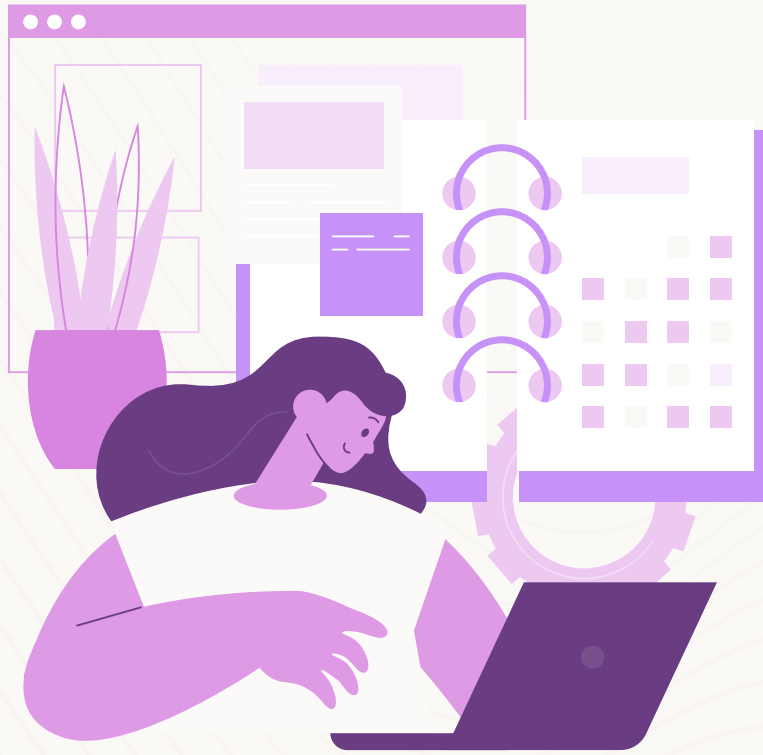


دليل المناصرة الرقمية النسوية المؤثرة في اليمن والمنطقة العربية



مستشارة الحماية والأمن الرقمي:
نور خالد

إعداد وتطوير المحتوى: غدير طيرة
(ناشطة نسوية، صحفية ومنتجة مستقلة،
عضوة في مشروع تعزيز الحركة النسوية وشبكة التضامن النسوي)

الجهات المصدرة والشركاء:

مبادرة مسار السلام (Peace Track Initiative) - مبادرة ومن امباكت

تمويل الإصدار:

تم إنتاج هذا الدليل ضمن مشروع «تعزيز الحركة النسوية والمبادرات لبناء سلام شامل في اليمن»، والذي تنفذه مبادرة مسار السلام (Peace Track Initiative) بتمويل من سفارة هولندا لدى اليمن، وتحت مظلة الخطة الاستراتيجية الخمسية لشبكة التضامن النسوي (٢٠٢٣-٢٠٣٠) - المسار الثاني المكرس لتعزيز القيادة النسوية وبناء سردية نسوية يمنية مؤثرة.



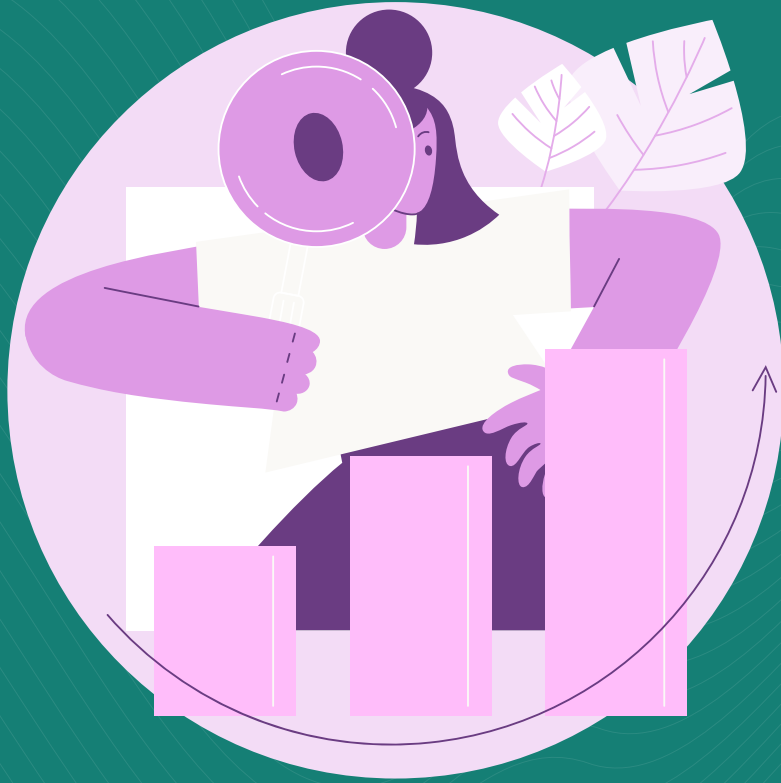
Embassy of the
Kingdom of the Netherlands

الفهرس



6-1	القسم التمهيدي والإطار المفاهيمي
2	- المقدمة والتمهيد: سد الفجوة بين العمل الميداني والأمان الرقمي
3	- الشكر والتقدير الرسمي: الشراكات والالتزام المؤسسي لشبكة التضامن النسوي
4	- إخلاء المسؤولية القانوني والفني والفهرس العام للدليل
5-6	- مدخل مفاهيمي: المفاهيم الأساسية للمناصرة والسردية البديلة
15-8	الفصل الأول: السرد والحضور الرقمي للنساء - السيادة الرقمية وتصميم وإطلاق السرديات البديلة
8	- السرد الرقمي كمساحة سيادية وتفكيك الفجوة الحقوقية في سياق بيئات النزاع
9	- تفكيك الفجوة بين العمل الميداني والمهارات التقنية للمدافعات
10	- قوة القصة الصحفية الإنسانية ومخطط ركائز هندسة البناء القصصي
11	- أدوات صياغة القصة (البساطة، الأنسنة، الدقة الحقوقية) والمعايير الأخلاقية
12	- الأبعاد الأخلاقية والمعايير الحمائية في الصحافة النسوية
13	- التكتيكات الفنية للدمج الذي للوسائط البسيطة والإنفوجرافيك والاقتراسات
14	- تفكيك وفهم حملات التشويه والتضليل الإعلامي الجندري
15-16	- المرجع الميداني لإدارة الأزمات والرد السردية التضامني
27-18	الفصل الثاني: التخطيط الاستراتيجي لحملات المناصرة النسوية الرقمية
18	- مدخل إلى التخطيط الاستراتيجي لحملات المناصرة النسوية الرقمية وسد الفجوة الميدانية
19	- تحديد القضية وتفكيك المشكلة المجتمعية باستخدام منهجية شجرة المشكلات
20	- تطوير السردية وصياغة قضية الحملة وجمع الأدلة الميدانية الموثقة
21	- صياغة الأهداف الاستراتيجية والمرحلية وتطبيق معادلة الأهداف الذكية (SMART)
22	- رسم رحلة تفاعل الجمهور وحشد الدعم وتوجيه السلوك الرقمي للمستخدم
23	- مصفوفة تحليل وتحديد أصحاب المصلحة والجمهور المستهدف (حلفاء ومحايدين وخصوم)
24	- هندسة تكتيكات الحملة الرقمية وبناء هويتها وعلامتها البصرية ودلالات الألوان
25	- إنتاج وإدارة محتوى الحملة وجدولته وتكتيك الأمواج في النشر الرقمي
26	- قواعد التشبيك الرقمي وبناء الرسائل السياسية والحقوقية لصناع القرار والبعثات الدولية
27	- قائمة فحص فاعلية وجاهزية الحملة قبل الإطلاق الفعلي
36-40	الفصل الثالث: الأمان الرقمي والحماية الشاملة
27	- مدخل ومفاهيم أساسية في الأمان الرقمي
28	- إدارة الهوية الرقمية
29	- تحصين الحسابات وإعدادات الخصوصية المتقدمة
30	- المرونة الرقمية أثناء انقطاع الإنترنت
31	- بروتوكول المرور من النقاط الأمنية والتفتيش العشوائي
34	- جدار الحماية الذاتي (شبكات VPN والشبكات العامة)
35	- مواجهة الابتزاز الرقمي الموجه (الجانب التقني)
36	- مواجهة حملات التشويه الممنهجة والجيش الإلكتروني (الذباب الرقمي)
37	- كسر العزلة الرقمية وبناء شبكة الدعم والمساندة المتخصصة
39	- توثيق الأدلة وحفظ الحقوق (الجانب التقني والقانوني)

المقدمة والتمهيد



"سلامتك الرقمية هي ركيزة حضورك وسمودك الميداني؛
فحماية صوتك وإدارته بوعي تتجاوز حدود الإجراءات التقنية المعتادة
لتصبح استراتيجية أصيلة تضمن أثرك وتصنع المستقبل بأمان."

تمهيد: سد الفجوة بين العمل الميداني والأمان الرقمي

في ظل النزاع الممتد في اليمن والمنطقة العربية، تؤدي النساء أدواراً قيادية مزدوجة؛ فبينما يواجهن واقعاً ميدانياً معقداً لانتزاع الحقوق الأساسية وبناء السلام، يخضن في الفضاء الرقمي مواجهة لا تقل ضراوة ضد محاولات الإقصاء، وتشويه المسيرة الحقوقية، والتشهير الممنهج. إن الفجوة بين جسارة الأداء الميداني وافتقار بعض الناشطات لأدوات الحماية الرقمية هي الثغرة الأساسية التي ينفذ منها التضليل والترهيب الموجه.

● الواقع الميداني مقابل التهديد الرقمي:

تؤكد الشهادات الميدانية الدور الاستثنائي الذي تؤديه المدافعات عن حقوق الإنسان وبانيات السلام؛ حيث يقدن بنجاح وساطات محلية لحل نزاعات الموارد الشائكة كالأراضي والمياه، ويدرن مفاوضات إنسانية معقدة لتأمين هدن مؤقتة وإجلاء المدنيين من مناطق المواجهات، فضلاً عن جهودهن في الحد من تجنيد الأطفال وتسهيل الإفراج عن المعتقلين والمعتقلات.

ومع ذلك، تصطدم هذه الفاعلية ببيئة رقمية معادية تعتمد على التشهير والابتزاز الإلكتروني والطعن السلوكي؛ إذ تشير البيانات الإقليمية لهيئة الأمم المتحدة للمرأة إلى أن 49% من النساء مستخدمات الإنترنت في المنطقة لا يشعرن بالأمان من الاستهداف الرقمي، في حين توثق التقارير المحلية لمرصد الحريات الإعلامية في اليمن تعرض نحو 72% من الصحفيات والناشطات للتنمر والابتزاز الإلكتروني. وتستغل هذه الهجمات "الوصمة الاجتماعية" لفرض العزلة على الرائدات، مما يدفع ما يقارب 41% منهن إلى ممارسة "الرقابة الذاتية" والصمت حمايةً لسلامتهن الشخصية والأسرية، الأمر الذي يعوق وصولهن إلى الدعم القانوني والتقني الفعال، ويسهم في إفلات الجناة من المساءلة والمحاسبة.

● لماذا هذا الدليل؟

يأتي هذا الدليل كاستجابة منهجية وتطبيقية لسد الفجوة بين العمل الميداني والتمكين الرقمي، بهدف صياغة سردية بديلة قوية تواجه التضليل وتؤمن حضوراً آمناً للمدافعات ضد الاستهداف.

نحن ندرك تماماً أن امتلاك أدوات التواصل الرقمي وإدارتها بذكاء يتجاوز الرفاهية التقنية ليصبح ضرورة استراتيجية لحماية القيادة النسوية، وتنظيم العمل التضامني، وتأمين حضور فاعل وآمن للمرأة في مسارات صنع القرار وبناء السلام الشامل. يمثل هذا الكتيب أداة عمل ميدانية حية، صُممت لتوفر الحماية والتمكين وتصنع الأثر الحقيقي المستدام على الأرض.

● الشراكات والالتزام المؤسسي

تم تطوير هذا الدليل من قبل مبادرة مسار السلام (Peace Track Initiative) بتمويل من سفارة هولندا لدى اليمن، في إطار مشروع «تعزيز الحركة النسوية والمبادرات لبناء سلام شامل في اليمن»، وتحت مظلة الخطة الاستراتيجية الخمسية لشبكة التضامن النسوي (2026-2030) - المسار الثاني المكرس لتعزيز القيادة النسوية وبناء سردية نسوية مؤثرة.



يتوجه فريق العمل ببالغ الشكر والتقدير لكل الشركاء والناشطات اللواتي ساهمن في رصد الاحتياجات والمخاطر الميدانية التي تواجه النساء في الفضاء الافتراضي، وخصّصن وقتاً لتقديم الملاحظات والأفكار لإثراء هذا العمل وبناء محتواه بطريقة واقعية تلائم بيئة العمل المحلية.

إخلاء المسؤولية القانوني والفني

بموجب تصفح، استخدام، أو اعتماد الإرشادات الواردة في هذا الدليل (المُعد بجهد مشترك بين شبكة التضامن النسوي، مبادرة مسار السلام، والرابطة النسائية الدولية للسلام والحرية (WILPF)، فإنك توافقين على الالتزام بالشروط والبنود الفنية والقانونية الآتية:

● الواقع الميداني مقابل التهديد الرقمي:

- ديناميكية المعلومات التقنية: بذل فريق العمل والخبراء أقصى جهودهم لضمان دقة وتحديث الخطوات والبرمجيات حتى تاريخ الإصدار (يونيو 2026). ومع ذلك، فإن التطور المتسارع لأنظمة التشغيل والتطبيقات (Android & iOS) وتغير خوارزميات المنصات قد يؤدي إلى تغير بعض الإعدادات، مما يتطلب متابعة التحديثات الأمنية الرسمية دورياً وبشكل مستقل.
- المسؤولية الفردية للمستخدم: لا يتحمل فريق المشروع، الجهات الشريكة، أو الجهة الممولة (وزارة الخارجية الهولندية) أي مسؤولية قانونية، جنائية، أو مادية عن أي أضرار، أو خسارة بيانات، أو اختراق حسابات، أو ملاحظات أمنية تنشأ بشكل مباشر أو غير مباشر عن استخدام التطبيقات المقترحة (مثل شبكات الـ VPN وأدوات التشفير)، أو نتيجة سوء تطبيق البروتوكولات الأمنية في البيئات عالية الخطورة والمناطق الرمادية.
- الروابط الخارجية والمصادر المرفقة: يتضمن الدليل روابط وإحالات لأدوات رقمية ومواقع خارجية. إدراج هذه الروابط يهدف لتسهيل الوصول للموارد والحلول فقط، ولا يعبر عن مسؤولية فريق العمل تجاه أمن أو سياسات خصوصية تلك الجهات الخارجية أو الشركات المطورة للبرمجيات.
- تكامل الوعي الميداني: على الرغم من أن التدابير الموصى بها (كالمصادقة الثنائية وتشفير الاتصالات) ترفع مستوى الأمان الرقمي بشكل كبير، إلا أنه لا يوجد نظام أمني وتقني آمن بنسبة 100%. يجب دمج الوعي الشخصي والتحوط الميداني لتفادي المخاطر المادية كالتفتيش القسري للأجهزة أو اعتراض شبكات الاتصال المحلية.
- طبيعة الدليل الإرشادية: يمثل هذا الدليل مصدراً توجيهياً عاماً لبناء القدرات وتأمين الحسابات، ولا يغني عن طلب الدعم والاستشارة الفنية المخصصة والمباشرة من فرق الطوارئ الرقمية المعتمدة عند التعرض لاختراق نشط، أو ابتزاز إلكتروني حاد، أو تهديد أمني مباشر.

