، من المهم معرفة صحفيات، باحثات، أو منظمات ضغط دولي يمكن إبلاغها، مع مراعاة التوقيت المناسب وعدم تعريض أي طرف للخطر.

5. المراجع والمصادر والموارد الإضافية:

لأن المعرفة قوة... وهذه القوة يجب أن تكون في متناول يديكِ.

نعرض لكِ هنا مجموعة مختارة من الأدلة، الأدوات، والمنصات التي يمكن أن تساعدكِ على تعزيز مهاراتكِ في الحماية الرقمية، فهم التهديدات، وتعلّم كيفية الاستجابة لها. هذه الموارد متاحة مجانًا، ومُعتمدة من منظمات دولية اقليمية موثوقة في مجال حماية المدافعات والمدافعين عن حقوق الإنسان.

أولا: شبكات رقمية آمنة ومجتمعات دعم نسوية

- منصة دعم السلامة الرقمية – سميكس
  الموقع الالكتروني: https://smex.org/helpdesk
- مؤسسة أنسم للحقوق الرقمية
  البريد الإلكتروني: report@insm-iq.org

  الرقم المخصص عبر واتساب: +9647835882244

  www.insm-iq.org
- Digital Defenders Partnership – دعم الاستجابة السريعة في حالات الطوارئ.
  الموقع الالكتروني: www.digitaldefenders.org

- Access Now – Helpline - دعم مباشر لحوادث الأمان الرقمي.
الموقع الالكتروني: www.accessnow.org/help
- Front Line Defenders – الدعم العاجل والمرافقة الرقمية
الموقع الالكتروني: www.frontlinedefenders.org/en/get-help
- The Engine Room - تقدم دعمًا رقميًا تقنيًا ومنهجيًا للمنظمات النسوية والمدافعات.
الموقع الالكتروني: www.theengineroom.org

ثانيا: مصادر تعليمية ومرجعية حول الأمن الرقمي وحقوق الإنسان

- Security in a Box – Tactical Tech - دليل الحماية الرقمية للمدافعات/ين.
الموقع: https://securityinabox.org
- Digital First Aid Kit – Access Now - استجابات أولية لحالات الطوارئ الرقمية.
الموقع: https://digitalfirstaid.org
- TOTEM Project - منصة دورات إلكترونية في الحماية الرقمية والتوثيق.
الموقع: https://totem-project.org
- Front Line Defenders – دليل الأمان الشخصي والمؤسسي
الموقع: https://www.frontlinedefenders.org/en/resource-centre
- DefendDefenders – الدليل الرقمي للمدافعات/ين في أفريقيا والشرق الأوسط
الموقع: https://www.defenddefenders.org/resources
- Securityplanner – لوضع خطة سلامة رقمية خاصة.
الموقع: https://securityplanner.consumerreports.org

ادلة وتدريبات:

- https://riseup.net/en/security/device-security

- https://securityplanner.consumerreports.org/statements/
- https://citizenevidence.org/2020/06/03/protecting-protester-privacy-against-police-surveillance/
- https://www.frontlinedefenders.org/en/resources-hrds
- https://securityinabox.org/ar/
- https://digitalfirstaid.org/ar/
- https://cpj.org/ar/2020/01/post-550/
- https://www.hacksplaining.com/lessons
- https://www.privacytools.io/
- https://ssd.eff.org/ar/
- https://advocacyassembly.org/ar/courses?count=24
- https://gcatoolkit.org/
- https://datadetoxkit.org/ar/home

الخاتمة:

في الختام: هذا الدليل... لكِ

في كل خطوة من هذا الدليل، حاولنا أن نضع يدنا في يدكِ. لم يكن الغرض فقط أن تتعلمي كيف تؤمّنين جهازكِ، أو تحذفي بياناتكِ، أو تستخدمي تطبيقًا مشفّرًا، بل أن نمنحكِ ما هو أعمق: شعور بالأمان في عالمٍ رقميٍ قاسٍ، وأدوات تمنحكِ القوة بدل الخوف، والمعرفة بدل التردد.

