الأمن الشامل

إرشادات أساسية لمواجهة العنف القائم على النوع الاجتماعي

2024

المقدمة:

تم إعداد هذا الدليل بالتعاون مع، ومن أجل، الناشطات والمدافعات عن حقوق الإنسان من النساء في العراق. تلعب الناشطات العراقيات دورًا حيويًا في المطالبة بالمساواة في الحقوق والفرص للنساء والفتيات في جميع أنحاء البلاد، وفي مواجهة مستمرة مع العنف الجنسي والقائم على النوع الاجتماعي الذي تعاني منه العديد من النساء. وعلى الرغم من أن وتيرة التقدّم بطيئة، فقد مكّن هذا العمل الجوهري النساء من استرداد مساحات (عامة) كانت حكرًا على الرجال سابقًا. ومع ذلك، فإن هذا العمل، اليوم أكثر من أي وقت مضى، يرتبط بمخاطر أمنية وسلامة خاصة بالنشاط المتعلق بالعدالة بين الجنسين.

في الوقت الذي يُكتب فيه هذا الدليل، يشهد العراق موجةً من الهجمات المضادة على قضايا النوع الاجتماعي، تستهدف بشكل خاص الناشطات النسويات ومنظمات حقوق المرأة. لا يقتصر استهدافهن على التدقيق الأخلاقي والديني في عملهن، بل يشمل أيضًا حملات تشهير واعتداءات جنسية وعنفًا، سواء عبر الإنترنت أو خارجه، إلى جانب تزايد الشعور بعدم الأمان في الفضاءات العامة، واعتقالات وتهديدات، بل وفي أسوأ الحالات، اغتيالات. لذلك، هناك حاجة ملحة لتعزيز المعرفة بالأمن الشامل والسلامة، وزيادة الوعي والممارسات الجماعية، حتى تتمكن الناشطات والمنظمات النسوية من الاستمرار في نضالهن من أجل المساواة والعدالة.

يعتمد هذا الدليل إلى حدّ كبير على نهج وقائي، حيث يوفّر أدوات وتكتيكات سهلة الاستخدام تهدف إلى تعزيز السلامة والأمن، ودعم الصحة الجسدية والنفسية للناشطات في العراق. يتضمن الدليل موارد رقمية يمكن للمستخدمات الاستفادة منها مباشرة عبر الإنترنت أو تحميلها. أما الجزء الأخير من الدليل، فهو يتناول بشكل تفاعلي سيناريوهات شائعة — للأسف تواجهها الناشطات، مع عرض للإجراءات الأساسية التي يمكن اتخاذها في مثل تلك الحالات.

يُعد هذا الدليل وثيقة حيّة، وسيتم تحديثه بانتظام بما يتماشى مع تطورات الوضع الأمني.

تنويه:

المعلومات والنصائح والتوصيات (بما في ذلك البرامج والتطبيقات المُقترحة) الواردة في هذا الدليل تهدف فقط إلى توفير معلومات عامة. وعلى الرغم من أن مؤلفي هذه الوثيقة حرصوا على تقديم معلومات دقيقة قدر الإمكان في وقت النشر، فإن كل تهديد ومستوى خطر يختلف باختلاف السياق، ويتطلب استجابات محلية، فريدة، ومُحدّثة تقع خارج نطاق هذا الدليل التثقيفي. على المستخدمين اتخاذ قرارات مستنيرة عند اعتماد التوصيات الواردة أدناه بناءً على احتياجاتهم، وملفاتهم الشخصية، وسياقاتهم، ومواردهم.

جميع الموارد والأدوات المذكورة في هذا الدليل هي مجرد توصيات، ومشاركتنا لها لا تعني تأييدنا لها أو وجود أي تعاون أو إحالة أو علاقة شراكة مع المنظمات أو المطورين المالِكين لهذه الأدوات والموارد. كما أن مؤلفي هذا الدليل لا يقدمون أي ضمان أو كفالة من أي نوع، صريحة كانت أو ضمنية، فيما يتعلق بالخدمات التي تقدمها أطراف ثالثة نتيجة لهذه التوصيات.

النهج الشامل للأمن:

يشير مفهوم «الأمن الشامل» إلى استخدام تقنيات وتكتيكات متكاملة تهدف إلى حماية السلامة الفردية أو الجماعية، من خلال تأمين السلامة الجسدية والرقمية والنفسية-الاجتماعية للفرد أو المجموعة.

صدر دليل الأمن الشامل للمدافعين عن حقوق الإنسان، الذي أعدته منظمة تاكتيكال تك (Tactical Tech)، في عام ٢٠١٦، وكان نقطة تحوّل في كيفية تأطير مفهوم الأمن للمدافعين عن حقوق الإنسان، حيث عرّفه على أنه: «الرفاهية أثناء العمل؛ أن نكون بصحة جسدية وعاطفية جيدة، ونحافظ على أنفسنا بينما نواصل العمل الذي نؤمن به.»

يعكس هذا النهج عمداً كلمات أودري لورد القوية: «العناية بنفسي ليست رفاهية، بل هي حفظ للذات، وهذا بحد ذاته فعل من أفعال الحرب السياسية.» وقد تُرجم هذا المفهوم إلى الممارسة من خلال تقديم مجموعة من الاعتبارات التي تدمج بين جوانب الأمن والحماية والرفاهية المختلفة في إطار عملي يعزز الصمود. ويعني ذلك أيضًا أن مفهومنا للأمن هو في جوهره مسألة شخصية، ذاتية، ومُحمّلة بالبعد المبني على اساس الجنس.

تُعد المكونات الأساسية لإطار الأمن الشامل عناصر يجب الرجوع إليها باستمرار ودمجها في التخطيط الاستراتيجي للأمن الفردي والجماعي والمؤسساتي، وذلك وفقًا لخطوات: التحضير، الاستكشاف، وضع الاستراتيجية، والتنفيذ.

من الضروري الإقرار بأنه لا توجد حلول أو استراتيجيات موحدة تصلح للجميع. فلكي نتمكن من تقديم استجابة دقيقة وفعالة، لا بد من فهم السياق والظروف المحددة التي نهدف إلى التدخل فيها أو تطوير استراتيجية لها. وفي هذا الإطار، فإن القدرة على توفير مساحة للتعامل مع هذا النهج الوقائي تجاه السلامة تمُكّننا من الاستعداد بشكل أفضل لتقديم استجابة فورية عند الحاجة.