مدخل مفاهيمي



دليل إجرائي مبسط، صُمم ليقدم الدعم العملي للناشطات، والمدافعات عن حقوق الإنسان، والمجموعات النسوية في اليمن والمنطقة العربية. يهدف الدليل إلى مساعدتك على سرد وحماية صوتك، وتصميم حملات مناصرة رقمية فاعلة تتكامل مع جسارتك الميدانية، وتدعم حضورك القيادي في مسارات بناء السلام الشامل وصناعة القرار.

يمثل هذا الكتيب خارطة طريق عملية قابلة للتطبيق والملائمة المرنة وفقاً للظروف الأمنية والميدانية المحيطة بنشاطك، بما يضمن صيانة الهوية الرقمية ورفع كفاءة التأثير النسوي.

قبل أن نبدأ رحلتنا..

من أجل تحقيق أقصى استفادة من أدوات هذا الدليل، نضع بين يديك أربعة مرتكزات أساسية لتكون ركيزة انطلاقك:



1

الإيمان بالتغيير هو المحرك الأول:

العمل في حملات المناصرة الرقمية يبدأ بشعلة داخلية: لذا ابدئي دائماً وعينك على الأثر والتحول النهائي الذي تسعى لصناعته.

2

التفكير خارج القوالب النمطية المفروضة:

إذا ظللتِ تقديمين المحتوى بالطرق التقليدية ذاتها، فستحصلين على النتائج المعتادة. كوني مبدعة، تمردي على قوالب "الضحية السلبية"، وقدمي سردية ريادية ملهمة.



3

رسم المسار يبدأ بوعي الواقع:

التخطيط الناجح ينطلق من قراءة دقيقة لمحيطك؛ حددي أين تقفين الآن (نقاط قوتك، أدواتك، والمخاطر المحيطة بك)، لتصلي بأمان إلى غايتك وحلمك الميداني.



4

التضامن النسوي هو مصدر قوتنا:

التغيير الحقيقي يبدأ بالتحالفات؛ تذكري أن حماية صوتك وصمود زميلاتك في الميدان يقوى عندما نتكاتف ويساند بعضنا بعضاً.



مفاهيم أساسية على الطريق

● المناصرة (Advocacy):

جهد منظم ومنسق تقوده المجموعات والناشطات لتغيير السياسات، والقوانين، والممارسات، والتطرق للقضايا المغفلة أو المهمشة، من أجل التأثير في مواقف صناع القرار وبناء مجتمع عادل ومنصف للجميع.

● المناصرة الرقمية (Digital Advocacy):

استثمار قوة الشبكات الاجتماعية والأدوات الرقمية لنقل قضية ما من الهامش إلى صدارة الاهتمام العام. هي تكتيك لفت الانتباه، وتوجيه صناع القرار نحو الحلول، وكسب تأييد وحشد مختلف فئات المجتمع لصالح العدالة والحقوق الإنسانية بنهج حقوقي عادل.

● السردية البديلة (Alternative Narrative):

الفضاء الرقمي ليس مساحة محايدة؛ إنه بنية تحتية تعكس بنى القوة وموازين الهيمنة على الأرض وتضخمها. في سياقنا الإقليمي، لا تواجه المدافعات عن حقوق الإنسان عنفاً عابراً، بل تواجهن عنفاً رقمياً جندرياً ممنهجاً يسعى لمحوهن وعزلهن عن الفضاء العام. بناءً عليه، تتجاوز السردية البديلة خيارات التجميل اللفظي أو ردود الأفعال الدفاعية لتفنيد الأكاذيب، لتصبح استراتيجية سياسية وحقوقية واعية لانتزاع حق التمثيل والسيادة الرقمية. إنها انتقال فاعل من مربع "تبرير المواقف" إلى "فرض الخطاب وتوجيه النقاش"؛ لتقديم النساء كقائدات وصانعات قرار يبينن السلام برؤيتهن الخاصة، ويتصددين للصور النمطية والتضليل بشكل مباشر ودائم.



تذكري دائماً:

- المناصرة التقليدية والرقمية هما أداتان مكملتان لبعضهما؛ فالزخم الافتراضي يحمي ويقوي الصمود الميداني، والعمل الميداني هو الروح الحقيقية التي تغذي السرد الرقمي.
- إذا لم تبادري بسرد قصتك وتقديم حقائقك بنفسك، فسيقوم الآخرون بفبركتها وسردها بالنيابة عنك ووفقاً لمصالحهم.

الفصل الأول

السرد والحضور الرقمي للنساء

السيادة الرقمية وتصميم وإطلاق
السرديات البديلة

السرد الرقمي كمساحة سيادية وتفكيك الفجوة الحقوقية في سياق بيئات النزاع.
تفكيك الفجوة بين العمل الميداني والمهارات التقنية للمدافعات.
قوة القصة الصحفية الإنسانية ومخطط ركائز هندسة البناء القصصي.
أدوات صياغة القصة (البساطة، الأنسنة، الدقة الحقوقية) والمعايير الأخلاقية.
الأبعاد الأخلاقية والمعايير الحمائية في الصحافة النسوية.
التكتيكات الفنية للدمج الذكي للوسائط البسيطة والإنفوجرافيك والاقتراسات.
تفكيك وفهم حملات التشويه والتضليل الإعلامي الجندي.
المرجع الميداني لإدارة الأزمات والرد السردى التضامني.

السرد الرقمي كمساحة سيادية وتفكيك الفجوة الحقوقية في سياق بيئات النزاع



تؤدي النساء في اليمن أدواراً ميدانية جسيمة واستثنائية؛ حيث يقدن وساطات محلية معقدة لحل نزاعات الموارد الشائكة كالأراضي والمياه، ويدرن مفاوضات إنسانية لتأمين هدن مؤقتة، وإجلاء المدنيين، وتسهيل الإفراج عن المعتقلين والمعتقلات. ومع ذلك، فإن هذه الإنجازات تتعرض للتهميش والإقصاء الممنهج في وسائل الإعلام التقليدية الخاضعة للرقابة الصارمة من أطراف النزاع.

يتحول الفضاء الرقمي هنا ليصبح مساحة سيادية بديلة، تمكن المدافعات من رواية قصصهن وتوثيق تجاربهن برؤيتهن الخاصة. إن امتلاك هذه المساحة وإدارتها بوعي وحصافة يسمح بكسر أطواق العزلة المجتمعية، وتجاوز مقص الرقيب، وتقديم النساء كقائدات وصانعات قرار يبنين السلام، مما يتحدى الصور النمطية المفروضة عليهن.

تفكيك الفجوة بين العمل الميداني والمهارات التقنية



رغم الجسرة الاستثنائية للأداء الميداني، تشير البيانات المحلية لمرصد الحريات الإعلامية في اليمن إلى تعرض نحو 72% من الصحفيات والناشطات للتنمر والابتزاز الإلكتروني. كما تظهر بيانات هيئة الأمم المتحدة للمرأة أن 49% من النساء مستخدمات الإنترنت في المنطقة العربية لا يشعرن بالأمان من الاستهداف الرقمي. هذه الفجوة الحادة بين قوة العطاء الميداني وافتقار الناشطات للمهارات والتدابير التقنية لحماية حضورهن هي الثغرة الأساسية التي ينفذ منها التهريب الموجه.

تستغل الهجمات الرقمية "الوصمة الاجتماعية" لفرض العزلة على الرائدات، مما يدفع ما يقارب 41% منهن إلى ممارسة "الرقابة الذاتية" والصمت حمايةً لسلامتهن الأسرية والشخصية. لتفكيك هذه الفجوة، يضع الدليل خطة عمل تجمع بين مهارة التعبير الصحفي الملهم وبين الحصانة التقنية، مما يضمن استمرارية صمود القيادات النسوية في الفضاء العام دون خوف أو تراجع ويهيئ حضوراً فاعلاً وآمناً للمرأة في مسارات صنع القرار.

قوة القصة الصحفية الإنسانية وهندسة البناء القصصي

تواجه التقارير الحقوقية التقليدية فجوة تحريرية واضحة عندما تكتفي بسرد الأرقام الصامتة، والإحصائيات الجافة، والتوصيفات القانونية البحتة للانتهاكات. ورغم أهمية هذه البيانات في التوثيق القانوني والجنائي، إلا أنها غالباً ما تعجز بمفردها عن تحريك الوعي الجمعي أو حشد التضامن المطلوب والمؤثر. إن إغفال الوجه الإنساني للقضايا يحرم الحملات الرقمية من قدرتها على إحداث استجابة دولية ومحلية حقيقية.

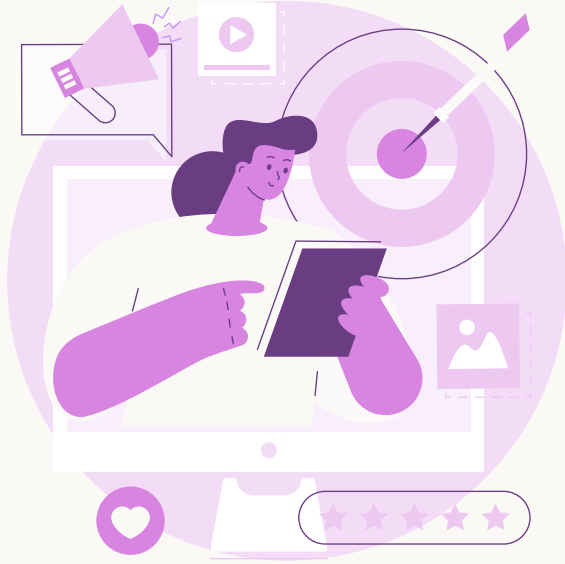
من هنا تبرز أهمية مفهوم "أنسنة" القضايا الحقوقية: وهي استراتيجية تحريرية تهدف إلى تفكيك القوالب النمطية التي تحصر النساء في دور "الضحية المستسلمة السلبية"، وإعادة تقديمهن كصانعات أثر وقائدات يمتلكن القدرة على الفعل والمقاومة والابتكار في شتى المجالات الميدانية. الأنسنة تعني إعطاء ملامح، وصوت، وحكاية نابضة بالحياة لتلك الأرقام الصماء، مما يجعل القضية قريبة من لغة الميدان ومفهومة للجمهور العام ومؤثرة في صناع القرار.

مخطط ركائز هندسة البناء القصصي الإنساني للمناصرة

الركيزة الأساسية	المضمون التحريري والحقوقى الميداني	الهدف الاستراتيجي من المناصرة
1. البطل (المرتكز الإنساني)	تقديم الشخصية المحورية (مثال: امرأة تقود وساطة محلية لحل نزاع مياه) بهويتها الإنسانية، وأخطامها، وسياقها الطبيعي بعيداً عن نمط الضحية.	خلق رابط تعاطف وجداني مباشر وعميق بين المتلقي وصاحبة القضية.
2. التحدي (تفكيك الانتهاك)	استعراض العائق أو الانتهاك الممنهج الذي واجهته البطلة (حملة تشهير، ابتزاز إلكتروني) وشرح أثره على سلامتها وعائلتها.	تجسيد القضية الحقوقية العامة وتوضيح أبعادها الاجتماعية والسياسية عبر تجربة ملموسة.
3. الفاعلية والمقاومة النشطة	تسليط الضوء على آليات المقاومة والخطوات الشجاعة التي اتخذتها البطلة لمواجهة الاستهداف واستمرار عملها الميداني وبناء شبكات التضامن.	إبراز قيم التضامن النسوي وتغيير الصورة النمطية لتقديم النساء كقائدات رياديات ملهمات.
4. الدعوة للمناصرة (Call to Action)	صياغة نداء واضح ومحدد للجمهور أو صناع القرار (مثل: المطالبة بحاسبة الجناة، وتوفير حماية قانونية للمدافعات).	تحويل التفاعل العاطفي إلى فعل ومشاركة تضامنية منظمة تخدم أهداف الحملة على الأرض.

إن توظيف هذا البناء الهندسي يضمن صياغة محتوى صحفي رفيع المستوى، يحفظ المصداقية المنهجية للحملة الحقوقية ويمنحها قوة انتشار واسعة النطاق عبر الفضاء الافتراضي والمنصات الرقمية.

أدوات صياغة القصة (البساطة، الأنسنة، الدقة الحقوقية)



البساطة



الأنسنة



الدقة الحقوقية



المبادئ الثلاثة لكتابة القصة الإنسانية

1. البساطة اللغوية الموجهة للجمهور العام:

يجب الابتعاد التام عن المصطلحات القانونية المعقدة أو التراكيب اللغوية المتكلفة والمحسنات البديعية. تُصاغ القصة بلغة واضحة، سلسلة، وقرينة من الواقع الميداني لضمان سرعة فهمها وانتشارها بين مختلف فئات المجتمع عبر منصات التواصل الاجتماعي والتطبيقات المختلفة.

2. الأنسنة والعمق التعبيري للتجربة:

التركيز على التفاصيل الإنسانية الحية التي تبرز شجاعة وصمود المدافعة في مواجهة التحديات. يهدف هذا المبدأ إلى إبراز الجوانب المعنوية والعملية للتجربة المعاشة، مما يجعل المتلقي شريكاً في استشعار أهمية القضية المطروحة وتجلياتها الإنسانية اليومية.

3. الدقة والحصافة الحقوقية الموثقة:

لحماية المحتوى والحملة بأكملها من الطعن، أو التشكيك، أو الاتهام بالتسييس من الجهات المضادة وقوى النزاع، يجب الالتزام الصارم بنقل الحقائق المثبتة، والوقائع الموثقة، والتواريخ الدقيقة دون مبالغة أو تهويل. إن الخطأ الحقوقي أو التاريخي الصغير قد يُستغل بذكاء وخبث لضرب مصداقية المدافعة والمنظمة والحملة بأكملها، لذا فإن الحصافة والدقة هما صمام الأمان الحقيقي للمحتوى الرقمي.

الأبعاد الأخلاقية والمعايير الحمائية في الصحافة النسوية



إن مناصرة قضايا النساء والدفاع عن حقوقهن لا يمكن، بأي حال من الأحوال، أن تتم على حساب خصوصيتهن، أو سلامتهن الجسدية، أو أمنهن الرقمي والميداني. إن الصحافة والمناصرة النسوية تنطلقان من مبدأ أساسي وهو "عدم إلحاق الضرر" (Do No Harm)، ولذلك يجب التزام الناشطات والمحركات بالضوابط الأخلاقية والحمائية الصارمة التالية:

1- الموافقة المستنيرة والوعي المسبقة

يُمنع منعاً باتاً نشر أي قصة، أو اسم، أو صورة، أو موقع، أو معلم، أو معلومة تفصيلية قد تدل بشكل مباشر أو غير مباشر على هوية المدافعة أو الضحية في البيئات عالية الخطورة دون الحصول على موافقة صريحة، واعية، وموثقة منها مسبقاً بشكل واضح. ويجب على المحررة شرح النطاق الرقمي للنشر، والجمهور المحتمل، والمخاطر الأمنية والميدانية المترتبة على صاحبة القصة وعائلتها بوضوح كامل وتفصيلي.

2- احترام الخصوصية والحق في النسيان الرقمي

تملك صاحبة القصة الحق الأخلاقي والقانوني الكامل والثابت في طلب تعديل تفاصيل حكايتها، أو حجب بعض المعلومات، أو حذف القصة نهائياً من كافة المنصات الرقمية ومواقع التواصل الاجتماعي في أي وقت تشاء، إذا استجبت ظروف ميدانية، أو اجتماعية، أو أمنية تهدد سلامتها الشخصية أو الأسرية ومحيطها الاجتماعي. ويجب الاستجابة الفورية لطلبها دون إبطاء أو نقاش مادي.