هذا الدليل لم يُكتب بلغة تقنية باردة، بل بلغة مدافعة لمدافعة. كتفًا بكتف، لأننا نعرف أن حمايةَ نفسكِ الرقمية ليست مجرد سلوك، بل قرار يومي بالاستمرار، رغم التهديد، رغم التشهير، رغم من يحاول أن يجعل وجودكِ صعبًا.

نعرف أن كل رسالة تهديد، كل صورة مُفبركة، كل اختراق، ليس مجرد حادث، بل محاولة لإسكاتكِ...

لكننا نؤمن أنكِ لن تصمتي.

تعلمنا هنا كيف:

نحول الحماية الرقمية إلى روتين يومي.

نستخدم أدوات وتطبيقات تجعلنا أقل هشاشة وأكثر مرونة.

نتصرف بذكاء في الأزمات، ونخطط قبل أن تشتعل الطوارئ.

نربط التقنية بالمعنى، والمعلومة بالكرامة.

لا تدعي كثرة التفاصيل تُثقل قلبكِ. خذي من هذا الدليل ما تحتاجينه اليوم، وعودي إليه كلما شعرتِ أنكِ بحاجة إلى بوصلة في هذا العالم الرقمي المتسارع.

تذكّري:

أنتِ لستِ وحدكِ.

صوتكِ مهم.

ومقاومتكِ الرقمية... فعل نضال

"أدركت أن حماية نفسي هي أيضاً حماية لضحايا الانتهاكات، وزميلاتي، والمؤسسات التي نؤمن بها. المسألة لم تعد فقط أن أكون آمنة، بل أن أكون مستعدة."

مدافعة شاركت في مراجعة الدليل

شكر وتقدير:

يتقـدم فريـق إعـداد هـذا الدليـل بخالـص الشـكر والتقديـر لـكل مـن سـاهم في إنجـازه، دعمًا للمدافعـات عـن حقـوق الإنسـان في العـراق وتعزيـزًا لحمايتهـن في الفضـاء الرقمـي.

نخـصّ بالشـكر منظمـة (SMEX (Social Media Exchange، الجهـة الممولـة لهـذا المـشروع، عـلى دعمهـا المتواصـل والتزامهـا بتمكـين المدافعـات عـن حقـوق الإنسـان وتعزيـز الحقـوق الرقميـة في منطقـة غـرب آسـيا وشـمال أفريقيـا. لقـد كان لثقتهـا ودعمهـا أثـرٌ بالـغ في تحويـل هـذا العمـل مـن فكـرة إلى دليـل عمـلي يضـع السـلامة الرقميـة في متنـاول مـن هـنّ بأمـسّ الحاجـة إليهـا.

كما نوجّـه خالـص الشـكر والتقديـر إلى نـانسي عـود، منسـقة الحمايـة السـابقة في الشرق الأوسـط في منظمـة «فرونـت لايـن ديفنـدرز»، ومديـرة المشروع حكمـت علامي اللتان سـاعدتا من خلال مشـاركتهما في المقـابلات مع المدافعـات العراقيات في تسـليط الضـوء على واقعهـن، وسـاهمت في تعميـق فهـم السـياق المـحلي والديناميكيـات المحيطـة بـه.

كما نثمّـن كل مـن شـاركت أو سـاهمت بشـهادة، أو مراجعـة، أو تجربـة، أو فكـرة، أو ملاحظـة. هـذا الدليـل ليـس مجـرّد نصـوص وأدوات، بـل هـو حصيلـة ذاكـرة جماعيـة وتضامـن نسـويّ ومهنـيّ مـن أجـل أمـان جميـع مـن اختـارت أن ترفـع صوتهـا دفاعًـا عـن العدالـة وحقـوق الإنسـان.

إلى كل مـن يعمـل في الخطـوط الأماميـة للدفـاع عـن حقـوق الإنسـان، هـذا الدليـل أُعـدّ لأجلكـم، وبصوتكـم، ومـن أجلكـم جميعًـا.

نؤمـن أن التضامـن الرقمـي هـو امتـداد للتضامـن الإنسـاني، وأن كل خطـوة في طريـق البيئـة الرقميـة الامنـة هـي خطـوة نحـو حريـة أكبر وعدالـة أوسـع.