في بعض الحالات، يمكن أن يكون إنشاء «مسار» أو مجموعة من الخطوات المتّبعة وسيلة فعّالة لسد الفجوات المتعلقة بإمكانية الوصول إلى المعلومات أو تطوير المهارات. ومن خلال مراجعة هذا المسار بشكل جماعي كفريق أو كمنظمة، يمكن لعدد أكبر من الأشخاص أن يتعرّفوا على أفضل الممارسات المتعلقة بالسلامة، وأن يشاركوا بملاحظاتهم حول التحديات المحتملة، مما يعزز من النهج الجماعي للأمن من خلال ضمان إطلاع جميع أفراد الفريق على الخطط الأساسية المتفق عليها للتعامل مع مختلف السيناريوهات، وكيفية تكييف هذه الخطط بما يتناسب مع كل حالة على حدة.

في هذا الدليل، سنستعرض بعض المبادئ الأساسية، والتوصيات، والأدوات، والموارد التي تساعد في تطوير خطط أمن شامل يمكنها الاستجابة للمخاطر التي حددناها من خلال نموذج التهديد الخاص بنا. إن نموذج التهديد يختلف من شخص لآخر ومن منظمة لأخرى، كما أنه يتغيّر باستمرار.

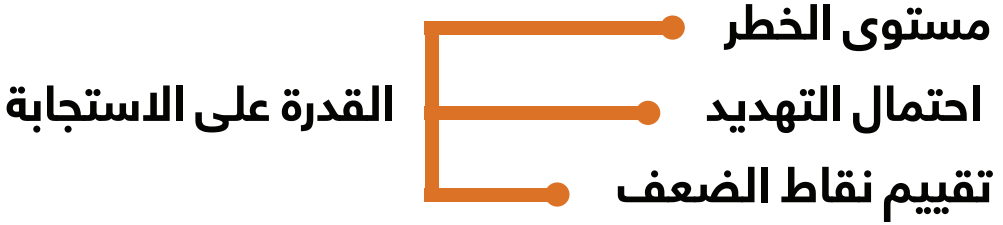
إذا كنتِ تعتبرين أن عملكِ حساس، فقد يكون من المفيد القيام بتمارين نمذجة التهديد هي عملية منهجية تُستخدم لتحديد وتحليل وتقييم التهديدات الأمنية المحتملة التي يمكن أن تستهدف نظامًا، مؤسسة، أو حتى فردًا، بهدف اتخاذ تدابير وقائية قبل وقوع الخطر. بشكل دوري كل ستة أشهر، وكذلك قبل تنفيذ أي نشاط قد يزيد من مستوى ظهوركِ أو تعرّضكِ للخطر.

نمذجة/ تحليل التهديدات:

يساعد نمذجة التهديدات في زيادة الوعي بالأولويات التي قد يرغب الشخص في التركيز عليها عند تحديد الخطوات التالية لإعادة بناء أمنه وسلامته بشكل شامل. وللبدء في إعداد خطة أمنية تشمل الجوانب النفسية-الاجتماعية، الجسدية، والرقمية، من المهم أخذ الأسئلة التالية بعين الاعتبار:

١. ما الذي أريد حمايته؟
٢. ممّن أريد حمايته؟
٣. ما مدى خطورة العواقب إذا فشلت في حمايته؟
٤. ما احتمالية أن أحتاج إلى حمايته؟
٥. هل توجد حوادث حالية أو أنماط أو تهديدات مرتبطة به؟
٦. هل سبق أن وقعت حوادث أو تهديدات تتعلق به؟
٧. هل يمكنني حمايته ومنع العواقب بنفسي؟
٨. من هم حلفائي، وكيف يمكنهم دعمي؟

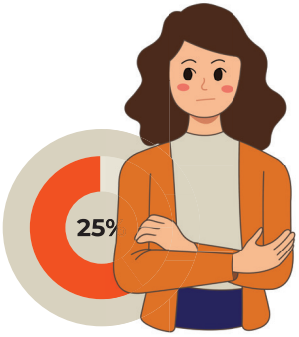
بمجرد أن تجيب على هذه الأسئلة، يمكنك استخدام معادلة المخاطر من خلال تقييم كيفية استغلال التهديد لنقاط الضعف الحالية لديك، وتحديد القدرات المتوفرة لديك حاليًا لتقليل احتمالية وقوع التهديد أو الحد من شدة آثاره.



مستوى الخطر:

يساعد نمذجة التهديدات في زيادة الوعي بالأولويات التي قد يرغب الشخص من خلال معادلة المخاطر، نحدد مستوى الخطر على أنه احتمال حدوث شيء ما وشدة تأثيراته. يمكن ترجمة هذا إلى الفئات التالية:

1.



مستوى الخطر المنخفض:

من غير المحتمل حدوث التهديد، ولكن إذا حدث، فقد قمت بمعالجة أي نقاط ضعف قد تعرضك لأضراره، ولديك الموارد والأدوات والشبكات اللازمة للحد من تأثيراته إلى أدنى حد. تشعر بالثقة في قدرتك على الاستجابة. لديك الوقت للتحضير. قدرة استجابتك تفوق أو تتساوى مع التأثيرات المحتملة للتهديد.

2.

مستوى الخطر المتوسط:

يوجد احتمال كبير لحدوث التهديد أو أنه قائم حالياً. أنت معرض لبعض أضراره. قد لا تشعر بالثقة الكافية أو تكون غير متأكد من الموارد والأدوات والشبكات التي تمتلكها حاليًا للحد من تأثيراته إلى الحد الأدنى. لديك الوقت للتحضير أو يمكن للإجراءات الحالية أن تمنحك بعض الوقت لتحسين قدرة استجابتك. قدرة استجابتك بالكاد تتساوى مع أو تتفوق عليها التأثيرات الحالية والمحتملة للتهديد (الحالي او المحتمل).

3.

مستوى الخطر العالي:

التهديد مستمر. أنت معرض تمامًا لأضراره ولا تمتلك الموارد والأدوات والشبكات اللازمة للتعامل مع تأثيراته. ليس لديك وقت للتحضير أو لتحسين قدرة استجابتك. لا يمكنك الاستجابة لتأثيرات التهديد وتحتاج إلى العثور على دعم طارئ (جسدي، طبي، نفسي، رقمي، أو حتى النظر في خدمات الانتقال).

1.

احتمالية التهديد:

تشير إلى مدى احتمالية تنفيذ خصومك للتهديد، أو أن التهديد سيحقق أهدافهم، مثل الاسكات، أو الترهيب، أو الردع عن المشاركة السياسية، أو فرض الرقابة، أو الإضرار (سواءً بسلامتك الجسدية، أو الرقمية، أو النفسية، أو بسمعتك ومكانتك داخل المجتمع). قد تستهدف هذه التهديدات فردًا، أو منظمة/مجتمعًا/مجموعة، أو كليهما.

2.

تقييم نقاط الضعف:

يُشير هذا إلى مدى وعيك بأي فرص قد يستغلها خصومك لتقويض سلامتك في أي بُعد (جسدي، رقمي، نفسي، اجتماعي). يمكنك تحديد نقاط ضعفك من خلال تحديد المهارات التي قد تحتاج إلى تطويرها أو تعزيزها، والتي قد تتضح أكثر مع التعمق في تمرين نمذجة/تحليل التهديدات الموصى به في القسم السابق.