3- تجنب لقطات الضعف المهينة وصور الانكسار

ترفض الصحافة النسوية الرشيدة والمناصرة الأخلاقية استخدام الصور الفوتوغرافية أو التعبيرات التحريرية التي تظهر النساء في حالة انهيار تام، أو ضعف مهين، أو استجداء للعطف والانكسار لخدمة أغراض ترويجية. يتم استبدال ذلك بصور رمزية راقية، أو رسومات تعبيرية، أو لقطات محايدة توجي بالكرامة والكرامة الإنسانية، لتقديمهن كقوة فاعلة وصامدة في الميدان.

التكتيكات الفنية للدمج الذكي للوسائط البسيطة والإنفوجرافيك والاقتراسات

التكتيكات الفنية لإعداد ودمج الوسائط الرقمية خفيفة الوزن

تواجه المدافعات عن حقوق الإنسان في اليمن تحديات تقنية وبنوية خانقة، تتركز في الضعف الشديد لشبكات الإنترنت، والانقطاع المستمر للتيار الكهربائي، وارتفاع كلفة حزم البيانات. في ظل هذه الظروف، يصبح الاعتماد على الوسائط مرئية الثقيلة مثل مقاطع الفيديو الطويلة عالية الدقة عائقاً حقيقياً يحول دون وصول رسالة المناصرة إلى الجمهور المستهدف. يتطلب هذا الواقع تبني استراتيجية الدمج الذكي للوسائط خفيفة الوزن؛ وهي مواد رقمية مصممة خصيصاً لتستهلك حزماً ضئيلة من البيانات، وتملك قدرة فائقة على الانتشار الفيروسي السريع عبر تطبيقات المراسلة الفورية والمنصات.

● الاقتباسات النصية المصورة (Quotes)

تعد الاقتباسات المصورة أداة بالغة الأثر لكسر جمود النصوص الحقوقية الطويلة ولفت انتباه المستخدم أثناء التصفح السريع للحسابات.

معايير الضغط والحجم:

تُحفظ الصورة بصيغة WebP أو JPEG مضغوط، بحيث لا يتجاوز حجم الملف النهائي 150 كيلوبايت، مما يضمن تحميلها الفوري حتى في ظل تغطية شبكات الجيل الثاني الضعيفة (2G).

آلية التنفيذ الفنية:

يتم اختيار جملة قوية، ملهمة، ومحورية من القصة الإنسانية، وتوضع داخل قالب بصري بسيط يحمل الهوية البصرية للحملة (مثل استخدام ألوان الغلاف العاجي، البنفسجي، أو الفيروزي).

● التسجيلات الصوتية القصيرة: الشهادات المسموعة والرسائل الإرشادية السريعة

يعتبر تطبيق (واتساب) شريان الاتصال الرقمي الأكثر انتشاراً واستخداماً في اليمن، مما يجعله قناة إستراتيجية لتداول المحتوى الحقوقي ونشره على نطاق واسع في المناطق الريفية وشبه الحضرية التي تغيب عنها التغطية الجيدة للإنترنت.

معايير السلامة والأمن الرقمي:

عند وجود أي خطر أمني أو ملاحقة للمدافعة، يتم غمس الصوت أو تعديل طبقاته تقنياً لحماية هويتها الشخصية. يُحفظ الملف بصيغة MP3 بحجم ضئيل جداً يسهل تناقله وإعادة توجيهه بين مجموعات الواتساب المحلية بسلسلة كـ "رسائل وسائط تضامنية" بأقل كلفة بيانات ممكنة.

تكتيك الإنتاج والانتشار:

يتم تكثيف القصة والشهادة الميدانية إلى رسالة صوتية قصيرة ومكثفة لا تتجاوز مدتها 60 إلى 90 ثانية كحد أقصى، تركز على نبذة الصوت الدافئة التي تنقل الحقيقة بصدق وموثوقية وتخطب الفئات التي قد تعاني من صعوبات في القراءة.

● الرسوم البصرية المبسطة (Infographics):

يهدف الإنفوجرافيك المبسط إلى تلخيص سياق المعاناة وبيانات الانتهاكات الحقوقية المعقدة وعرضها بلمحة بصرية واحدة واضحة ومريحة للعين، مما يسهل الفهم والمقارنة الفورية للمتصفح السريع.

منهجية التصميم لبيئات النزاع:

يجب الابتعاد تماماً عن التصميمات المزدحمة بالرموز والألوان الفاقعة التي ترهق العين وتتطلب طاقة تشغيل عالية للأجهزة. يركز التصميم على عرض رقمين أو ثلاثة أرقام إحصائية محورية فقط (مثل إبراز نسبة 72% الخاصة بانتهاكات التنمر الإلكتروني في اليمن)، مع استخدام مساحات فارغة كافية تضمن وضوح المادة واستيعابها بلمحة سريعة دون استهلاك طاقة الجهاز أو حزمة الإنترنت الخاصة بالمستخدم.

تفكيك وفهم حملات التشويه والتضليل الإعلامي الجندري

تفكيك وفهم حملات التشويه والتضليل الموجهة ضد المدافعات

تتعرض الناشطات والمدافعات عن حقوق الإنسان في اليمن والمنطقة العربية لنمط عنيف ومنظم من الهجمات الرقمية المقترنة بنوع الجنس، حيث يُستغل الفضاء الافتراضي كأداة لتشويه المسيرة الحقوقية وفرض العزلة على الرائدات. لا تسعى هذه الحملات إلى نقد الآراء أو الأنشطة بأسلوب موضوعي، بل تتجه مباشرة نحو "اغتيال الشخصية" والطعن السلوكي الأخلاقي لإجبار النساء على ممارسة الرقابة الذاتية والانسحاب من الفضاء العام. إن فهم بنية هذه الحملات وآلياتها يمثل خط دفاع حاميته ونفسي يقي الناشطة من الصدمة الأولى ويمنع ارتباكها في الميدان.

● الأنماط الشائعة لحملات التشويه والتضليل الرقمي الموجه

رصد الخبراء والباحثون الحقوقيون ثلاثة أنماط رئيسية للحملات الموجهة ضد النساء في السياق المحلي والإقليمي:

حملات الطعن في السلوك الأخلاقي والاجتماعي:

استغلال العادات والتقاليد المجتمعية المحافظة وفبركة ادعاءات تمس الشرف والسمعة الشخصية للمدافعة. يهدف هذا النمط إلى تحريض العائلة والمحيط المحلي ضد الناشطة، مما يشكل تهديداً مباشراً على سلامتها الجسدية والأسرية ويحرمها من التضامن المجتمعي.

فبركة وتزوير المنشورات والصور (التزييف الرقمي):

استخدام برامج التعديل التقني لتركيب صور مفبركة أو تزوير محادثات نصية وهمية ونسبتها للناشطة ومشاركتها على مجموعات عامة. تُنشر هذه المواد عبر شبكات تنسيقية واسعة لإظهار المدافعة في مظهر يخالف قيمها ومبادئها الحقوقية المعلنة.

التخوين السياسي والتحريض على العنف المادي:

توجيه اتهامات جاهزة بالعمالة، أو الخيانة الوطنية، أو التبعية لجهات استخباراتية خارجية بسبب نشاطها المستقل في بناء السلام أو توثيق الانتهاكات. يهدف هذا التحريض إلى شرعنة الاعتداء عليها أو تبرير اعتقالها تعسفياً من سلطات الأمر الواقع والجهات الأمنية القائمة.

الوعي المسبق هو حصانك أمام حملات التشويه

إن إدراك المدافعة المسبق بأن هذه الهجمات الشرسة ليست سلوكاً عفوياً أو شخصياً، بل هي استراتيجية وتدبير ممنهج وممول لإسكات صوتها ومنعها من التأثير، يسهم بشكل قطعي في امتصاص الصدمة النفسية الأولى ومنع الانهيار المعنوي. يمنح هذا الوعي الناشطة الثبات والقدرة على ضبط النفس، ويقيها من الوقوع في فخ الردود المتسارعة أو المهارات الرقمية التي تغذي خوارزميات المنصات وتزيد من انتشار الحملة. بدلاً من ذلك، تتربص الناشطة لتطبيق البروتوكولات السردية الباردة بهدوء ورصانة وموثوقية عالية.

المرجع الميداني لإدارة الأزمات والرد السري التضامني

المرجع الميداني لإدارة الأزمات والرد السري التضامني

عند حدوث أو انتشار حملة تشويه أو تشهير جندي منظم ضد مدافعة أو مبادرة نسوية، يتطلب المشهد استجابة فورية وحازمة تتجاوز التدابير التقنية الصرفة لحماية الهوية الرقمية (والتي تم تفصيلها بدقة منهجية مخصصة في الفصل الثالث من هذا الدليل). يركز هذا القسم على المرونة الاتصالية والسياسية واستراتيجية استعادة زمام الخطاب والتحكم في الرسالة العامة، من خلال بروتوكول ميداني يشتمل على أدوات وقوالب كتابية مباشرة لحملات المناصرة:

● مصفوفة القرار الإعلامي (الرد العام مقابل الكتمان الاستراتيجي)

إن اتخاذ قرار عشوائي بالرد على الهجوم في وسائل التواصل الاجتماعي قد يحقق للمهاجمين هدفهم الأساسي وهو زيادة معدلات التفاعل والخوارزميات (Engagement Feed). استخدم المصفوفة الميدانية التالية لتوجيه تصرفك وتصرف فريقك الإعلامي:

حالات الرد السري البارد والموجه (Cold Narrative Response):

المؤشر:

عندما يبدأ التضليل والتشهير بالانتقال إلى شخصيات عامة أو مجتمعية مؤثرة، أو عندما يهدد بشكل حقيقي سلامة الناشطة الميدانية وعلاقاتها العائلية والقبلية أو يتسلسل لتعطيل عمل المنظمة على الأرض.



الإجراء:

تفعيل تكتيك "إحباط سلاح الوصمة" بصياغة بيان إعلامي بارد، تقني، وحيادي جداً، وتوجيه الأنظار مجدداً نحو القضية الحقوقية الإنسانية الأساسية.

حالات الكتمان والتجاهل الاستراتيجي (Strategic Muting):

المؤشر:

عندما يكون الهجوم صادراً عن حسابات وهمية حديثة العهد (ذباب إلكتروني برمجي) بلا تأثير حقيقي، أو تعليقات بذيئة عشوائية تهدف لجّر الناشطة للجدال.



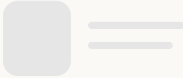
الإجراء:

التجاهل المطلق للرد العام، والبدء الفوري بالتنظيف البرمجي والأرشفة الجنائية الصامتة الموصى بها في الفصل الثالث، دون إعطاء الحملة وقوداً من التفاعل المباشر.

المرجع الميداني لإدارة الأزمات والرد السري التضامني

قالب البيان التوضيحي (رد مباشر للتعامل مع التضليل)

يهدف هذا القالب التحريري إلى إضفاء طابع رسمي ومؤسسي على رد المنظمة، مما يضع القضية في إطارها القانوني الصحيح أمام الرأي العام والجهات المختصة، ويحول التشويه الرقمي من "جدل اجتماعي" إلى "انتهاك قانوني":



ترويسة المنظمة / الجهة الرسمية

**موضوع بيان توضيحي بشأن تعرض منظمة / مبادرة (اسم الجهة)
لحملة تشهير وتضليل رقمي**

إلى من يهمه الأمر / الجهات الأمنية والقضائية المختصة / الرأي العام

تود (اسم الجهة) التأكيد على التزامها الثابت بمهامها الإنسانية والحقوقية وفقاً للقوانين النافذة والمواثيق المهنية. وفي هذا الإطار، نود إحاطة الرأي العام والجهات الرسمية، وعلى رأسها مكتب النائب العام والجهات المختصة بأننا تعرضنا خلال الفترة حدد الفترة لهجمات رقمية ممنهجة شملت تزيف محتوى إعلامي ونشر معلومات مضللة تهدف إلى عرقلة أعمالنا وتقويض أمننا المهني.

إن هذه الحملات التي تتجاوز حدود النقد المشروع إلى التشهير الصريح وتزوير الحقائق، تعد انتهاكاً للقوانين الوطنية ذات الصلة بجرائم المعلوماتية. لذا، نؤكد للجميع أننا بصدد استكمال ملف الأدلة الفنية والجنائية الخاصة بمصادر هذه الهجمات والجهات المحرصة، تمهيداً لتقديمها للجهات القضائية المختصة والنيابة العامة لاتخاذ الإجراءات القانونية اللازمة بحق المتورطين.

إننا إذ نصدر هذا التوضيح، نحفظ بحقنا القانوني الكامل في ملاحقة كافة الأطراف المتورطة في هذه الحملة وندعو شركاءنا في منظمات المجتمع المدني والجهات المعنية إلى اليقظة تجاه محاولات التضليل الممنهجة التي تستهدف العمل المدني والحقوق.

الختم الرسمي :
(في حال النشر الورقي)

صادر عن (اسم الجهة)
(التاريخ)

ملاحظة إجرائية: يُنصح بشدة إرسال نسخة رسمية من هذا البيان، مرفقة بملف الأدلة الرقمية (Screenshots للروابط والمنشورات)، إلى مكتب النائب العام أو إدارة الجرائم الإلكترونية فوراً، حتى لو كان الرد للنشر العام؛ فهذا الإجراء يوثق التزامك القانوني ويحمي كيانك المؤسسي.

الفصل الثاني

التخطيط الاستراتيجي لحملات المناصرة النسوية الرقمية

مدخل إلى التخطيط الاستراتيجي لحملات المناصرة النسوية الرقمية وسد الفجوة الميدانية.
تحديد القضية وتفكيك المشكلة المجتمعية باستخدام منهجية شجرة المشكلات.
تطوير السردية وصياغة قضية الحملة وجمع الأدلة الميدانية الموثقة.
صياغة الأهداف الاستراتيجية والمرحلية وتطبيق معادلة الأهداف الذكية (SMART).
رسم رحلة تفاعل الجمهور وحشد الدعم وتوجيه السلوك الرقمي للمستخدم.
مصفوفة تحليل وتحديد أصحاب المصلحة والجمهور المستهدف (حلفاء ومحايدين وخصوم).
هندسة تكتيكات الحملة الرقمية وبناء هويتها وعلامتها البصرية ودلالات الألوان.
إنتاج وإدارة محتوى الحملة وجدولته وتكتيك الأمواج في النشر الرقمي.
قواعد التشبيك الرقمي وبناء الرسائل السياسية والحقوقية لصناع القرار والبعثات الدولية.
قائمة فحص فاعلية وجاهزية الحملة قبل الإطلاق الفعلي

مدخل إلى التخطيط الاستراتيجي لحملات المناصرة النسوية الرقمية

مقدمة: مدخل إلى المناصرة الرقمية

المناصرة الرقمية هي استخدام الأدوات والمنصات الرقمية لتعزيز قضية حقوقية أو نسوية، بهدف إحداث تغيير في السياسات، القوانين، أو الممارسات الاجتماعية. لا يختلف جوهر المناصرة عن العمل الميداني، بل هو امتداد له، يهدف إلى تكبير الأثر والوصول لشرائح أوسع من الجمهور وصناع القرار.

مفهوم المناصرة: هي جهد منظم يهدف إلى إقناع صناع القرار أو الجمهور باتخاذ إجراء محدد تجاه مشكلة معينة.

أساسيات المناصرة

1- الاستناد إلى الدليل:

تركز حملة المناصرة الموثوقة على البيانات الدقيقة، الإحصاءات، والوقائع المستخلصة من الميدان.

2- تحديد الهدف:

صياغة واضحة للمطالب الأساسية (ما هو التغيير التشريعي أو الإداري المحدد الذي نسعى لتحقيقه؟).