وليد علي | إقليم كوردستان - العراق

محامٍ ومدافع عن حقوق الانسان من إقليم كوردستان-العراق. يشغل حالياً رئيس منظمة «سلامتك» للدفاع عن حقوق الإنسان» في العراق، وخبيراً قانونياً لدى نقابة المحامين الامريكية (ABA)-مركز حقوق الانسان في الشرق الأوسط وشمال أفريقيا. يتميز بخبرة ميدانية في تقديم الاستشارات القانونية والرقمية للمدافعين/ات عن حقوق الإنسان، وبالمشاركة في توثيق انتهاكات حقوق الإنسان في العراق. كما يقدم تدريبات متخصص في مراقبة المحاكمات، الحقوق الرقمية، تحليل المخاطر والتهديدات وأدوات الاستجابة للمدافعين، مساهمًا في بناء قدرات المجتمع المدني والمدافعين عن حقوق الانسان.

راية شاربين | الأردن

منسقة تربوية وخبيرة في أمن الإنترنت والحماية الرقمية، تعمل حاليًا مع منظمة «تور TOR» غير الربحية التي تعنى بمكافحة المراقبة والرقابة على الإنترنت، حيث تُدير برامج تدريبية مخصصة للصحفيين والمدافعات عن حقوق الإنسان لتعزيز قدراتهم في بيئات رقمية آمنة. تعمل أيضًا كزميلة بحثية في مختبر Citizen Lab بجامعة تورونتو، حيث يتركز بحثها على تحليل الأجهزة الرقمية وأنظمة المراقبة المستهدفة. كما تعاونت سابقًا مع مؤسسة "روري بيك" للصحفيين المستقلين كمستشارة أمنية، ومع الجمعية الأردنية للمصدر المفتوح كمنسقة برامج، مساهمةً في تصميم وتنفيذ أنشطة مبتكرة لتعزيز الأمن الرقمي وحرية التعبير.

نبذة عن منظمة SMEX

SMEX «سمكس» هي منظمة غير ربحيّة تسعى إلى النهوض والدفاع عن حقوق الإنسان في العالم الرقمي في منطقة غرب آسيا وشمال إفريقيا.

تتمثّل رؤيتها في أن يكون كلّ فردٍ في منطقة غرب آسيا وشمال أفريقيا وخارجها قادراً على الوصول إلى الإنترنت وشبكات الاتصالات وغيرها من المساحات المترابطة الأخرى، من أجل التواصل والتعبير بأمان وبدون قلق الرقابة الذاتية، ورقابة الحكومات، وتداعيات التعبير على الانترنت.

وتعمل على تعزيز حرية التعبير والحق في الخصوصيّة، وذلك عن طريق الأبحاث، والتقارير، ومراقبة السياسات التي تتبنّاها الحكومات وشركات التكنولوجيا، وحماية سلامة وأمن المستخدمين/ات على الإنترنت، والتعاون مع مناصري/ات هذه الحقوق في المنطقة في سبيل الوصول إلى فضاءٍ رقمي أكثر أماناً.

info@smex.org

https://www.facebook.com/smex/

https://www.instagram.com/smexorg/

نبذة عن منظمة SODHR

منظمة سلامتك للدفاع عن حقوق الإنسان (SODHR) هي منظمة غير حكومية مجازة من قبل الأمانة العامة لمجلس الوزراء، إدارة المنظمات غير الحكومية في العراق. تأسست في أكتوبر ٢٠٢٢ من قبل مجموعة من المدافعين عن حقوق الإنسان في مختلف مناطق العراق، وتعمل في مجال الحقوق الرقمية وحماية المدافعين عن حقوق الإنسان في مواضيع مختلفة مثل مراقبة المحاكمات، والحماية الرقمية، وتقديم دراسات حول التشريعات المتعلقة بالحقوق والحريات في العراق.

تتمثل رؤيتها بالأمان الرقمي للجميع، بحيث يتمتع المجتمع العراقي بالحقوق الرقمية وجميع حقوق الإنسان في الفضاء الرقمي.

info@salamtakorganization.org

https://www.instagram.com/salamtakorganization/


SMEX


SODHR NGO