3.

القدرة على الاستجابة:

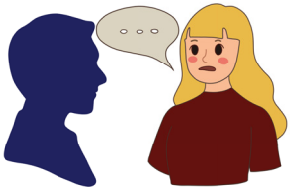
تشير إلى مدى توافر الموارد والأدوات والمهارات والشبكات والدعم لديك لمواجهة المخاطر والاستجابة لآثارها. من المهم أن تُتابع هذه الموارد، وأن تفكر في مدى سهولة الوصول إليها عند الحاجة إليها أثناء الأزمات. فكّر في التواصل مع زملائك والشبكات التي قد تدعمك لاطلاعهم على مستوى المخاطر الحالي لديك واحتياجاتك، لوضع توقعات واتفاقيات وقائية.

بعد تحديد المخاطر التي يمثلها التهديد، قد ترغب في اللجوء إلى بعض التدخلات للحد من التهديدات، مثل:

مواجهة التهديد:

ينبغي استخدام هذه الاستراتيجيات لمواجهة التهديدات منخفضة الخطورة.

1. التواصل مع الزملاء أو المنظمات التي يمكن أن تقدم الدعم في تعزيز قدرتك على الاستجابة أو معالجة نقاط الضعف لديك.



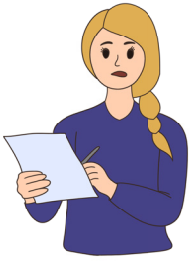
2. بعد التشاور مع الزملاء أو المجموعات الداعمة لك، قم بتطوير حوار مع الجناة لتفادي التصعيد.

3. ابلغ الجناة – سواء بشكل مباشر أو من خلال آخرين – الرسالة بأن تهديدك أو مهاجمتك سيكلفهم ثمناً سياسياً.

مشاركة التهديد:

ينبغي استخدام هذه الاستراتيجيات للتهديدات متوسطة الخطورة.

1. انشر التهديدات التي تلقيتها بصفتك جزءًا من تحالف، وليس بشكل فردي أو باسم منظمتك فقط.



2. لا تذكر أسماء الأفراد في التقارير أو الوثائق الحساسة، بل انشر كل شيء باسم مؤسسة أو تحالف.

3. تابع أي تصعيد محتمل للتهديدات، وأبلغ زملائك والمجموعات الداعمة بأي حوادث.

مشاركة التهديد:

ينبغي استخدام هذه الاستراتيجيات لمواجهة التهديدات عالية الخطورة.

1. أوقف أي أنشطة علنية أو الترويج العلني لما يتم استخدامه لتهديدك (مثل عملك في الدفاع عن حقوق الإنسان، أو حملة أو تقرير).

2. عزّز تدابير الحماية الخاصة بك وابقِ زملاءك والمجموعات الداعمة على اطلاع دائم حتى زوال التهديد، وحدد مواعيد منتظمة للتواصل والمتابعة.

3. فكّر في الانتقال مؤقتًا إلى مكان أكثر أمانًا (مثل بيوت الأمان التابعة لمنظمات أخرى). تجنّب العزلة، ولكن استغل هذا الوقت للتوقف والتأمل في كيفية تأثير هذه التهديدات عليك.

تذكّر أن معايير تقييم المخاطر ونمذجة التهديدات ستتغير بمرور الوقت، وذلك تبعًا لأنشطتك والتغيّرات في السياقات المحيطة بك.

أفضل أداة لدينا لحماية أنفسنا هي الوقاية، لذا احرص على أن تخضع لهذه التقييمات بشكل دوري، سواء على المستوى الفردي أو الجماعي، حتى تتمكن من تطوير مهاراتك وزيادة قدرتك على الاستجابة، مع التعرف على استراتيجيات مختلفة تتناسب مع سياقك واحتياجاتك الخاصة.

المنظمات الدولية التي تقدم خدمات الدعم:
الأمن الجسدي:
خط الطوارئ لمنظمة فرونت لاين ديفندرز: الاتصال الطارئ| Front Line Defenders
حملة المدافعين عن حقوق الإنسان:

مدينة الملاذ الآمن:
قدّم طلباً إلى مدينة الملاذ
الأمن الرقمي:
منظمة اكسس ناو
(Access Now)
خط الدعم للأمن الرقمي
المنظمات العراقية
التي تقدم خدمات:

1. مقدم الخدمة:
جمعية نساء بغداد

تفاصيل الخدمات :
١. الدعم النفسي الاجتماعي والعنف القائم على النوع الاجتماعي
٢. الإرشاد القانوني والمساعدة القانونية
٣. التمكين الاقتصادي
٤. بناء القدرات والتدريب
٥. خدمات الحماية الرقمية

بيانات الاتصال/الخط الساخن:
بغداد والانبار: ٠٧٨٠٦٦٥٤٧٧٣ - ٠٧٧٣٠١٦٩٧٩٠
دهوك: ٠٧٥٠٧١٠١٧٠١
سنجار: ٠٧٥١٠٤٥٢٥٥٤

الموقع:
بغداد و دهوك و سنجار

2. مقدم الخدمة:
منظمة حواء للإغاثة والتنمية

تفاصيل الخدمات :
الدعم النفسي الاجتماعي والعنف القائم على النوع الاجتماعي

بيانات الاتصال/الخط الساخن:
٠٧٧٢١٧٠٩٩١٥

الموقع:
ديالى – المقدادية

3. مقدم الخدمة:
جمعية الفردوس العراقية

تفاصيل الخدمات :
ملاجئ آمنة مؤقتة بالتعاون مع مكاتب الأمن، مجموعات الدعم النفسي الاجتماعي والجلسات الفردية، ودعم الإسعافات الأولية.