3- تحديد وفهم الجمهور:

تحديد دقيق للفئات المستهدفة بالقضية وقنوات الاتصال الرقمي المفضلة لديهم.

4- السردية البديلة المؤثرة:

صياغة القضية في قالب قصصي يمس الوجدان ويحترم الحقيقة.

مقارنة: استراتيجية المؤسسات مقابل استراتيجية المدافعات

وجه المقارنة	المناصرة المؤسسية (المنظمات)	المناصرة الفردية (المدافعات عن الحقوق)
بنية اتخاذ القرار	معقدة وبيروقراطية، تتطلب موافقات إدارية وقانونية مطولة.	مرنة وفورية، تعتمد على استجابة المدافعة السريعة للأحداث الميدانية.
الموارد والميزانية	تعتمد على تمويل المشاريع، حملات مدفوعة، وتوظيف مصممين ومحللين.	تعتمد على تمويل المشاريع، حملات مدفوعة، وتوظيف مصممين ومحللين.
تقييم وإدارة المخاطر	تركز على المخاطر القانونية للمؤسسة، والسمعة المؤسسية، وإغلاق المقرات.	تركز على السلامة الشخصية، الابتزاز، التشهير، والتهديدات الأمنية المباشرة.
قنوات الوصول والانتشار	الحسابات الرسمية الموثوقة للمنظمات، ومواقع الويب، والبيانات الصحفية الجافة.	الحسابات الشخصية، مجموعات الواتساب، وصناعة المحتوى الإنساني القريب من الناس.

مثال تطبيقي:

في المناصرة المؤسسية، يتطلب إطلاق حملة حول العنف الرقمي لجان مراجعة، وتصميم قوالب معقدة، وموافقة المانحين. أما بالنسبة لك كمدافعة، فيمكنك رصد حالة تشهير لزميلة في الميدان، والتنسيق الفوري مع شبكة حليفة من المدافعات لإطلاق وسم #هاشتاق تضامني سريع مدعوم بنصائح أمان تقني مقتضبة، مما يطوق الأزمة ميدانياً قبل تفاقمها.

تمرين عملي:

بالاعتماد على مسيرتك كمدافعة، حددي في جدول من عمودين قضية محلية واجهتها. في العمود الأول، اكتبي كيف كانت ستتعامل معها منظمة دولية كبرى بصورة رسمية، وفي العمود الثاني، كيف يمكنك قيادتها كمدافعة ميدانية بمزيد من المرونة والتأثير المباشر؟

تحديد القضية وتفكيك المشكلة المجتمعية (منهجية شجرة المشكلات)

تحديد القضية وتفكيك المشكلة المجتمعية

قبل إطلاق أي حملة مناصرة، من المهم تذكر أننا لا نستطيع مناصرة "كل القضايا" في آن واحد. النجاح يبدأ بتركيز الجهود على مشكلة مجتمعية أو حقوقية واحدة محددة بوضوح.

نستخدم أداة "شجرة المشكلات" التخطيطية لتفكيك الأزمات الكبرى إلى أجزاء تفصيلية قابلة للتحليل والمناصرة، مما يمنع تشتت رسالة الحملة.

● مثال تطبيقي ل شجرة المشكلات :

إن اتخاذ قرار عشوائي بالرد على الهجوم في وسائل التواصل الاجتماعي قد يحقق للمهاجمين هدفهم الأساسي وهو زيادة معدلات التفاعل والخوارزميات (Engagement Feed). استخدم المصفوفة الميدانية التالية لتوجيه تصرفك وتصرف فريقك الإعلامي:



● مثال تطبيقي:

كمدافعة عن الحقوق، عند تفكيك قضية "العنف الرقمي ضد الناشطات"، لن نذهب لمعالجة الثغرات التشريعية الدولية البعيدة كالمؤسسات، بل ستركزين جذع الشجرة على مشكلة محورية تمس محيطك المباشر: "انتشار حملات الابتزاز والتشهير الإلكتروني لثني الناشطات المحليات عن العمل العام". جذورها ستكون غياب الوعي بالأمان التقني في مجتمعك، وآثارها هي فرض الرقابة الذاتية والانسحاب الاختياري للمدافعات من الفضاء العام.

● تمرين عملي:

ارسمي شجرة مشكلات مبسطة لقضية المناصرة التي تتبنيها كمدافعة على ورقة العمل المرفقة. حددي بدقة مشكلة محورية واحدة في الجذع، ثم تتبعي 3 أسباب جذرية في الأسفل، و3 آثار ظاهرة في الأعلى. بناءً على هذا التفكيك، حددي أي الجذور ستستهدفها حملتك الرقمية بالمعالجة والمناصرة؟

المرجع الميداني لإدارة الأزمات والرد السري التصادمني

السردية هي العمود القلبي والقصة الجوهرية لحملة المناصرة الرقمية الخاصة بك. لضمان صمود السردية أمام محاولات التشكيك أو التشويه الممنهج من الأطراف المضادة، يجب أن تُبنى وفق معادلة تجمع بين العمق الإنساني والصلابة العلمية والحقوقية.

هرم بناء السردية: يربط القصة الإنسانية في القاعدة، بالحقائق والأرقام في الوسط، ليصل إلى الهدف السري الواضح في القمة.



مثال تطبيقي:

وثقت المدافعة الميدانية (أ. م) مصادرة أراضي المزارعات في مديريتها، لتواجه حملة تشويه رقمية شرسة استهدفت سمعتها لإجبارها على الصمت والتراجع. يمثل هذا الاستهداف نمطاً متكرراً كشفت عنه التقارير المحلية، حيث تتعرض 74% من الناشطات المستقلات لانتهاكات وابتزاز رقمي مماثل عند ممارستن للعمل العام. ورغم هذه الضغوط، واصلت (أ. م) عملها الميداني، مؤكدة صمود المدافعات وقدرتهن على مواصلة حماية مجتمعاتهن والوقوف في صدارة المشهد.

في هذا النموذج، نظهر مستويات الهرم الثلاثة: نبدأ بالقصة الشخصية لـ (أ. م) لنلمس وجدان القارئ (القاعدة)، ثم نسند الواقعة بالإحصائية (74%) لتوثيقها علمياً (الوسط)، ونختم برسالة فاعلية تضع المدافعة في موقع القيادة عوضاً عن مظهر الضحية (القمة).

تمرين عملي:

بالاعتماد على القضية التي تم تفكيكها في شجرة المشكلات بالصفحة السابقة، صيغ مسودة سردية لحملتك في حدود 100 كلمة فقط. احرص على كتابتها في شكل قصة متماسكة ومسترسلة (مثل النموذج المرجعي أعلاه) بحيث تدمج أبعاد الهرم الثلاثة بشكل غير مباشر ومرن: (شهادة إنسانية حية + رقم إحصائي موثق + هدف سري يبرز صمود وقيادة المدافعات).

صياغة الأهداف الاستراتيجية والمرحلية (تطبيق معادلة SMART)

التخطيط الاستراتيجي الناجح يتطلب تحويل الرغبات العامة والأمنيات التغييرية العريضة إلى أهداف إجرائية ذكية ومحددة بدقة. أي هدف استراتيجي أو مرحلي لحملتك الرقمية يجب صياغته واختباره بالكامل بناءً على معادلة الأهداف الذكية (SMART):

SMART = Specific + Measurable + Achievable + Relevant + Time-bound

● معايير الهدف الذكي (SMART) الموجه للمدافعات:

إن اتخاذ قرار عشوائي بالرد على الهجوم في وسائل التواصل الاجتماعي قد يحقق للمهاجمين هدفهم الأساسي وهو زيادة معدلات التفاعل والخوارزميات (Engagement Feed). استخدم المصفوفة الميدانية التالية لتوجيه تصرفك وتصرف فريقك الإعلامي:

محدد (Specific): تحديد دقيق ومباشر لنوع التدخل الرقمي (ما الذي تسعى لتحقيقه شخصياً وبأدواتك البسيطة؟).	قابل للقياس (Measurable): وجود مؤشرات إحصائية أو كمية تمكنك من التقييم الذاتي (مثال: عدد التوقيعات على عريضة محلية، أو عدد المشاركات في مساحة نقاش رقمية تديرها بنفسك).	قابل للتحقيق (Achievable): صياغة هدف يتناسب مع القدرات الفردية، الوقت المتاح، والبيئة الأمنية المحيطة، لحماية النفس من الإرهاق اللوجستي أو المخاطر الميدانية.	واقعي وذو صلة (Relevant): ارتباط الهدف مباشرة بحل المشكلة المحورية التي حدتها في محيطك كمداخلة وتكامله مع أمنك الشخصي.	مقيد بزمان (Time-bound): تحديد إطار زمني واضح لبداية العمل ونهايته لضمان الحفاظ على زخم التفاعل وحسن إدارة جهدك الفردي.
--	---	---	--	---

جدول مقارنة بين أهداف المؤسسات وأهداف المدافعات الذكية:

أهداف المؤسسات الكبرى (ذات ميزانية)	أهداف المدافعات الفردية SMART (مرنة وعملية)
الضغط لتعديل اللوائح التنفيذية للوزارات المعنية بالحماية الجنائية خلال عامين.	تدريب 20 ناشطة في شبكتي المحلية على استخدام أدوات التشفير والتأمين الثنائي للحسابات عبر الإنترنت خلال 30 يوماً
بناء شراكة وطنية تضم كافة الاتحادات النسائية لتعديل كوتا المشاركة السياسية بحلول عام 2028.	إطلاق عريضة إلكترونية محلية لجمع 1000 توقيع تطالب السلطة المحلية بإشراك مدافعة واحدة على الأقل في لجان حل النزاعات بمديرتي خلال شهرين.

مثال تطبيقي:

لتجنب صياغة أهداف عامة يصعب تحقيقها فردياً مثل "القضاء على الابتزاز الرقمي في البلاد"، تضع المدافعة والناشطة النسوية المستقلة هدفاً ذكياً ومقاساً على قدراتها المتاحة: "صياغة ونشر بطاقة إرشادية رقمية مبسطة للأمان التقني، وتوزيعها عبر مجموعات الواتساب لتصل إلى 100 ناشطة في محافظتي خلال 15 يوماً القادمة".

تمرين عملي:

اكتبي هدفاً واحداً تسعى لتحقيقه عبر حملتك الرقمية المقترحة بصيغة عامة أولاً، ثم قومي بإعادة صياغته وتطويره بالكامل ليصبح هدفاً ذكياً يتوافق مع معادلة SMART ومقيداً بمؤشرات أداء وزمن تتناسب مع طاقتك الفردية ومواردك المتاحة.

رسم رحلة تفاعل الجمهور وحشد الدعم وتوجيه السلوك الرقمي

يتشكل الجمهور الرقمي من فئات متنوعة تمر بمسار نفسي وسلوكي تدريجي قبل التحول إلى مناصرين فاعلين للقضية. ويعتمد نجاح الحملة على تصميم محتوى يلائم المتطلبات السلوكية لكل مرحلة من هذا المسار.

رحلة تفاعل الجمهور للمدافعات: تبدأ بالوعي لاكتشاف القضية لأول مرة، تليها مرحلة الاهتمام لبناء الصلة الإنسانية واستشعار المشكلة، ثم اتخاذ الموقف للتفاعل بإجراءات بسيطة، وصولاً إلى مرحلة التنفيذ ليتحول المتابع إلى مناصر فاعل يحمي السردية وينشرها.

المراحل الأربع لرحلة تفاعل الجمهور:

1- الوعي (Awareness): يكتشف المستخدم القضية لأول مرة. المحتوى المناسب هنا هو المنشورات التوضيحية خفيفة الوزن، الرسوم البيانية البسيطة، والشهادات السريعة المبتدئة بسؤال جذاب.	2- الاهتمام (Interest): يبدأ المستخدم في استشعار صلة القضية بواقعه الإنساني أو القيمي ويبحث عن تفاصيل أعمق. المحتوى الملئم هو القصص الإنسانية المكتوبة، الفيديوهات القصيرة، والكبسولات الصوتية التي تحلل الأسباب والحلول الممكنة.	3- اتخاذ موقف (Action/Decision): يقرر المستخدم التفاعل والمساهمة العملية لدعم حملتك. الخطوة الإجرائية هنا يجب أن تكون مبسطة ومباشرة، مثل التوقيع على العريضة الإلكترونية للحملة، أو وسم منشوراته بهاشتاغ الحملة الرسمي.	4- التنفيذ والولاء (Advocacy): يتحول المتابع من مجرد مؤيد صامت إلى "مناصر فاعل" وناشر نشط لسردية الحملة البديلة ومدافع عنها ضد التشويش في مجموعات الواتساب ومنصات التواصل الاجتماعي.
---	---	---	--

مثال تطبيقي: نموذج جدولة نشر (حملة: أصواتنا آمنة) المخصصة للأمان الرقمي للمدافعات:

المرحلة	التوقيت	المنصة وقناة النشر	نوع المحتوى	مسودة المنشور / الفكرة العملية
1. الوعي	اليوم 1 (6 - 9 مساءً)	فيسبوك ومنصة X (العامة)	إنفوجرافيك خفيف	72% من الناشطات يتعرضن للابتزاز الإلكتروني الصامت. لست وحدك، المعرفة أمان.
2. الاهتمام	اليوم 3 (1 - 3 ظهراً)	فيسبوك وإنستغرام	تسجيل صوتي قصير أو بطاقة	قصة ملهمة لزميله مدافعة تغلبت على الابتزاز الرقمي بفضل الأمان التقني والدعم الفني
3. اتخاذ الموقف	اليوم 5 (6 - 9 مساءً)	المنصات العامة + الواتساب	منشور تفاعلي برابط مختصر	صوتك يحمي زميلاتك. اضغطي على الرابط لتوقيع عريضتنا لتفعيل خطوط طوارئ الجرائم الرقمية.
4. الولاء والتمكين	اليوم 7 والأسبوع الثاني	مجموعات مغلقة (واتساب/تليجرام)	رسالة نصية قصيرة للتداول	السلامة تضامن متبادل. شاركي دليل الأمان الرقمي المصغر في مجموعتك النسوية لتكوني صمام أمان. السلامة تضامن متبادل. شاركي

● تنويه هام حول جدولة النشر:

النشر الجماعي المتزامن:

نسقي مسبقاً مع 3 إلى 5 زميلات أو شبكات طيفة لنشر مواد كل مرحلة في ذات التوقيت والموازة؛ فالتزامن يزيد من وصول السردية بشكل عضوي دون الحاجة لاستثمار إعلانات ممولة معقدة.

بيئة النشر المتدرجة والأمنة:

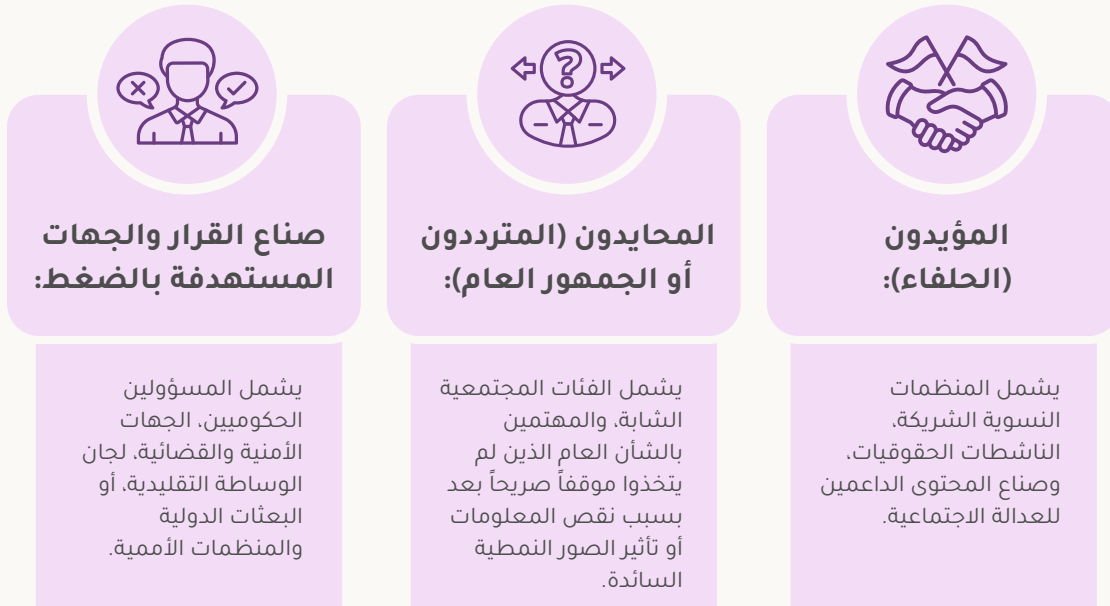
ابدئي بالمنصات العامة المفتوحة لبناء الوعي والاهتمام، وعند الانتقال لمرحلتين "اتخاذ الموقف" و"التنفيذ"، انقلي روابط الحشد والمواد الحساسة إلى المجموعات النسوية المغلقة والأمنة (مثل مجموعات سيفغال أو مجموعات واتساب الموثوقة) لتأمين التفاعلات ضد هجمات التصيد والتشويه.

تمرين عملي:

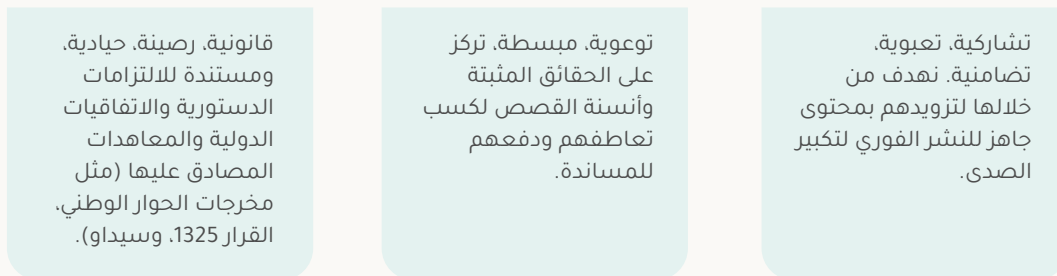
اختراري موضوعاً واحداً لحملتك، وقومي بتصميم فكرة محتوى رقمي محدد ومبتكر لكل مرحلة من المراحل الأربع (الوعي، الاهتمام، الموقف، التنفيذ). حددي نوع الوسيط الرقمي المقترح لكل منشور (فيديو، صورة، تسجيل صوتي، نص).

مصفوفة تحليل وتحديد أصحاب المصلحة والجمهور المستهدف

تقسيم فئات أصحاب المصلحة:



لغة الخطاب



مثال تطبيقي:

تركز المدافعة والناشطة النسوية المستقلة خطابها المباشر والمكتوب على صناع القرار المحليين والجهات الرسمية لانتزاع مطالب إجرائية واضحة لتعزيز حماية النساء، مع تجنب توجيه أي خطاب أو تواصل مع الخصوم (المحرضين أو الحسابات الوهمية) الذين يمثلون تهديداً أمنياً مباشراً يُتعامل معه حصرياً عبر بروتوكولات الحماية الذاتية والأمن الرقمي الموضحة في الفصل الثالث، وليس عبر الحوار والمناصرة.

تمرين عملي:

املئي مصفوفة أصحاب المصلحة الخاصة بقضيتك بالتفصيل. حددي اسماً واحداً على الأقل لحليف، ومتردد، وصانع قرار مستهدف بالحملة. ثم صوغي مسودة رسالة رقمية قصيرة وموجهة لكل فئة منهم مع الالتزام التام بتباين لغة الخطاب المناسبة لكل فئة.

هندسة تكتيكات الحملة الرقمية وبناء هويتها وعلامتها البصرية دلالات الألوان

تعد الهوية البصرية جزءاً أصيلاً من البنية الاستراتيجية للمناصرة: فهي تمنح الحملة مصداقية وتميزاً فورياً في بيئة وسائل التواصل الاجتماعي المزدهمة، وتسهل التعرف على القضية بلمحة بصرية سريعة ومريحة للعين.

مكونات وعناصر الهوية البصرية للمدافعات:

الألوان ودلالاتها النفسية والاجتماعية:

رمز تعبيرى مبسط جداً يدمج بين فكرة الحملة وبنائها الحقوقي، ويسهل التعرف عليه وضغطه في الصور بمختلف الأحجام والوسائط دون تشويش.

العاجي الدافئ

يُستخدم كخلفية بسيطة ومريحة للعين تضمن سهولة قراءة النصوص وتثبيت هوية الدليل البصرية الهادئة والراقية.



البنفسجي الغني:

يرمز دولياً للعدالة، النضال النسوي، الصمود، والالتزام المؤسسي بحقوق المدافعات.



الفيروزي الحيوي والتركواز

يرمز للأمان الرقمي والميداني، التوازن، الأمل، وبناء السلام والتضامن الإيجابي.



الشعار البسيط (Logo):

رمز تعبيرى مبسط جداً يدمج بين فكرة الحملة وبنائها الحقوقي، ويسهل التعرف عليه وضغطه في الصور بمختلف الأحجام والوسائط دون تشويش.

الخطوط الموحدة (Typography):

استخدام خط رسمي واضح، عريض ومقروء بسهولة على الأجهزة الذكية مثل خط "Tajawal Bold" للعناوين الرئيسية، وخطوط كلاسيكية ميسرة لقراءة النصوص الطويلة لتفادي إرهاق العين أثناء التصفح.

● صناعة المحتوى والمونتاج السريع (عبر الهاتف):



Phonto

إضافة نصوص عربية بخطوط احترافية وواضحة على تصاميم الصور بأحجام خفيفة ومضغوطة.



VN Video Editor

Capcut

لمونتاج الفيديوهات الميدانية والقصص الإنسانية وإضافة الترجمة النصية بمرونة تامة من الهاتف.



Canva

Adobe Express

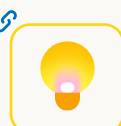
لإنشاء الهوية البصرية، وتصميم الصور وإزالة الخلفيات وتجهيز قوالب متنسقة وسريعة بجهد أقل.

● التنسيق الميداني والعمل دون اتصال بالإنترنت (Offline):

لكتابة وجدولة مسودات ومحتوى الحملات وحفظها تلقائياً للمزامنة والنشر فور توفر اتصال بالشبكة.



Adobe Express



Google Keep

للتواصل الجماعي الآمن والمشفّر بين المدافعات عند انقطاع الإنترنت بالكامل، حيث يعتمد على شبكة الواي فاي المحلية والبلوتوث لتمرير الرسائل.



Briar

تمرين عملي:

اختاري ثلاثة ألوان أساسية تتسق مع جوهر قضيتك لتشكّل لوحة الألوان الرسمية (Color Palette) لحملتك الرقمية. برري كتابه اختيارك لهذه الألوان وما دلالاتها النفسية والاجتماعية في سياق الحملة والميدان المحلي المحيط بالجمهور المستهدف.

إنتاج وإدارة محتوى الحملة وجدولته وتكتيك النشر الرقمي المتزامن

النشر المنسق والمشارك في النشر الرقمي:

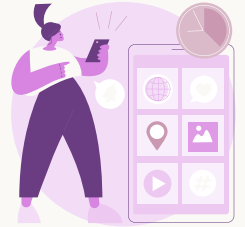
النشر الجماعي المتزامن: هو تركيز نشر محتوى الحملة وتكثيفه وإعلانه بالتزامن والتنسيق الجماعي مع الحلفاء والشركاء في ساعات ذروة تصفح الجمهور المستهدف (على سبيل المثال: من الساعة 6 مساءً وحتى 9 مساءً)، بدلاً من النشر المشتت والعشوائي طوال اليوم. هذا النشر المنسق يحدث تأثيراً متراكماً كبيراً يجبر خوارزميات المنصات على رفع مستوى الانكشاف العضوي وإظهار وسم الحملة وتصدير قضيتك في صدارة الاهتمام العام.

إعادة تدوير المحتوى المكتبي (Content Recycling): تحويل المادة الحقوقية الطويلة أو التقرير الحقوقي المنهجي الرسمي إلى قوالب متعددة وخفيفة الوزن يسهل تحميلها وتناولها بأقل كلفة بيانات ممكنة عبر تطبيقات المراسلة الفورية مثل الواتساب:

قالب (2): تسجيل صوتي قصير (Audio Flash / Voice Note) مدته من 60 إلى 90 ثانية، يركز على نبذة الصوت الدافئة لشرح الانتهاك وحلول الحماية بأسلوب مبسط وسهل التداول.



قالب (1): اقتباس نصي مصور قصير يحمل جملة ملهمة من السردية بخلفية موحدة وبحجم ضئيل لا يتجاوز 150 كيلوبايت.



قالب (4): سؤال تفاعلي مفتوح يشرك المستخدم في حوار تضامني لفرض النقاش.



قالب (3): رسم بياني تفاعلي مبسط (Infographic) يعرض رقمين أو ثلاثة أرقام محورية فقط محاطة بمساحة فارغة مريحة للعين.



تواجه الناشطة المستقلة في المناطق الريفية ضعف شبكة الإنترنت بضغط الصور وإعادة تدوير الشهادات الميدانية إلى تسجيلات صوتية مقتضبة ورسائل نصية مركزة، لسهولة تداولها وتمريضها عبر مجموعات الواتساب المحلية بأقل كلفة بيانات، متفادياً رفع الفيديوهات الطويلة أو الملفات الثقيلة التي تعتمد عليها المنظمات الكبرى.

تمرين عملي:

خذي موضوعاً حقوقياً واحداً من حملتك وقومي بتقسيمه وإعادة تدويره يدوياً إلى 4 أشكال وقوالب تفاعلية مختلفة خفيفة الوزن للمحتوى: (مسودة اقتباس نصي مصور، مسودة سيناريو لتسجيل صوتي سري بمدة 60 ثانية، مسودة رسم بياني برقمين فقط، وسؤال حواري تفاعلي مفتوح للجمهور).

إنتاج وإدارة محتوى الحملة وجدولته وتكتيك النشر الرقمي المتزامن

إنتاج وإدارة محتوى الحملة وجدولته وتكتيك النشر الرقمي المتزامن

تمثيل القضايا النسوية ومناصرتها رقمياً أمام صناع القرار المحليين، والجهات الأمنية، والقضائية، والبعثات الإقليمية، والدبلوماسية يتطلبان الالتزام الصارم بقواعد كتابة رصينة ومحترفة تتعد تماماً عن الانفعال اللفظي، الصراخ الإعلامي، أو تسييس الحقائق الصرفة. لغة التشبيك وبناء الرسائل السياسية يجب أن تتحلّى بالصلابة المنهجية والحصافة القانونية التي ترغم صانع القرار على التعامل مع مطالبك بجدية ومسؤولية بالغة.

● القواعد الذهبية لصياغة الخطاب السياسي والحقوقى للمدافعات:

لملخص الواضح والمباشر: ابدئي رسالتك أو مذكرتك الرسمية بفقرة تمهيدية مكثفة لا تتجاوز 50 كلمة توضح بدقة غرض الاتصال والمطلب الفوري للحملة، دون إطالة إنشائية أو تفاصيل سردية غير ضرورية في البداية.

المرجعية القانونية والدولية الصلبة: اسندي مطالبك دائماً إلى المرجعيات الدستورية والقوانين الوطنية المعمول بها، أو القرارات والمواثيق الدولية المصادق عليها، وعلى رأسها اتفاقية القضاء على جميع أشكال التمييز ضد المرأة (سيداو)، وقرار مجلس الأمن الدولي رقم 1325 ومجموعة القرارات اللاحقة التابعة لأجندة المرأة والسلام والأمن.

تقديم مطالب عملية قابلة للتنفيذ: تجنبي صياغة مطالب مطاطة أو هلامية مثل "نطالب بتمكين المرأة وتوفير السلام". استبدليها بمطالب موضوعية، واقعية، ومحددة تضع صانع القرار أمام مسؤولياته الإجرائية المباشرة (مثال: المطالبة بإلغاء قرار تعديل لائحة، تفعيل تمثيل، أو فتح تحقيق رسمي مستقل).

مثال تطبيقي:

الموضوع: مذكرة بشأن توفير بيئة عمل آمنة للمدافعات عن حقوق الإنسان والناشطات في لجان الوساطة المحلية.
إلى: السيدة/

الجهة المستهدفة

تحية طيبة وبعد،

بصفتنا ائتلافاً غير رسمي للمدافعات والناشطات النسويات المستقلات العاملات في الوساطة المحلية وبناء السلام في مديريات

... محافظة ... ، نكتب إليكم للإبلاغ عن تصاعد مقلق في حملات التشهير والابتزاز الإلكتروني المنظم التي استهدفت زميلاتنا خلال الأسبوعين الماضيين، عقب مشاركتهن في تسوية نزاع المياه والأراضي الميداني في منطقة...

الاسم

إن هذه الهجمات الرقمية الممنهجة تعيق مباشرة مشاركتنا الفاعلة في مسارات بناء السلام المحلي، وتعد انتهاكاً صارخاً لجوهر قرار مجلس الأمن رقم 1325. وتأسيساً على ذلك، نطالبكم بالتعاون والتدخل العاجل عبر قنواتكم الدبلوماسية والدبلوماسية والضغط على السلطات المحلية والأمنية من أجل:

فتح تحقيق رسمي مستقل وسريع في وقائع التهديد والابتزاز الرقمي التي تعرضت لها الناشطات المذكورات في الملف المرفق.

الالتزام بإصدار بيان علني يدعم دور المدافعات المستقلات ويجرم التحريض الإلكتروني ضدهن. تيسير سبل حركتنا الميدانية وتوفير قنوات اتصال طارئة وأمنة بالتنسيق مع شبكات الحماية المحلية الموثوقة.

شاكرين لكم التزامكم المشترك بدعم قيادة النساء وحمايتهن، ونتطلع لتجاوبكم العاجل.

تمرين عملي: اكتبي مسودة رسالة أو مذكرة رسمية موجهة لصانع قرار محلي في بلدك (لا تتجاوز 150 كلمة) تطالبينه فيها بتبني مطلب محدد وواضح لحملتك الرقمية المقترحة، مع الالتزام التام بالهيكل المهني والحيادي الصارم: (تحديد الموضوع ثم إرجاع المطلب للالتزام دستوري أو دولي حدد ثم صياغة مطلب إجرائي واضح ومباشر وقابل للتنفيذ).

قائمة فحص فاعلية وجاهزية الحملة قبل الإطلاق الفعلي

قبل إطلاق البدء وضغط زر النشر الفعلي لحملتك الرقمية وتجنب الأخطاء اللوجستية الحادة أو التهديدات الأمنية التي قد تلحق الضرر بسلامة فريق العمل الميداني والناشطات الرقميات، يجب مراجعة جميع تدابير الجاهزية والالتزام بقائمة فحص الفاعلية والجاهزية التالية بدقة وعناية تامة:

- هل تمت تصفية وتطوير جميع الأهداف لتصبح ذكية وتتوافق مع معادلة SMART؟
- هل الهوية البصرية للحملة موحدة وخلفيات الصور ملائمة للأحجام والوزن؟
- هل جميع البيانات، الشهادات، والأدلة الميدانية مدققة ومراجعة حقوقياً؟
- هل حصلت على موافقة واعية ومستنيرة مسبقاً من كافة بطلات وصاحبات القصص؟
- هل تمت معالجة وتعديل الأصوات الحساسة لحماية الهوية الرقمية للمدافعات؟
- هل مسودات الرسائل الموجهة لصناع القرار مصاغة بلغة قانونية رصينة؟
- هل تمت جدولة المحتوى بالكامل في أوقات ذروة تصفح الجمهور (تكتيك النشر الجماعي المتزامن)؟
- هل تم تفعيل تدابير الأمان الرقمي الثنائية لكافة حسابات الحملة وفريقها؟

بروتوكول المرونة والجاهزية الميدانية في حال حدوث الهجوم المضاد للمدافعات:

حالات الهجوم العشوائي (الذباب الرقمي والتعليقات المسيئة): تفعيل الكتم والتجاهل الاستراتيجي الفوري لتفادي تغذية الخوارزميات وتنشيط الحظر البرمجي والأرشفة الجنائية الموصى بها في الفصل الثالث دون تشنج أو انفعال لغوي قد يزيد من استهدافك شخصياً.