بيانات الاتصال/الخط الساخن:
٠٧٧٣٥٦٢٦٢٤٦

الموقع:
محافظة البصرة

4. مقدم الخدمة:
منظمة الحب والسلام

تفاصيل الخدمات :
العنف القائم على النوع الاجتماعي

بيانات الاتصال/الخط الساخن:

الموقع الالكتروني:
http://www.iraq-ilp.org
٠٧٨٥٢٢٠٢٢٠٤

الموقع:
محافظة الانبار

5. مقدم الخدمة:
مؤسسة السلام المستدام (SPF)
تفاصيل الخدمات :
الابتزاز الجنسي والانتقام الإباحي
بيانات الاتصال/الخط الساخن:
الموقع الالكتروني:
www.sustainablepeacefoundation.org
الموقع:
أربيل ونينوى

6. مقدم الخدمة:
مركز تدريب وتطوير الأرامل
تفاصيل الخدمات :
الدعم النفسي والقانوني
(جلسات استشارة قانونية مجانية)
بيانات الاتصال/الخط الساخن:
الموقع الالكتروني:
https://www.facebook.com/share/1WPUQQjXR/?mibextid=wwXIfr/p
الموقع:
بغداد

7. مقدم الخدمة:
المسلة
تفاصيل الخدمات :
العنف القائم على النوع الاجتماعي (GBV)،
سبل العيش، والدعم النفسي الاجتماعي (PSS)
بيانات الاتصال/الخط الساخن:
٠٧٥٠١٨٠١٩٧٥٤
الموقع:
أربيل ونينوى

8. مقدم الخدمة:
نساء من اجل العدالة
تفاصيل الخدمات :
الدعم النفسي الاجتماعي (MHPSS)، الاستشارات القانونية، دعم مالي للأيتام والأرامل
بيانات الاتصال/الخط الساخن:
الموقع الالكتروني:
٠٧٨٥٣٣٦٧٩٤
الموقع:
كربلاء، شارع مستشفى الكفيل

9. مقدم الخدمة:
فري تو رن (Free to Run)
تفاصيل الخدمات :
العنف القائم على النوع الاجتماعي والتحرش ضد النساء والفتيات
بيانات الاتصال/الخط الساخن:
الموقع الالكتروني: https://freetorun.org/
الايميل: info@freetorun.org
رقم الهاتف: ٠٧٥٠٨٢١٨٧٠٢
الموقع:
اربيل

إنشاء سجل للحوادث:

بالإضافة إلى ذلك، وخاصة عند مواجهة العنف القائم على النوع الاجتماعي (سواء كان عبر الإنترنت، أو خارج الإنترنت، أو كليهما)، يُوصى بالاحتفاظ بسجل للحوادث حيث يمكنك تتبع الهجمات المختلفة، وتوثيق أي أدلة، وتنظيم المعلومات التي قد تحتاجها في حال رغبت في اتخاذ إجراء قانوني أو أي نوع من الدعم الذي سيفيد من وجود تلك المعلومات متاحة بطريقة منظمة.

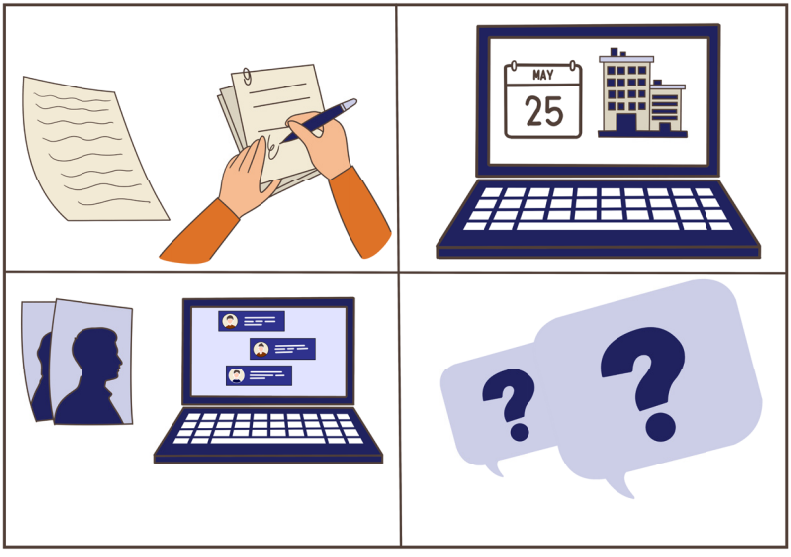
من الافضل ان يعتمد الجميع دمج كلا الممارستين (نمذجة التهديدات وإنشاء سجل للحوادث) كجزء من تخطيط السلامة القياسي. على عكس إجراء تمرين كامل لنمذجة التهديدات، يعد هذا المورد أداة مفيدة يمكن أن تُمكن أي شخص من تتبع الحوادث كوسيلة لاستعادة السيطرة على حالة عدم اليقين والارتباك والترهيب التي تهدف معظم الهجمات إلى إثارتها.

من الممكن أن بعض الأشخاص قد لا يكون لديهم إمكانية الوصول إلى الأجهزة الشخصية أو الخاصة، أو قد يتعرضون للمراقبة والتفتيش من قبل الأشخاص الذين يتسببون في الإساءة التي يتعرضون لها. في هذه الحالات، نوصي بإرسال المعلومات إلى شخص أو منظمة موثوقة عبر تطبيق رسائل آمن مثل Signal، الذي يوفر تشفيرًا متكامل و وميزة إخفاء الرسائل. لإخفاء الأدلة الموثقة داخل الهاتف المحمول، يمكن استخدام تطبيق Tella باتباع الدروس التوجيهية الرسمية المتاحة هنا:

تعلم استخدام tella!!

للاحتفاظ بسجلّ دقيق للحوادث، يُرجى تضمين ما يلي:

- التاريخ (المكان - سواءً كان متصلاً بالإنترنت أو غير متصل - والوقت إن أمكن).
- وصف موجز لما حدث.
- من تعتقد أنه المسؤول (ولماذا).
- قائمة بالأدلة التي قد تحتاجها للتحقق من هوية المسؤول عن الحادث.
- أدلة على الحادث (صور، مستندات، حسابات على مواقع التواصل الاجتماعي، عناوين الكترونية URL، إلخ.)



موارد التهدئة النفسية عبر الإنترنت:

تطبيق المساعدة الذاتية (متوفر باللغة العربية):

تطبيق المساعد الذاتية

هدوء مساحة ذهنية

قناة يوتيوب (باللغة الكردية):

حماية الاتصالات الداخلية للمنظمات

قناة يوتيوب (باللغة العربية):

mindfulness- Muslih - Kurdish resource

الأمن النفسي والاجتماعي:

يتعلق الأمن النفسي والاجتماعي بتخفيف المخاطر التي تهدد صحتنا النفسية. نتعامل مع هذا الأمر من خلال التركيز على المرونة، مما يتيح لنا تطوير مهارات فردية وجماعية لتحقيق الاستقرار والأمان، مما يمُكّن الجميع من تحديد تحديات وآثار المشاركة في التحول السياسي والدعوة إلى العدالة، والاستعداد لها، ومواجهتها، والتعافي منها.

تاكدي من:

• ضمان السلامة

- تحديد السياق وترتيب أولويات احتياجات السلامة الأساسية التي ينبغي معالجتها (مثل رعاية الجروح الجسدية، وإيجاد مأوى بعيدًا عن الأذى).
- تحديد التهديدات النشطة والاستجابات المتوافقة مع خطة السلامة الخاصة بك.
- التواصل مع شبكة الدعم أو جهات الاتصال في حالات الطوارئ.