حالات التشويه المنظم (الابتزاز واغتيال الشخصية): يستلزم الهجوم المنظم تفعيل شبكة تضامن المدافعات الحليفة فوراً لإصدار موقف تضامني موحد، مع التوجه بملف الأدلة الرقمية الجنائية والأرشفة الصامتة إلى الجهات القضائية المختصة أو فرق الطوارئ الرقمية المعتمدة لحماية الهوية الرقمية والسلامة الشخصية، وتجنب المواجهة الفردية المنفصلة.

تمرين عملي:

اجتمعي بزميلاتك الناشطات والشركاء الحقوقيين في مساحة التخطيط المشتركة. قوموا بمراجعة بنود قائمة فحص الفاعلية والجاهزية بالكامل والتأكد من مطابقتها لكل بند بالتفصيل. بعد الانتهاء، صوغوا بياناً توضيحياً تجريبياً قصيراً كاستعداد لوضعه كخط دفاع وقائي أولي وجدار حماية إعلامي للتعامل مع أي هجمات مضادة، تمهيداً للانتقال إلى الفصل الثالث المخصص بالكامل لتفاصيل الأمان الرقمي والحماية الشاملة للمدافعات.

الفصل الثالث

الأمان الرقمي والحماية الشاملة

مدخل ومفاهيم أساسية في الأمان الرقمي

إدارة الهوية الرقمية

تحسين الحسابات وإعدادات الخصوصية المتقدمة

المرونة الرقمية أثناء انقطاع الإنترنت

بروتوكول المرور من النقاط الأمنية والتفتيش العشوائي

جدار الحماية الذاتي (شبكات VPN والشبكات العامة)

مواجهة الابتزاز الرقمي الموجه (الجانب التقني)

مواجهة حملات التشويه الممنهجة والجوش الإلكترونية (الذباب الرقمي)

كسر العزلة الرقمية وبناء شبكة الدعم والمساندة المتخصصة

توثيق الأدلة وحفظ الحقوق (الجانب التقني والقانوني)

مدخل ومفاهيم أساسية في الأمان الرقمي

الأمان الرقمي: جزء من السلامة الشخصية

في البيئة الرقمية المعقدة لليمن و المنطقة العربية، فإن التهديدات الرقمية لا تقتصر آثارها على فقدان الحسابات أو البيانات، بل قد تمتد لتشمل السلامة الجسدية، والنفسية والاجتماعية والمهنية.

ولهذا علينا التأكد أن الحسابات الرقمية، والأجهزة الذكية، ووسائل الاتصال، لم تعد مجرد أدوات تقنية، بل أصبحت امتداداً للحياة الشخصية والمهنية، واختراقها قد يتحول إلى تهديد يمس السلامة الجسدية والشخصية.

فالأمان الرقمي ليس حماية للأجهزة فقط، بل حماية لحياة الأشخاص وعلاقاتهم ومعلوماتهم

● لماذا نهتم بالأمان الرقمي؟

قد يؤدي حادث رقمي واحد إلى:

- كشف معلومات حساسة أو بيانات شخصية
- التعرض للتشهير أو الابتزاز الإلكتروني.
- استهداف الأسرة أو الشركاء أو المستفيدين
- فقدان الثقة أو السمعة المهنية.
- تعطيل العمل أو خسارة البيانات المهمة.
- في بعض الأحيان قد يؤدي للعزلة المجتمعية أو الإحتكار

منهجية تحليل المخاطر (Threat Modeling)

مصفوفة الأسئلة الخمسة

السؤال	الغاية منه	أمثلة
ما الذي أريد حمايته؟	تحديد الأصول المهمة	الحسابات، الملفات، الصور، جهات الاتصال
ممن أريد الحماية؟	تحديد مصادر التهديد	مبتزون إلكترونيون، جهات مراقبة، أشخاص من المحيط الاجتماعي
ما مدى احتمالية حدوث الخطر؟	تقييم مستوى التهديد	منخفض - متوسط - مرتفع
ما العواقب إذا حدث الاختراق؟	تقدير حجم الضرر	تشهير، ابتزاز، خسارة بيانات، تعطيل العمل
كيف يمكن تقليل المخاطر؟	اختيار إجراءات الحماية المناسبة	المصادقة الثنائية، النسخ الاحتياطي، تشفير البيانات

● أنواع التهديدات الشائعة:

- تقنية: مثل التصيد الاحتيالي، والبرمجيات الخبيثة، واختراق الحسابات
- اجتماعية ونفسية: مثل حملات التشهير، والعنف الرقمي، والابتزاز الإلكتروني.
- تهديدات فيزيائية-رقمية: مثل فقدان الأجهزة أو سرقتها، أو الوصول القسري إلى الهاتف، أو مصادرة الأجهزة وتفتيشها.

ملاحظة: في عالم الإنترنت لا توجد حماية أو خصوصية بنسبة 100%.

مدخل ومفاهيم أساسية في الأمان الرقمي



الهوية الرقمية: خط الدفاع الأول

تمثل الحسابات الرقمية بوابة الوصول إلى المعلومات لشخصية والمهنية، وقد يؤدي اختراق حساب واحد إلى الوصول إلى بقية حساباتك ومعلوماتك وفي البيئات المعقدة، حيث تتداخل التهديدات الرقمية مع العنف القائم على النوع الاجتماعي والابتزاز والتشهير، تصبح حماية الهوية الرقمية جزءاً أساسياً من السلامة الشخصية والمهنية.

1. كلمات مرور قوية

يوصى بها:

- طويلة (16 حرفاً أو أكثر)
- عبارة يسهل تذكرها
- مختلفة لكل حساب
- غير شخصية
- محفوظة بطريقة آمنة
- اجعلي كلمة المرور قابلة للتذكر باستخدام عبارات أو جمل تكون أكثر أماناً وأسهل في التذكر

تجنبي:

- أسماء أفراد الأسرة
- أرقام الهواتف أو تواريخ الميلاد
- كلمة مرور واحدة لجميع الحسابات
- كلمات شائعة أو سهلة التخمين

مثال:

I Love mama and baba 2026
نقوم بتشفيرها وتحويلها لكلمة مرور
!.L0ve.m@m@.&.b@b@.2026
كلما زاد طول العبارة، زادت صعوبة تخمينها أو كسرها

2. إدارة كلمات المرور بأمان

يفضل استخدام مدير كلمات مرور موثوق لإنشاء كلمات قوية وتخزينها بأمان.

أهم برامج مدير كلمات المرور

Bitwarden - KeePassXC- 1Password

حلول إضافية:

تجنبي حفظ كلمات المرور في الملاحظات أو المحادثات.
لا تشاركي كلمات المرور مع الآخرين.
احتفظي بنسخة احتياطية لرموز الاسترداد في مكان منفصل وآمن.
احتفظي بنسخة ورقية في مكان آمن.

3. المصادقة متعددة العوامل (MFA)

تضيف طبقة حماية إضافية بحيث لا تكفي كلمة المرور وحدها للوصول إلى الحساب

مستوى الحماية	الوسيلة
جيد	رسائل SMS
مرتفع	تطبيقات المصادقة (Authenticator)
مرتفع جداً	مفاتيح الأمان المادية

قاعدة أساسية:

احمي البريد الإلكتروني أولاً.

فهو مفتاح استعادة معظم الحسابات الأخرى،

والسيطرة عليه قد تعني السيطرة على هويتك الرقمية بالكامل.

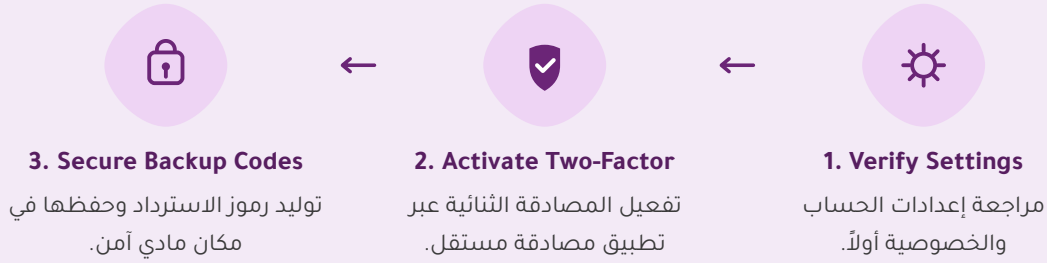
تحسين الحسابات وإعدادات الخصوصية المتقدمة



الخطوات التطبيقية الميدانية لتأمين قنوات الاتصال والعمل والشبكات اللاسلكية للناشطات والقيادات النسوية

تمثل الحسابات الرقمية بوابة الوصول الأساسية للمعلومات الشخصية والمهنية للعمل الميداني والنسوي في اليمن والمنطقة العربية. إن اختراق حساب واحد أو بريد إلكتروني قد يؤدي قسراً لتسريب قواعد بيانات العمل وملفات الضحايا الحساسة. تأمين الهوية الرقمية يبدأ ببناء جدار حماية هيكلي مشفر يعزل الحسابات ويرتقي بمستويات التوثيق والمصادقة.

General Safety Workflow: 3 Key Actions

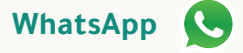


بروتوكول تأمين واستعادة بريد Google / Gmail

- افتح البريد ثم الضغط على صورة الملف الشخصي بالأعلى ثم اختيار "إدارة حسابك على جوجل" (Manage Google Account).
- الذهاب لتبويب "الأمان" (Security) من القائمة العلوية أو الجانبية لحسابك.
- النزول لأسفل والضغط على خيار "التحقق بخطوتين" (Step Verification-2) لتفعيله.
- اختيار طريقة التحقق عبر "تطبيق المصادقة" (Authenticator app) بدلاً من الاعتماد المطلق على الرسائل النصية القصيرة SMS.
- تحميل تطبيق Google Authenticator ثم فتح الحساب بالبريد والضغط على زر (+) ثم اختيار إدخال مفتاح الإعداد يدوياً (Enter a setup key) ولصق رمز التشفير المعروض بنظام بريدك لربط الكود السداسي المتغير.
- توليد رموز الاسترداد الاحتياطية (Backup codes): اضغط على رموز العشرة الاحتياطية وقومي بتصويرها وحفظها في مكان مادي آمن ومستقل: لتتمكني من استعادة حسابك في حال فقدان الهاتف أو الشريحة.
- إضافة "بريد إلكتروني للاسترداد" (Recovery email) بديل وآمن ومحمي لاستلام أكواد الإنقاذ والتحقق السري.

تحسين الحسابات وإعدادات الخصوصية المتقدمة

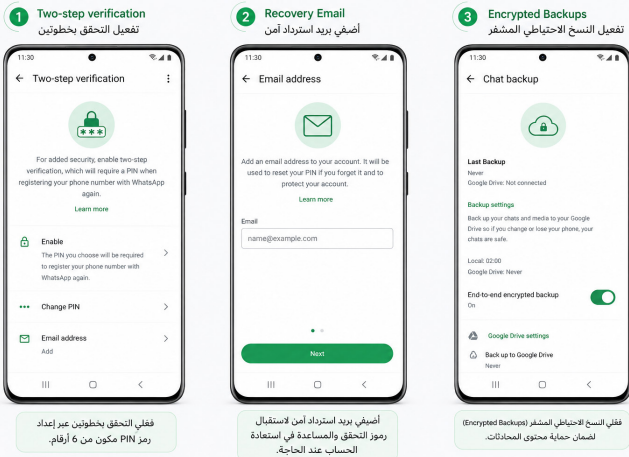
بروتوكول تأمين حساب فيسبوك (Meta) وحظر التجسس



تأمين حساب الواتساب

الإعدادات ثم الحساب ثم التحقق بخطوتين (Two-step verification) ثم تفعيل ثم إدخال رمز تعريف PIN مكون من 6 أرقام وتأكيده مع

ربط إيميل استرداد حقيقي لتجنب سحب الحساب ومصادرته.



فغلي التحقق بخطوتين عبر إعداد رمز PIN مكون من 6 أرقام.

أضف بريد استرداد آمن لاستقبال رموز التحقق والمساعدة في استعادة الحساب عند الحاجة.

فغلي النسخ الاحتياطي المشفر (Encrypted Backups) لضمان حماية محتوى المحادثات.

تشفير النسخ الاحتياطية للدرشة (Encrypted Backups)

الإعدادات ثم الدردشات ثم نسخ احتياطي للدردشات ثم تفعيل النسخ الاحتياطي المشفر بين الطرفين (End-to-end encrypted backup) برمز مرور خاص لحماية أرشيف محادثاتك من الرصد الخارجي بسيرفرات السحاب.



تأمين حسابات Signal

الإعدادات ثم الخصوصية ثم تفعيل قفل التسجيل (Registration Lock) لمنع أي جهة من إعادة تفعيل رقمك على جهاز آخر دون رمز PIN السري، مع تعطيل ميزة مؤشرات قراءة الرسائل وتثبيت التدمير التلقائي.



واجهة تطبيق Signal الرئيسية

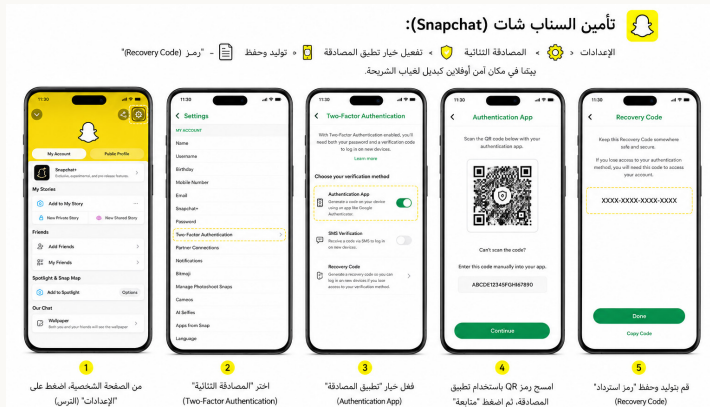
الإعدادات الرئيسية للتطبيق

من الإعدادات، اختر "Registration Lock"

فعل قفل التسجيل وأنشي رمز PIN لخاص بك.

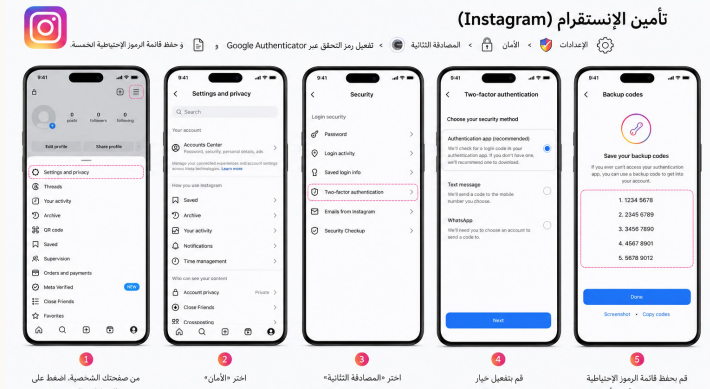
تحسين الحسابات وإعدادات الخصوصية المتقدمة

بروتوكول تأمين حساب Instagram \ X \ Snapchat



تأمين السناب شات

الإعدادات ثم المصادقة الثنائية ثم تفعيل خيار تطبيق المصادقة ثم توليد وحفظ "رمز استرداد" (Recovery Code) في مكان آمن أوفلاين كبدل لغياب الشريحة.