• تعزيز الهدوء

- تحديد الأشخاص والموارد والأماكن المتاحة لاستعادة الأمان.
- تحديد ردود الفعل العاطفية وتوثيق التأثيرات التي تستجيب لها.
- البحث عن موارد داعمة لاستعادة الاستقرار والوضوح.

يُرجى ملاحظة أن الأدلة ستحتاج على الأرجح إلى تخزينها على وحدة تخزين ملفات أو ذاكرة منفصلة (USB، أو قرص ثابت، أو حتى منصة تخزين إلكترونية موثوقة)، إذ يُسهّل الاحتفاظ بسجل الحادثة لمجرد سرد الأحداث. قد ترغب في استخدام قسم «الأدلة» لإعداد قائمة بالأدلة المتوفرة لديك ومكان تخزينها.

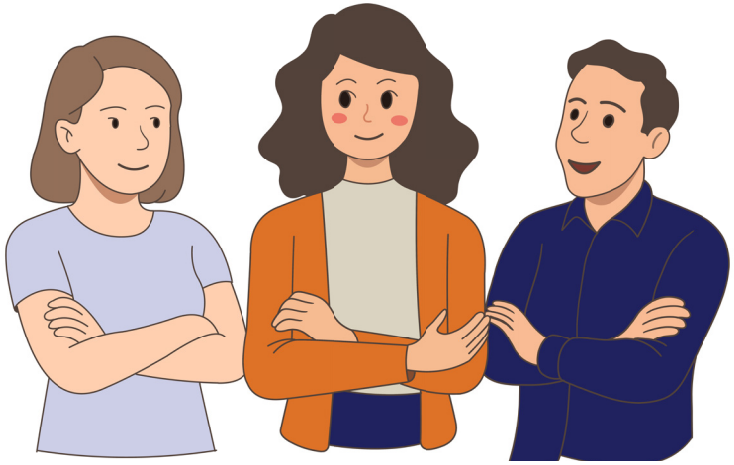
يوصي دليل التحرش الإلكتروني الصادر عن منظمة القلم الأمريكية (PEN America) بتتبع رسائل البريد الإلكتروني، والتفاعلات على مواقع التواصل الاجتماعي، وأي رسائل نصية أو مكالمات هاتفية تتضمن مضايقة. يحتوي هذا الدليل (المتوفر باللغة العربية على الرابط اضغط هنا :

أيضًا على معلومات مهمة حول فهم التحرش الإلكتروني، والاستعداد له، والاستجابة له، وتركيز الرعاية الذاتية، وكيفية طلب الدعم أو تقديمه عند مواجهة هذا النوع من العنف.

تذكر أنه من خلال استكشاف نموذج التهديد الخاص بك وتوثيقه، والوعي بالحوادث التي قد تُعرّض سلامتك للخطر، قد تتمكن أيضًا من تحديد تهديدات جديدة، بالإضافة إلى القدرات والموارد الجديدة اللازمة لمواجهتها. يمكنك تقييم هذه التهديدات في كل مرة تُعيد فيها تقييم نموذج التهديد الخاص بك وفقًا لحساسية عملك أو أي مواقف قد تؤثر على ظهورك أو تعرضك للخطر.

في الأقسام التالية، سنشارككم اعتبارات أساسية قد ترغبون في دمجها في تطوير خطة أمنكم الشخصية أو الجماعية. مع ذلك، لا ينبغي اعتبار هذه الاعتبارات نموذجًا محددًا للأمن. كما أوضحنا في القسم الأول من هذا الدليل: ينبغي أن يُحدد سياقكم الخاص خطتكم الأمنية، لأنه سيحدد الأدوات والموارد والخطوات التي ستكونون مستعدين لتطبيقها عند الاستجابة لتهديدات محددة وفقًا لنموذج المخاطر الخاص بكم (الفردي أو الجماعي).

- **تعزيز القدرة الذاتية على المواجهة**
  - تواصل مع الآخرين واطلب الدعم.
  - ابحث عن المعلومات المتعلقة بخدمات الدعم التي تلبي احتياجاتك.
  - تعامل مع المشكلات العملية واطلب المساعدة إذا واجهت صعوبة في ذلك.
- **تعزيز الترابط والتواصل مع مجتمعك**
  - تواصل مع أحبائك وشاركهم الوضع الذي تمر به.
  - حافظ على تواصل دائم مع شبكة الدعم وجهات الاتصال الطارئة.
  - حاول إيجاد شخص مقرّب يمكنه الاطمئنان عليك بشكل دوري.
- **تعزيز الامل والايجابية الذاتية**
  - لا تستسلم للشعور بالعجز، وضع رفاهيتك النفسية في المقام الأول.
  - إذا شعرت بالإرهاق أو التهديد، اعترف بذلك وشاركه مع شبكات الدعم وجهات الاتصال الطارئة
  - حدّد تأثيرات الوضع الذي تمر به، واعترف بالمهارات والموارد التي تملكها لتتمكن من التعافي.



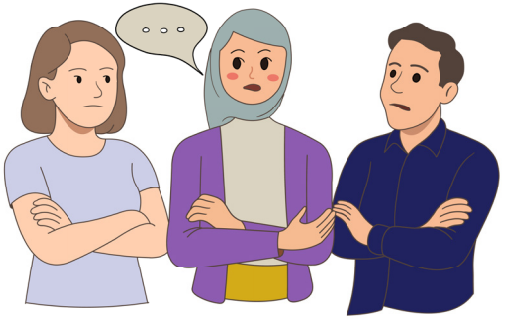
الأمن الجسدي:

يرتبط الأمن الجسدي بالتخفيف من التهديدات التي تستهدف سلامتنا الجسدية، سواء كانت موجهة لأجسادنا أو للمباني التي نعيش أو نعمل فيها (مثل المنازل ومواقع العمل)، أو للمركبات التي نستخدمها في حياتنا اليومية.
نقوم بالتعامل مع هذا الموضوع من خلال فهم السياق الذي نعيش فيه ومعالجة نقاط الضعف والتهديدات التي قد تؤثر على مستوى الأمان المحيط بأجسادنا، ومبانينا، ومركباتنا.
في هذا الدليل، سنركّز على البُعد الأول من الأمن الجسدي: **أجسادنا**.

• تاكدي من:

تأكد من ترتيب احتياجاتك وإبلاغ جهات الاتصال الموثوقة بها

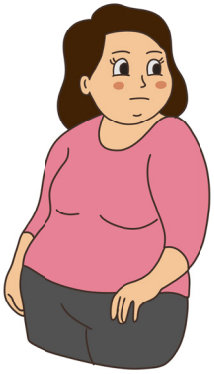
- هل تتناول أي أدوية؟
- هل لديك أي حساسية أو تحسس تجاه أطعمة أو أدوية معينة؟
- هل لديك أي حالات صحية محددة يجب أن يكون الآخرون على دراية بها؟



• تاكدي من:

شارك جهات الاتصال وخطط الطوارئ مع أشخاص تثق بهم

- من يجب التواصل معه في حال احتجت إلى مساعدة طبية؟
- هل تمنح موافقتك لتلقي المساعدة في حالة الطوارئ؟
- هل تشارك هذه المعلومات مع زملائك أو أقرانك؟



• تاكدي من:

احفظ مستنداتك الشخصية والحساسة في مكان آمن

- هل وثائقك (جواز السفر، التأشيرات، التصاريح، إلخ) محدثة؟
- هل تحتفظ بهذه الوثائق في مكان آمن؟
- هل قمت برقمنة المستندات تحسبًا لحالات الطوارئ؟

• تاكدي من:

عزّز وعيك بالمنظمات التي تقدم الدعم أثناء الأزمات

- حدّد المنظمات التي يمكنها تقديم الدعم في حالات الطوارئ (المساعدات الإنسانية، الطوارئ الطبية، الدعم النفسي الاجتماعي، أو خطوط المساعدة الرقمية).
- أعط الأولوية للمنظمات المحلية التيَ يمكنك التحقق من سمعتها.
- ابحث عن منظمات يمكن أن توفر دعمًا عالي المستوى في الأزمات مثل إعادة التوطين أو المساعدة المالية للمدافعين عن حقوق الإنسان.

• تاكدي من:

احتفظ بصندوق طوارئ شخصي

- فكّر في احتياجاتك الأساسية وضع ميزانية لها (السكن، الصحة، النقل).
- حاول الحفاظ على توفر ميزانية تغطي احتياجاتك الأساسية (يوصي البعض بتوفير ما يعادل ٣ إلى ٦ أشهر من راتبك).
- حتى إن لم تتمكن من ادخار المبلغ الكامل، فإن أي مبلغ تخصصه للطوارئ قد يُحدث فرقًا كبيراً.

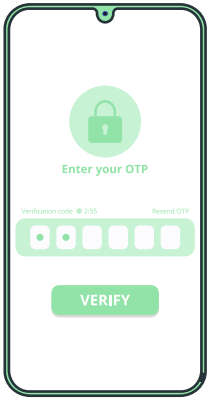
الأمن الرقمي

يرتبط الأمن الرقمي بالتخفيف من التهديدات التي تستهدف معلوماتنا، واتصالاتنا، ومعداتنا. نتعامل مع هذا المجال من خلال رفع مستوى الوعي الرقمي لدينا، وتحسين الإجراءات التي نتخذها لضمان سلامة معلوماتنا الحساسة، والأجهزة التي ننتج معلوماتنا من خلالها، ونتشاركها من خلالها، ونخزنها عليها.
يشمل ذلك أيضًا التزامنا بممارسات وعادات أمنية تهدف إلى الوقاية من الهجمات الرقمية أو الثغرات الأمنية.

• تاكدي من:

احمِ جهاز الكمبيوتر والهاتف من الفيروسات والبرمجيات الخبيثة

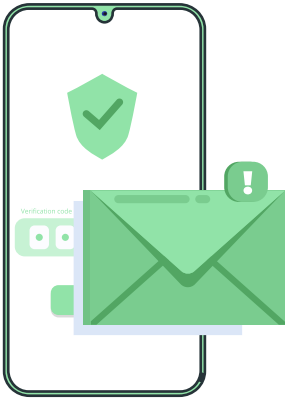
- حافظ على تحديث أجهزتك، وقم بتثبيت برامج مكافحة الفيروسات من مصادر موثوقة.هل تحتفظ بهذه الوثائق في مكان آمن؟
- تجنب فتح الروابط أو تحميل الوسائط، الملفات أو البرامج من مواقع غير رسمية أو من مرسلين غير معروفين عبر البريد الإلكتروني أو الرسائل النصية.
- حافظ على نظافة أجهزتك، وتجنب الاحتفاظ بملفات غير ضرورية، وقم بمسح بيانات جهازك بشكل دوري.



- **تأكدي من:**

استخدم كلمات مرور آمنة، المصادقة، ومدير كلمات مرور

- حدّث كلمات المرور مرة واحدة على الأقل في السنة، ولا تعيد استخدامها أو تشاركها مع الآخرين.
- استخدم مديرًا ومولّدًا لكلمات المرور. لا تقم بحفظ كلمات المرور على المتصفح أو الجهاز مباشرة.
- فعّل المصادقة متعددة العوامل (Multi Factor Authentication) في جميع الحسابات الممكنة، واحتفظ برموز الاسترجاع الخاصة بكل حساب في مكان آمن بعيدًا عن مدير كلمات المرور (ويُفضّل أيضًا استخدام المصادقة متعددة العوامل لحماية مدير كلمات المرور نفسه).



- **تأكدي من:**

احم المعلومات الحساسة على أجهزتك

- احتفظ بنسخ احتياطية من ملفاتك بانتظام، واحفظ النسخة الاحتياطية في مكان آمن.
- تأكد من حماية النسخ الاحتياطية بكلمة مرور، وقم بتشفيرها إن أمكن.
- كن حذرًا عند مشاركة المعلومات الحساسة. لا تشارك تفاصيل بنكية أو معلومات تواصل أو عناوين أو بريد إلكتروني أو أرقام هواتف دون موافقة صريحة.

أدلة التشفير:

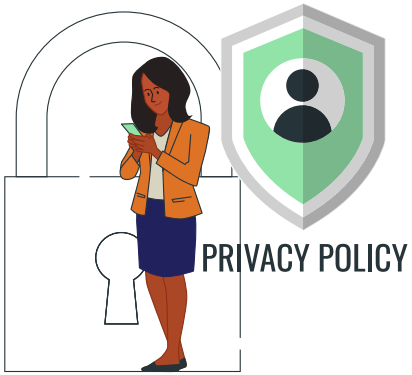
١. النسخة المجانية (bitwarden)

٢. keepassdx لاجهزة الاندرويد/ keepassim للاجهزة الايفون فقط

٣. النسخة المجانية (nordpass)

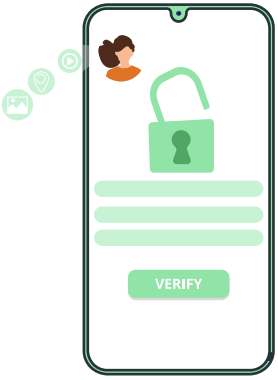
٤. النسخة المجانية (dashlane)

٥. مدير كلمات المرور من غوغل:



• حافظ على خصوصية اتصالاتك

- استخدم أدوات الاتصال الفوري التي توفّر تشفيرًا من شاملا، وفعّل خاصية الرسائل التي تختفي تلقائيًا عند الإمكان، مثل تطبيق Signal
- تجنّب مشاركة المعلومات الشخصية عبر منصات التواصل الاجتماعي، سواء على الملفات الشخصية العامة أو من خلال الرسائل الخاصة.
- استخدم متصفحات آمنة عند تصفح الإنترنت، واستعن بشبكة افتراضية خاصة (VPN) متى ما أمكن ذلك.