تأمين الإنستغرام

الإعدادات ثم الأمان ثم المصادقة الثنائية ثم تفعيل رمز التحقق عبر Google Authenticator وحفظ قائمة الرموز الاحتياطية الخمسة.



تأمين تويتر (X)

الإعدادات ثم الأمان والوصول إلى الحساب ثم الأمان ثم توثيق تسجيل الدخول (Login verification) ثم اختيار تطبيق المصادقة كطريقة أساسية ومفتاح الأمان المادي لمنع الاختراق.

تنبيه أمني وجنائي بالغ الحساسية (شريحة الهاتف ليست جدار أمان كافٍ):

نحذر بشدة من الاعتماد الفردي على الرموز المرسله عبر الرسائل النصية القصيرة (SMS) كطريقة وحيدة للمصادقة الثنائية في اليمن والمنطقة العربية؛ لأن شرائح الاتصال المحلية يسهل استنساخها، أو سحبها برمجياً من قبل مزودي الخدمة المحليين في حال توقف الرقم أو مصادره. مما يمكن المخترق من تجاوز كلمة السر وسحب الحسابات فوراً. اعتمد دائماً على تطبيقات المصادقة المستقلة مثل Google Authenticator كبوابة تشفيرية أولى لا تقبل الاختراق الخارجي.

المرونة الرقمية أثناء انقطاع الإنترنت

الأمان الرقمي في ظروف الاتصال الضعيف

في بيئات العمل الحقوقي والإنساني في اليمن والمنطقة العربية، قد يؤدي انقطاع الإنترنت أو ضعف الشبكات إلى فرض عزلة رقمية وتعميق الرقابة وتشتيت التنسيق والوصول إلى المعلومات. امتلاك بدائل اتصال مرنة وخطط طوارئ مسبقة يعد جزءاً أساسياً من السلامة الرقمية واستمرارية العمل والدفاع عن حقوق الإنسان.



الشبكات المتشابكة (Mesh Networks)
الهواتف القريبة تتحول إلى حلقات ريلي تمرر الرسائل بين عدة أجهزة للوصول إلى وجهتها. لا يستطيع الهاتف في المنتصف قراءة الرسالة.



كيف تتواصل الأجهزة دون إنترنت؟

التراسل المباشر (Peer-to-Peer)
تبادل الرسائل مباشرة بين الأجهزة دون خوادم مركزية أو مزودي إنترنت. تنتقل البيانات من جهاز لآخر بشكل مباشر ومستقل. مما يمنح الاتصال حصانة ضد الرقابة والحجب.

**ثبتيها الآن
وجربها مع فريقك.**

الاستعداد أهم من الأداة (خطوات وقائية) بدأ الاستعداد لانقطاع الإنترنت قبل حدوثه وليس بعده (تطبيقات الطوارئ)

Organic Maps

- نزلي خرائط اليمن، أو مناطق العمل مسبقاً باستخدام Organic Maps.
- احفظي المواقع المهمة ونقاط اللقاء.

Berty Chat

- احفظي برمز الاسترداد. احفظي جهات الاتصال المهمة.
- نزلي الملفات الأساسية محلياً.

Briar

- تبادل رموز QR الخاصة بالتطبيقات. أجري التطبيقات عملياً.
- اتفقي على خطة اتصال بديلة.

ماذا أفعل عند انقطاع الإنترنت؟ (بروتوكول الاستجابة)

ليست كل حالات الانقطاع متشابهة.

- إذا انقطع الإنترنت والأبراج معاً: يفضل استخدام Briar • Berty Chat • Meshenger

- انقطاع طويل الأمد:

- استخدم Meshtastic.
- اتجهي إلى نقاط اللقاء المتفق عليها.
- اتبعي خطط التواصل البديلة.

- إذا توقف الإنترنت وبقيت الأبراج بفضل: الرسائل النصية

القصيرة (SMS) والمكالمات الهاتفية.

تنبيه هام (الاتصالات التقليدية غير مشفرة، لذلك تجنبي مشاركة معلومات حساسة).

أدوات مهمة للتواصل المباشر والأوف لاين

Organic Maps

- خريطتك الآمنة دون اتصال.
- يعمل دون إنترنت
- لا يتتبع الموقع
- أقل استهلاكاً للطاقة

Meshenger

- يعتمد على Wi-Fi Direct.
- المدى: من 50 إلى 100 متر.
- لا يحتاج إنترنت.
- يدعم المكالمات والرسائل.

Berty Chat

- يعتمد على Peer-to-Peer و البلوتوث منخفض الطاقة (BLE).
- مناسب لـ:
- الفرق الصغيرة.
- التنسيق المحلي
- حالات التعقيم الكامل

Briar

- مصمم للمدافعين عن حقوق الإنسان والصحفيين. يعمل عبر البلوتوث والواي فاي المحلي.
- المدى: BT (10-100م) / واي فاي (200-500م).
- لا يحتاج لرقم هاتف.
- لا يعتمد على خادم

تجنبي:

- مشاركة مواقع الأشخاص.
- إرسال صور التجمعات.
- نشر الشائعات والأخبار غير الموثقة.
- تداول معلومات غير مؤكدة.
- تخزين بيانات حساسة غير ضرورية.

افتراضي دائماً:

- أن هاتفك قد يُفقد أو يُصادر لحظة.
- أن الرسائل قد تُقرأ.
- أن الاتصالات العادية غير مشفرة ومراقبة

نصائح أثناء الانقطاع

بروتوكول المرور من النقاط الأمنية والتفتيش العشوائي

تأمين قنوات الاتصال وتجاوز الرقابة والحجب الحكومي ومصادد الشبكات العامة في اليمن

في البيئات التي تعاني من الرقابة الممنهجة أو ضعف البنية التحتية كاليمن والمنطقة العربية، لا يمثل الـ VPN أداة لتجاوز الحجب فقط، بل طبقة إضافية لحماية الاتصال، وتقليل التتبع والمراقبة، وإدارة الثقة بالشبكات اللاسلكية والفيزيائية.

• مخاطر شبكات الواي فاي العامة ومصادد الميدان

المقاهي - الفنادق - المطارات - مساحات العمل المشتركة - الشبكات غير الموثوقة

Man-in-the-Middle



اعتراض البيانات وتصفحك الجاري بين الهاتف ومودم الشبكة العامة مباشرة، مما يتيح للمهاجم المتصل بنفس الشبكة رصد كلمات المرور والملفات غير المشفرة.

Evil Twin Attack



إنشاء شبكة واي فاي وهمية من قبل مهاجم تحمل نفس اسم شبكة المكان الأصلية وتسهل انضمام هاتفك إليها تلقائياً لاعتراض اتصالاتك بالكامل وسرقتها.

الصفحات المزيفة والتحديثات الوهمية



تقوم بعض الشبكات العامة بإعادة توجيه تصفحك لصفحات كاذبة وإجبارك على تنزيل تحديثات برمجية وهمية لاختراق الهاتف بالكامل وزرع برمجيات التجسس الخبيثة.

مصروفة شبكات الـ VPN المفتوحة المصدر والموصى بها للنشاط الحقوقي

استخدمي هذه الحلول المشفرة والمفتوحة المصدر الموثوقة لتفادي الرقابة وفحص الحزم DPI باليمن.

Geph (جيف)

مجاني ومفتوح المصدر - مستوى حماية مرتفع

Proton VPN

مجاني ومفتوح المصدر - مستوى حماية مرتفع جداً

Psiphon

مجاني ومفتوح المصدر - مستوى حماية مرتفع

Outline VPN

مجاني ومفتوح المصدر - مستوى حماية مرتفع

Orbot (Tor)

مجاني ومفتوح المصدر - مستوى حماية مرتفع

تجنبني تخزين:

- ✓ صور الهويات والوثائق الحساسة.
- ✓ قوائم المستفيدين أو الضحايا.
- ✓ كلمات المرور ورموز الاسترداد.
- ✓ أرشيفات المشاريع القديمة.
- ✓ الصور ولقطات الشاشة غير الضرورية.

• إذا اضطررتِ مرغمة لاستخدام الواي فاي العام، طبّقي هذه الخطوات التكتيكية فوراً:

3 · AFTER DISCONNECTION



قومي بعمل نسيان للشبكة **Forget Network** فوراً لمنع الاتصال التلقائي لاحقاً.

2 · DURING CONNECTION



أولاً وقبل فتح أي تطبيق أو متصفح، تفعيل خيار تصفح **HTTPS Only** بالكامل، تجنبى نهائياً تنزيل البرامج أو التحديثات الميدانية، وتجنبى تماماً الوصول للحسابات البنكية والمالية.

1 · BEFORE CONNECTION



تأكدي من اسم الشبكة الصحيح من إدارة المكان. أوقفى ميزة "الاتصال التلقائي بالشبكات" تماماً. فعلى ميزة عنوان **MAC** عشوائي لإخفاء هوية هاتفك المادية ومنع تتبع حركتك.

[SCREENSHOT B: FORGET NETWORK DIALOG]

[SCREENSHOT A: ANDROID WIFI SETTINGS - RANDOMIZED MAC]

DNS المشفر - Cloudflare / Quad9

يفضل استخدام:

اعتماد مزود **DNS** مشفر وموثوق لمنع تسريب استعلامات التصفح وتفاذي التوجيه القسري.

RethinkDNS - جدار حماية الهاتف (مفتوح المصدر)

من أقوى أدوات الحماية الذاتية لأجهزة أندرويد. يوفر نظام **DNS** مشفر، جدار حماية محلي، حجب أدوات التعقب والإعلانات، ومراقبة دقيقة لكافة التطبيقات التي تحاول الاتصال بالإنترنت لمنع تسريب الملفات بالخلفية.

• خصائص الـ VPN التي يجب تفعيلها

- تأكدي من تفعيل هذه الخيارات لحماية اتصالاتك:
- تفعيل **Kill Switch** لإيقاف النت فوراً عند تعثر النفق.
- تفعيل **Always-on VPN** لمنع تسرب البيانات خارج النفق.
- اعتماد بروتوكول **WireGuard** لسرعة وثبات أفضل باليمن.
- تفعيل ميزة **Split Tunneling** لتمرير تطبيقات محددة فقط بالنفق.
- استخدام خاصية التمويه **Obfuscation** لتجاوز فحص الحزم **DPI**.
- إقران الـ **VPN** مع تشفير نظام الـ **DNS** المدمج بالهاتف.

تطبيقات الـ VPN التجارية والسرية الكاذبة (تجنبها تماماً كأدوات):

نحذر بأشد العبارات من الاعتماد على تطبيقات الـ **VPN** التجارية المجانية ومجهولة المصدر المتوفرة على المتاجر؛ لكونها مغلقة المصدر وتعمل كأدوات تتبع ومصادد للبيانات. تقوم هذه الشركات بجمع بياناتك وبيع سجل تصفحك وزياراتك للمعلنين، أو فك تشفير البيانات وتسريب حركة مرورك للجهات المراقبة. وبعضها يزرع برمجيات تتبع خبيثة تخرق خصوصية الأجهزة بالخلفية. اعتمدى فقط على الـ **VPN** اللامركزي وغير التجاري الموصى به بالدليل.

× Hola × SuperVPN × Turbo VPN × Proxy Master

جدار الحماية الذاتي (شبكات ال VPN والشبكات العامة)

الخطوات السليمة فنياً وجنائياً لالتقاط
وحفظ الأدلة الرقمية لضمان سلامتها
القضائية وسرية الضحية



Fingerprint



Archive



Capture

أولاً: بروتوكول التقاط لقطات الشاشة (Screenshots) المقبولة

تجنبي التقاط صور مبتورة: اتبعي الخطوات السليمة فنياً وقانونياً.

- إظهار المعرف الرقمي (User ID) وتفاصيل الحساب

لا تكتفي بلقطة للمحادثة: بل ادخلي الملف الشخصي للمبتز والتقطي صورة تظهر المعرف الفريد الثابت (User ID) ورقم هاتف الجاني صراحة. فاسم المستخدم المكتوب سهل التعديل والتهرب، بينما المعرف الرقمي مادي وثابت.

- تجنب الاقتصاص (No Cropping) أو التعديل الفني

التقطي الشاشة كاملة بحيث تظهر شريط الحالة العلوي للهاتف (مستوى الإشارة والبطارية). طابع الوقت والتاريخ التلقائي. والرسالة في سياقها الكامل: فالإقتصاص يثير تهمة فبركة الدليل ويعطل قبوله قضائياً.

- تزامن طابع الوقت والمنطقة الزمنية (Timestamping)

تأكدي من توثيق التوقيت والمنطقة الزمنية (GMT) بدقة لربطها ببيانات مزودي الخدمة المحليين لاحقاً لإثبات حيازة المتهم للحساب وقت الهجوم. مع الحفاظ على التدرج السليم للمحادثة.

• ثانياً: أرشفة الويب وتجميد الأدلة الرقمية

أدوات تمنع الجاني من حذف الحساب والتوصل من مسؤوليته الجنائية.

أدوات الأرشفة اللامركزية:

إذا نشر المبتز تشهيراً على ويب أو شبكات تواصل، استخدم **Archive.today** أو **Archive.org** لحفظ وتجميد نسخة مادية ثابتة من الرابط تمنع الجاني من التملص بحذف المنشور لاحقاً.

استخراج ال User ID المادي:

الاسم الظاهر (Username) يمكن تعديله بلحظة. استخدم أدوات استخراج المعرفات (مثل بوتات **Telegram ID** أو أدوات استخراج **Facebook UID**) لتحديد الرقم التسلسلي الفريد لحساب الجاني.

ترويسة البريد (Email Headers):

عند تلقي رسالة تهديد بالبريد، قومي بتحميل الملف الأصلي للرسالة بصيغة **eml**. واستخرجي الترويسة الكاملة لتحديد عنوان ال IP الحقيقي ل خادم الإرسال وتجاوز انتحال الهوية.



رسم توضيحي لبوت استخراج
معرفات التليجرام (ID)

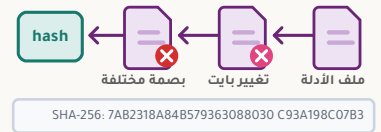


• ثالثاً: بصمة الدليل الرقمي (Metadata & Hash Value) وضمان عدم العبث الفني

تطبيق الممارسات الرياضية لإثبات نزاهة ملف الأدلة المادية ومنع الطعن فيه قضائياً.

1 بصمة الملف الرياضية (SHA-256)

قيمة ال Hash هي خوارزمية رياضية فريدة تُؤد بصمة رقمية لأي ملف أدلة (Evidence Package). أي تغيير ولو بنقطة واحدة بالملف يغيّر البصمة كلياً، مما يثبت أمام النيابة العامة عدم تعديل الأدلة منذ التقاطها.



2 توليد البصمة أوفلاين

لإثبات سلامة الأدلة، يمكن إنشاء بصمة رقمية للملفات (SHA-256) باستخدام أدوات مجانية مثل **QuickHash** أو **OpenHashTab** أو الأدوات المدمجة في نظام التشغيل، ثم حفظها مع ملف التوثيق لتعزيز موثوقية الأدلة وقيمتها القانونية.