• ارفع وعيك بأمان الهاتف المحمول

- فعّل الحماية بكلمة مرور وقفل الشاشة، وحاول إعطاء الأولوية لاستخدام كلمات المرور بدلاً من وسائل التعريف البيومترية.
- عطّل الاتصال بشبكات الانترنيت (WiFi) والبلوتوث عندما لا تكون قيد الاستخدام، وراجع التطبيقات التي تملك صلاحية الوصول إلى موقعك الجغرافي.
- فعّل «وضع الإغلاق الكامل» (Lockdown Mode) إذا كان متاحًا، وتعرّف على إعدادات الخصوصية في جهازك وقم بضبطها حسب احتياجاتك.
- تخلّص دوريًا من التطبيقات التي لم تعد تستخدمها، واحرص على إزالة بياناتك منها وحذف حساباتك المرتبطة بها بشكل صحيح.

- عزّز أمان حساباتك على وسائل التواصل الاجتماعي والتطبيقات.

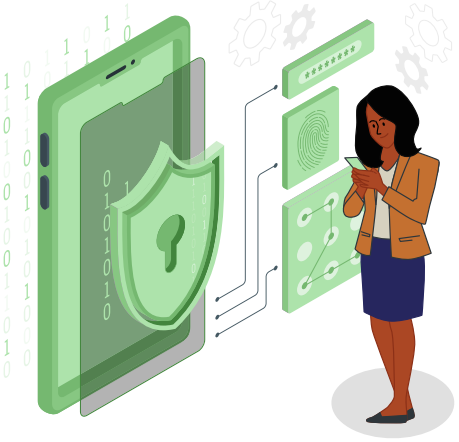
- فعّل المصادقة متعددة العوامل (Multi Factor Authentication) كلما أمكن.

- تحقق دوريًا من التطبيقات أو الخدمات المرتبطة بحساباتك، وأزل الوصول من التطبيقات التي لم تعد تستخدمها (قم بذلك أيضًا مع حسابات بريدك الإلكتروني)

- تحقق بشكل دوري من التحديثات على إعدادات الخصوصية واضبطها وفقًا لاحتياجاتك. ركز على تعديل ما يلي:

* من يمكنه مشاهدة منشوراتك (فكر أيضًا في حذف المنشورات بشكل دوري).
* من يمكنه التعليق على منشوراتك أو الإعجاب بها.
* من يمكنه الإشارة إليك في المنشورات.
* من يمكنه إرسال طلبات صداقة إليك.
* من يمكنه إرسال رسائل خاصة أو مباشرة إليك.
* من يمكنه العثور عليك عبر البريد الإلكتروني أو الهاتف.
* وضوح حسابك في محركات البحث خارج المنصة.

- تأكد من تحديث كلمات مرورك
- وبريدك الإلكتروني للاسترجاع واحتفظ بها في
- مدير كلمات المرور الخاص بك.



اجراءات لابد من اتخاذها اذا كنت...

• تحضر تظاهرات

مستوى المخاطر: عالي (الاعتقال، مصادرة الوثائق، العنف الجسدي)

- دائمًا ضع سلامتك البدنية وسلامة الأشخاص من حولك في الأولوية. إذا كان ذلك ممكنًا، تجنب الذهاب إلى التظاهرة بمفردك.
- تجنب أخذ هاتف يحتوي على أي معلومات شخصية أو حساسة (جهات الاتصال، الوثائق، الصور). حاول استخدام هاتف يمكن التخلص منه.
- فعّل حماية بكلمة مرور لفتح هاتفك، ولا تستخدم التحقق البيو متري لفتح الهاتف لأنه يمكن استخدام هذا الأسلوب تحت الضغط لفتح هاتفك دون موافقتك.
- حافظ على إطلاع جهات الاتصال الموثوقة على مكانك، وتعطيل أي تطبيقات تتبع المواقع الجغرافية على هاتفك.
- تجنب حمل المعدات أو الوثائق أو الأشياء القيمة معك. حاول أن تظل متحفظًا ولا تثير الانتباه لتقليل المخاطر.
- لا تترك التظاهرة بمفردك وحاول تجنب الاتصال بالشرطة أو الأشخاص الذين يمارسون العنف ضد المتظاهرين.
- إذا كنت توثق التظاهرة، تجنب التقاط صور لوجوه الحضور واحذف أي بيانات وصفية من الوثائق التي ترغب في مشاركتها.
- امتنِع عن مشاركة أي وثائق عبر حساباتك الشخصية على وسائل التواصل الاجتماعي. تواصَل مع المنظمات الموثوقة إذا كانت لديك أدلة على العنف ضد المتظاهرين أو إذا كان لديك وثائق ذات قيمة.

الموارد الموصى بها:

- SURVEILLANCE SELF-DEFENSE
- WITNESS - RESOURCES
- حماية الاتصالات الداخلية للمنظمات

الموارد الموصى بها:

- قائمة التحقق من الحماية الشخصية
- حماية الاتصالات الداخلية للمنظمات
- الحفاظ على بياناتك آمنة

- اطلب من مؤسستك إدارة جميع التصريحات العامة المتعلقة بعملك، وفكّر في تعديل مستوى تعرضك للخطر حتى ينخفض.
- احتفظ بسجل لأي حوادث تبدو غير عادية، واستشر فريقك أو شبكتك الموثوقة بشأن كيفية التصرف.
- إذا كنت تعتقد أن سلامتك الجسدية في خطر، ففكّر في إنشاء نظام تواصل مع الأقران لمساعدة الآخرين على إدراك سلامتك.
- إذا كنت تعتقد أن صحتك النفسية تتأثر بهذا، ففكّر في طلب الدعم النفسي والاجتماعي أو العلاج النفسي لمعالجة آثار هذا الوضع والتغلب عليه.
- في حالات الطوارئ المتعلقة بعملك ونشاطك، فكّر في التواصل مع المنظمات المحلية التي يمكنها تقديم الدعم الأمني الجسدي أو النفسي أو الرقمي.

لا تعتمد على وضع التصفح الخفي، ويفضل ضبط DuckDuckGo كمحرّك البحث الافتراضي لديك.