الحفاظ على الملفات الخام (Raw)

تجنبي تماماً إرسال الصور ولقطات الشاشة عبر تطبيقات تقلل الجودة وتعديل الميتاداتا (مثل الرفع العادي بالواتساب). احفظيها كملفات خام أولية (Raw Documents) غير مضغوطة داخل مجلد مشفر لحين طلب المحكمة.



مواجهة الابتزاز الرقمي الموجه (الجانب التقني)

خطة الاستجابة الفورية والخطوات التقنية الطارئة للناشطة فور تعرض حساباتها للاختراق، أو تسريب بياناتها الحساسة، أو مواجهة حملات ابتزاز إلكتروني تهدف لتشويه سمعتها السياسية أو الشخصية.

يُعد الابتزاز الرقمي أحد أخطر أشكال العنف الرقمي الموجه ضد المدافعات والقيادات النسوية، حيث يستخدم المهاجم الحسابات المخترقة أو الصور الخاصة أو الملفات الحساسة لإسكات الأصوات وتقويض النشاط الحقوقي والمجتمعي. تذكر جيداً: المبتز لا يستمد قوته من قدراته التقنية بقدر اعتماده التام على الخوف والعزلة والشعور بالعار.

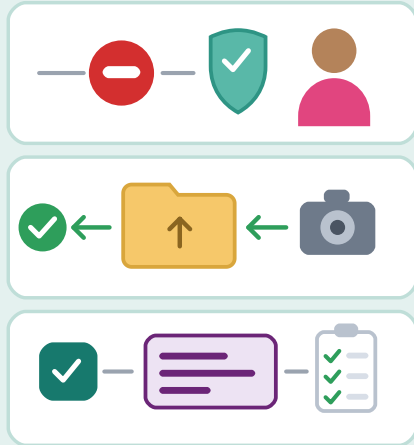
القاعدة الأساسية:

الهاك = صفر | التفاوض = صفر



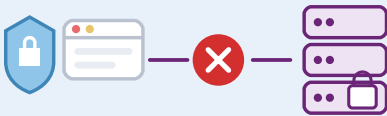
كلما انخفض مستوى التفاعل مع المبتز، انخفضت قدرته المطلقة على التحكم والضغط.

1 أولاً: بروتوكول الساعة الأولى من الابتزاز



- أوقفني التجاوب كلياً أو التفاوض مع المبتز.
- احتفظي بالرسائل والروابط وتجنبي إرسال صور أو ملفات جديدة.
- التقطي صور شاشة كاملة، وتجنبي حذف المحادثات أو الأدلة.
- سجلي الحسابات والأرقام.
- حظر المبتز قبل التوثيق.
- الإبلاغ الفوري للمنصات.
- طلب إزالة المحتوى.
- الاستعانة بجهة حقوقية.

2 ثانياً: احتواء الحادث وعزل الكارثة الرقمية



سحب التطبيقات المرتبطة:

إلغاء التطبيقات الخارجية غير المعروفة، ملحقات المتصفح، رموز OAuth القديمة، والخدمات المرتبطة غير الضرورية.

قطع وصول المهاجم:

- تسجيل الخروج من جميع الأجهزة.
- إزالة الجلسات النشطة.
- تغيير كلمات المرور ووسائل الاسترداد.
- استبدال رموز المصادقة الثنائية (2FA).

مواجهة الابتزاز الرقمي الموجه (الجانب التقني)

3 ثالثاً: استعادة السيطرة على الحسابات (سلسلة الأولويات)

البريد الإلكتروني هو مفتاح استعادة معظم الحسابات الأخرى، ولذلك يجب تأمينه أولاً وفقاً للتدرج التالي:



4 رابعاً: الحد من انتشار المحتوى على الشبكة

1 طلبات إزالة المحتوى (DMCA):

إزالة الصور والملفات المنشورة من المواقع والخوادم المستضيفة.

2 طلبات إزالة النتائج من Google:

لحذف الصور الخاصة، الوثائق الشخصية، والبيانات الحساسة كلياً من نتائج البحث.

3 الإبلاغ للمنصات:

تفعيل الإبلاغ العاجل (التشهير، والابتزاز بالصور الحميمة غير الرضائية) لدى المنصات التالية.



تحذير أمني واستراتيجي بالغ الخطورة (الرضوخ للمطالب يمول تكرار الهجوم):



إن دفع المبالغ المالية للمبتز، أو محاولة تقديم تنازلات مهنية أو سياسية، أو الامتنثال لتهديداته بإرسال المزيد من الملفات والصور لتجنب الفضيحة؛ هو تصرف كارثي ومدمر كلياً لسلامتك الجسدية والرقمية؛ حيث يثبت للمخترق فاعلية سلاحه، ويمول خواتمه وخطوط هجومه، ويدخل الضحية في ابتزاز متكرر. واجه الموقف كحادث فني بارد، واقطعي الاتصال بالمبتز تماماً، واجعلي الهاكر يساوي صفراً.

مواجهة حملات التشويه الممنهجة والجيوش الإلكترونية (الذباب الرقمي)

● بروتوكول البلاغات الجماعية المنسقة (Mass Reporting & Solidarity Routing)

عند استشعار بدء حملة تشويه أو تشهير منظمة وممولة، يجب فوراً حظر منافذ التجسس والتسلل إلى مساحتك وعائلتك وتطبيق القيود الأمنية التالية في أول 60 دقيقة:

إعداد "ورقة البلاغات الفنية" (Shared Reporting Sheet):

تقوم خلية التوثيق الصديقة بإنشاء ملف مشترك (مشفر) يحتوي فقط على الروابط المباشرة للحسابات والمنشورات المحرصة والمسيئة. وتحديد نوع الانتهاك الدقيق المتوافق مع شروط المنصات (تشهير منظم، كراهية قائمة على النوع الاجتماعي، تحريض مادي على العنف).

تنسيق قنوات التضامن (Solidarity Routing):

تعميم ورقة البلاغات فوراً على شبكات التضامن النسوية والحقوقية الموثوقة محلياً وإقليمياً، لتنسيق إرسال بلاغات مكثفة في توقيت موحد (الاتفاق على تفعيل البلاغات من قبل 100 ناشطة في نافذة زمنية لا تتجاوز 15 دقيقة)؛ مما يجبر خوارزميات السلامة في المنصة على تعليق الحسابات المستهدفة تلقائياً لحين المراجعة البشرية.

تفعيل قنوات الدعم السريع والشركاء الموثوقين:

راسلي فوراً قنوات الاتصال المباشرة والساخنة المفتوحة للشركاء، تمتلك هذه الجهات خطوط اتصال ساخنة ومدعومة (Trusted Partner Channels) تتيح سحب وحظر منشورات التحريض وحماية حياة المدافعة في غضون دقائق معدودة بعيداً عن البيروقراطية البرمجية التقليدية.

● إدارة المخاطر الاجتماعية والقبلية في السياق اليمني والمنطقة العربية

تكتيكات باردة لصيانة السمعة وامتصاص الضغط العائلي لحمايتك من التفكير المجتمعي:

تكتيك "إحباط سلاح الوصمة":

صياغة رواية تقنية محايدة وباردة (مثال: "تعرضت حساباتنا لاختراق وهجوم إلكتروني منسق ومستهدف بالصور المفبركة والمنشورات الكاذبة") ومشاركتها فوراً مع كبار العائلة والقبيلة والدوائر المقربة لامتصاص الصدمة وتجريد المهاجم من سلاح الفضيحة والتهديد الاجتماعي والقبلي ومصادرتة كلياً.

إيقاف النشر المساعد:

تجنبي إظهار أي نشاط غير مهني أو نشر قصص (Stories) جانبية أثناء الحملة لتجنب إعطاء المهاجمين فرصة لاستخلاص ثغرات إضافية أو استخدام صورك الجديدة في المفركة

كسر العزلة الرقمية وبناء شبكة الدعم والمساندة المتخصصة

تفكيك قوى المبتز (الخوف - العزلة - الشعور بالعار)

كسر الصمت والوصمة الاجتماعية هو سلاح الضحية الأول:

كسر سلاح الصمت: عاملي الحادث كملف تقني وقانوني يمكن احتواؤه، وافصلي كلياً بين هجوم المبتز وقيمتك الشخصية السامية.
لا تواجهي الأزمة وحدك: كلما زادت العزلة زادت قوة المبتز، وتوسيع دائرة الدعم الآمن (شخص موثوق، خبير سلامة، مستشار قانوني، منظمة مختصة) يسلب المهاجم قدرته على الضغط.

جهات الدعم والمساندة المتخصصة (روابط الاتصال المباشر عناوين الاستجابة):

StopNCII

كيف تعمل؟ بدلاً من رفع صورك الحساسة للخارج، يقوم الموقع بإنشاء بصمة تشفيرية رياضية (Hash) محلياً على جهازك دون رفع الصورة الأصلية، وتُرسل هذه البصمة لشركاء المنصة (ميتا، تيك توك، وغيرهم) لمنع رفع أو تداول هذه الصور كلياً. متى تستخدم؟ عند التهديد بنشر صور خاصة، أو عند حدوث تسريب فعلي، أو اختراق الأجهزة، حتى وإن لم يقم المبتز بالنشر بعد.



StopNCII.org
Stop Non-Consensual Intimate Image Abuse



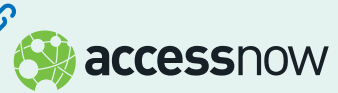
SMEX Helpdesk

دعم رقمي سريع لحوادث العنف والابتزاز، استشارات تقنية متخصصة وحماية الحقوق الرقمية في المنطقة العربية.



Front Line Defenders

توفير الحماية والدعم العاجل والاستشارات الأمنية والقانونية الفورية للمدافعات عن حقوق الإنسان المعرضات للمخاطر



Access Now Helpline

استجابة تقنية طارئة على مدار الساعة، دعم استعادة الحسابات المخترقة، وتحليل الحوادث الأمنية للمدافعين والمنظمات.



YODET Organization

منظمة يمنية محلية رائدة تقدم التوعية بالأمن الرقمي، دعم وإحالة النساء والفتيات والمبادرات المجتمعية في اليمن



Urgent Action Fund

تقديم الدعم المالي الطارئ والاستجابة السريعة والمنح العاجلة لحماية المدافعات والقيادات النسوية بالميدان.



Speak UP Platform

منصة نسوية توفر مساحة آمنة للنساء والفتيات لمواجهة الابتزاز والعنف الرقمي، وتوفير الإحالة والدعم المجتمعي التمكيني

لا يقتصر طلب الدعم على المنظمات الدولية والخطوط الساخنة الخارجية؛ فوجود مستشارات وخبرات حماية وسلامة رقمية محليات وموثوقات يوفر دعماً سريعاً وأكثر فهماً للسياق اليمني والعربي، ويساعد المدافعات والقيادات النسوية على الاستجابة الآمنة للحوادث الرقمية، والتعامل مع الابتزاز وحملات التشهير، وحماية الخصوصية، وتوثيق الأدلة وحفظ الحقوق.

توثيق الأدلة وحفظ الحقوق (الجانب التقني والقانوني)



سرية الضحية وتطهير مبادرات الأدلة قبل مشاركتها

- عند إرسال ملفات الأدلة لجهات دعم قانوني أو أممي، تذكر أن لقطات الشاشة والصور تسجل مبادرات (Metadata) تكشف موقعك الجغرافي، ونوع هاتفك وهويتك ومحيطك.
- قومي بتطهير الأدلة كلياً من المبادرات الخاصة بك باستخدام أداة Scrambled Exif (مفتوح المصدر).
- مع إبقاء مبادرات الجاني سليمة دون مسّ؛ لضمان أمانك الشخصي وسريتك التامة.

حفظ الدليل وحمايته من التلف أو الطعن القانوني

سجل النقل (Log):

توثيق أسماء الأشخاص الذين اطلعوا على الأدلة وتواريخ استلامهم لها لمنع تسريبها.

الاحتفاظ بالأصل:

عدم استخدام الهاتف الأساسي الذي يحمل الأدلة بعد تجميده، والتبديل لهاتف طوارئ.

تجنب التعديل العرضي:

عدم تشغيل أي برامج تنظيف تلقائية قد تحذف كاش الأدلة والملفات المؤقتة.

المراجع المستخدمة في الدليل

هيئة الأمم المتحدة للمرأة (2022): تقرير "العنف ضد المرأة في الفضاء الرقمي: نظرة عامة والممارسات القانونية الجيدة في الدول العربية" [التقرير الإقليمي الكامل لعام 2022](#). PDF⁸

هيئة الأمم المتحدة للمرأة، واليونسكو، والمركز الدولي للصحفيين (2025): تقرير "نقطة التحول: التصاعد المقلق للعنف الرقمي ضد النساء في المجال العام في عصر الذكاء الاصطناعي". [Tipping Point Report 2025](#) PDF⁴¹

منظمة اليونسكو والمركز الدولي للصحفيين (UNESCO & ICFJ - 2021): دراسة "The Chilling: الاتجاهات العالمية للعنف الإلكتروني ضد الصحفيات". [UNESCO "The Chilling" Study](#)⁵⁰

مرصد الحريات الإعلامية في اليمن (2022): تقرير التنمر والابتزاز الإلكتروني ضد الصحفيات والناشطات والآثار الاجتماعية للوصمة والرقابة الذاتية دراسة مرصد الحريات الإعلامية لعام 2022.⁴⁹

مجلس الأمن التابع للأمم المتحدة (2000): القرار رقم 1325 بشأن المرأة والسلام والأمن وتأكيد دور النساء في تسير لجان الوساطة. [S/RES/1325 \(2000\)](#) PDF³⁸

الجمعية العامة للأمم المتحدة (1979): اتفاقية القضاء على جميع أشكال التمييز ضد المرأة (سيداو) كأداة للمناصرة وبناء الرسائل السياسية [Convention on the Elimination of All Forms of Discrimination Against Women](#) PDF⁵¹

الجمعية العامة للأمم المتحدة (1998): إعلان حماية المدافعين عن حقوق الإنسان (حق ومسؤولية الأفراد والجماعات في تعزيز الحقوق). [UN Declaration on Human Rights Defenders - OHCHR Portal](#)⁵²

المفوضية السامية لحقوق الإنسان بالأمم المتحدة (OHCHR - 2020): تقرير المقرر الخاص المعني بالعنف ضد المرأة حول مكافحة العنف ضد الصحفيات والمراسلات. [UN Report A/HRC/44/52](#) PDF³

منظمة فرونت لاين ديفنדרز (Front Line Defenders): الأدلة والبروتوكولات الحمائية لتأمين المدافعات عن حقوق الإنسان (WHRDs) المعرضات للمخاطر. [Protection Manual for Human Rights Defenders](#) PDF⁵³

منصة StopNCII.org بالشراكة مع (SWGfL): تكنولوجيا التجزئة الإدراكية لإنشاء بصمة الصورة لحماية الخصوصية ومنع انتشار المحتوى الحساس [StopNCII Platform](#)⁵⁴ و [Privacy Policy](#)⁵⁴

أدلة تشغيل البرمجيات والتطبيقات الموصى بها بالدليل: وثائق الاستخدام الرسمية لتطبيقات (Briar Project [Signal Messenger](#) [RethinkDNS](#) [Shelter App](#) [Aegis Authenticator](#))³⁴

الخاتمة:

يضع دليل المناصرة الرقمية النسوية بين يديك الخطوات الأساسية لتخطيط حملاتك، وصناعة سرديتك، وتأمين سلامتك الرقمية.

إن حضورنا الرقمي هو امتداد مباشر لعملنا وصمودنا في الميدان وحماية لأصواتنا المستقلة، والتدابير التقنية ليست إلا وسائل لتأمين هذا الحضور. نتطلع أن يمثل هذا الدليل مرجعاً عملياً يرافقك ويساندك في بناء مساحات رقمية حرة، آمنة، ومؤثرة.