- **القيام بعمل مؤثر يصاحبه ظهور الإعلامي**

مستوى المخاطر: عالي (الانتقام، العنف الرقمي، العنف الجسدي)

- تأكد من أن حساباتك العامة على وسائل التواصل الاجتماعي لا تحتوي على أي معلومات شخصية أو حساسة عنك. ابحث عن اسمك وألقابك على غوغل واحذف أي معلومات شخصية باستخدام طلب إزالة المعلومات من بحث غوغل.
- تأكد من تفعيل المصادقة متعددة العوامل باستخدام رمز أو مفتاح فعلي في جميع حساباتك (وسائل التواصل الاجتماعي، البريد الإلكتروني، الحسابات البنكية الرقمية، إلخ).
- راجع إعدادات الخصوصية في حساباتك على وسائل التواصل الاجتماعي، وتجنّب التفاعل مع حسابات غير مألوفة.
- فكر في قفل حساباتك أو تقييد الوصول للمستخدمين غير المعروفين.
- استخدم متصفحاً خاصاً يدعم بروتوكول HTTPS لحماية هويتك على الإنترنت.

إذا كنت تقوم بعمل حساس للغاية (دون الاتصال بأي حسابات شخصية أو على وسائل التواصل الاجتماعي أو البريد الإلكتروني)، ففكر في استخدام متصفح (ToR).

وإذا كنت بحاجة للاتصال بحساب مرتبط بهويتك، ففكر في استخدام (FireFox) او (Mullvad) على جهاز الكمبيوتر، أو (Firefox Focus) على الأجهزة المحمولة مثل الهواتف والأجهزة اللوحية.

لا تعتمد على وضع التصفح الخفي، ويفضل ضبط DuckDuckGo كمحرّك البحث الافتراضي لديك.

• مواجهة العنف القائم على النوع الاجتماعي عبر الإنترنت مستوى الخطورة: عالٍ (النبذ، العنف النفسي، العنف الرقمي)

- شكّل فريق دعم من أشخاص تثق بهم لتقديم دعم طارئ مباشر (موثوق، وفي الوقت المناسب، ومحلي) ومرافقة.
- أبلغ عن أي صور متعلقة بهذا عبر منصة **«وقف الإساءة الجنسية غير الرضائية بالصور»**. بالإضافة إلى ذلك، فكّر في البحث عن اسمك وألقابك على غوغل، وإزالة أي معلومات شخصية من خلال ميزة **«متطلبات الإزالة»** في بحث جوجل.
- أبلغ عن أي حسابات متورطة في هذا الهجوم عبر آليات الإبلاغ على منصات التواصل الاجتماعي التي يقع فيها الهجوم. فكّر في توثيق أي أدلة قبل حظر الحسابات المسؤولة عن الهجوم.
- وثّق أي حوادث تتعلق بأمنك الرقمي والجسدي.
- أعط الأولوية لصحتك النفسية، وحاول البحث عن أي منظمات محلية يمكنها تقديم الدعَم النفسي والاجتماعي للأشخاص الذين يواجهون العنف القائم على النوع الاجتماعي.
- عزز أمنك الرقمي بتفعيل المصادقة متعددة العوامل في جميع حساباتك وتقييد الوصول إلى ملفاتك الشخصية.
- فكّر في أخذ قسط من الراحة من استخدام وسائل التواصل الاجتماعي، وتجنب الردود العلنية على الهجمات، فقد يمُكّن ذلك المهاجمين من استفزاز المزيد من ردودك («لا تُغذّ المتصيدين»).
- اطلب من فريق الدعم الخاص بك وأقرانك مساعدتك في إيصال هذا الوضع إلى عائلتك ومجتمعاتك التي قد تتأثر به.

الموارد الموصى بها:

- قائمة التحقق من الحماية الشخصية
- SURVEILLANCE SELF-DEFENSE
- مجموعة أدوات الأمن الرقمي

- **مواجهة حملة تشهير**

مستوى الخطر: مرتفع (التشهير، العنف النفسي، العنف الرقمي)

- تواصل مع زملائك الموثوق بهم أو شبكة دعمك أثناء تعاملك مع هذا الأمر، واطلب منهم المساعدة لاستعادة سلامتك والتغلب على آثار هذا الهجوم. فكّر في طلب دعم متخصص في الصحة النفسية.

- اتبع دليل مكافحة التشهير للعثور على أي معلومات شخصية أو حساسة عنك على الإنترنت، واحذف أي شيء قد يُستخدم للمساس بسلامتك. ابحث عن اسمك وألقابك على جوجل وبينج ودك دك جو، واحذف أي معلومات شخصية معروضة على كل محرك بحث من خلال متطلبات الإزالة في بحث غوغل، أو من خلال مايكروسوفت - الإبلاغ عن مشكلة إلى بينج، أو إرسال طلب حذف عبر البريد الإلكتروني إلى فريق خصوية (DuckDuckGo) اضغط هنا وفقًا لذلك.

- فعّل المصادقة متعددة العوامل في جميع حساباتك (وسائل التواصل الاجتماعي، رسائل البريد الإلكتروني، الخدمات المصرفية الرقمية، الخ)

- فعّل المصادقة متعددة العوامل في جميع حساباتك (وسائل التواصل الاجتماعي، رسائل البريد الإلكتروني، الخدمات المصرفية الرقمية، الخ)

- راجع إعدادات خصوصية حساباتك على وسائل التواصل الاجتماعي، وتجنب التفاعل مع حسابات لا تعرفها. فكّر في قفل حساباتك أو تقييد وصول المستخدمين المجهولين.

- فكّر في أخذ قسط من الراحة من وسائل التواصل الاجتماعي، وتجنّب الانخراط في ردود فعل علنية على الهجمات، فقد يمُكّن ذلك المهاجمين من استفزاز للحصول على المزيد من ردودك («لا تُغذّ المتصيدين»). وثّق التهديدات، ومن ينشر المعلومات الكاذبة ضدك. أبلغ زملاءك والمجموعات الداعمة لك بأي حوادث.

- علّق أي تفاعلات عامة أو أي نشر إضافي باسمك لأي شيء قد يُستخدم لتهديدك أو تصعيد الهجوم (مثل أعمال الدفاع عن حقوق الإنسان، أو حملة، أو تقرير).

- اطلب من مؤسستك إصدار بيان دعم لك. أقرّ بالهجوم، ولكن تجنّب إعطاء أي ذريعة للجهات المؤذية لتصعيده.

الموارد الموصى بها:

- قائمة التحقق من الحماية الشخصية
- الحفاظ على بياناتك آمنة
- دليل ميداني للحماية من الإساءة و المضايقات الإلكترونية

يُسلّط هذا الدليل، الذي أُعدّ بالتعاون مع ناشطات عراقيات ومدافعات عن حقوق الإنسان ولصالحهن، الضوء على جهودهن الحاسمة في النضال من أجل المساواة في الحقوق والفرص للنساء والفتيات. ورغم بطء التقدم، فقد ساعد عملهن النساء على استعادة الأماكن العامة، حتى في ظلّ مواجهة العنف الجنسي والعنف القائم على النوع الاجتماعي على نطاق واسع. إلا أن هذا العمل الحيوي يترافق مع تزايد المخاطر الأمنية المرتبطة بالنوع الاجتماعي.