

دليل السلامة في الفضاء العام

● إصدار 2026

أدوات عملية لحياة مدنية أكثر أماناً

أدوات عملية للمشاركة الأكثر أماناً في الحياة المدنية والسياسية في لبنان
خلال فترات الخطر المتصاعد.

للمدافعات عن حقوق الإنسان · للنساء في الحياة العامة والمدنية · للمرشحات · للمدافعين/
ات من مجتمع الميم-عين · للحلفاء · لمشرفي/ات المجتمعات الرقمية



HuMENA For Human Rights and Civic Engagement
HuMENA pour les Droits de l'Homme et l'Engagement Civique
هيومنينا لحقوق الإنسان والمشاركة المدنية



INNOVATION
FOR CHANGE
MIDDLE EAST & NORTH AFRICA



Digital Democracy
Initiative

جدول المحتويات

02	عن منظمة هيومينا	
03	مسرّد المصطلحات الرئيسية	
03	نبذة عن هذا الدليل	01
05	لماذا تزيد الفترات السياسية والانتخابية من المخاطر الرقمية؟	02
08	أنواع الهجمات التي يغطّيها هذا الدليل	03
13	التعرّف السريع على المخاطر وتصنيفها حسب درجة الخطورة	04
19	مسار الاستجابة خلال أوّل 24 إلى 72 ساعة	05
25	خيارات المشاركة الأكثر أماناً	06
29	الذكاء الاصطناعي والسلامة الرقمية	07
31	إرشادات الإبلاغ عبر المنصّات	08
34	مسارات الدعم والإحالة	09
38	توجيهات للحلفاء والصدّيقات والزملاء	10
41	توجيهات لمشرفي الصفحات والمنصّات المجتمعية والقائمين على الإشراف	11
45	قوائم تحقّق سريعة	12
51	ملاحظات ختامية وموارد رئيسية	13
53	المراجع	
53	قراءات إضافية	

عن منظمة هيومينا

منظمة هيومينا لحقوق الإنسان والمشاركة المدنية منظمةً مستقلة غير ربحية تعمل على حماية الفضاء المدني وتوسيعه في منطقة الشرق الأوسط وشمال أفريقيا. يقع مقرها الرئيسي في بروكسل ولها مكتب إقليمي في بيروت، وتدعم المدافعين والمدافعات عن حقوق الإنسان والفاعلين والفاعلات في المجتمع المدني، ولا سيما المنفيين منهم وأبناء الشتات، من خلال المناصرة والبحث والتدريب. يمتدّ عملها ليشمل الحريات المدنية الأساسية المتمثلة في حرية التعبير والتجمع السلمي وتكوين الجمعيات، رقمياً وواقعياً على حدّ سواء. وتساعد منظمة هيومينا الأفراد والحركات على التنظيم بأمان ومواصلة نشاطهم في مواجهة القمع. وتعمل المنظمة عن قرب مع النساء واللاجئين/ات وأفراد مجتمع الميم-عين وغيرهم من المجتمعات المهمشة، وتُدمج مبادئ المساواة الجندرية والعدالة الاجتماعية في برامجها. ويحتل التوثيق والمناصرة والنشاط الفني مكانةً محوريةً في منهجها.

تقديم

ينبثق هذا الدليل من الأوضاع التي تعيشها النساء اللبنانيات والمدافعات عن حقوق الإنسان وناشطو ومدافعو مجتمع الميم-عين والفاعلون المدنيون منذ سنوات عدة، ومن المخاطر المحددة المرتبطة بتصاعد العنف الرقمي في لحظات الحضور العلني.

وقد صدر في إطار مشروع تنقّذه منظمة هيومينا عام 2026 بدعم من شبكة الابتكار للتغيير في منطقة الشرق الأوسط وشمال أفريقيا، ضمن مبادرة الديمقراطية الرقمية. وقد طُوّر محتوى الدليل في حوار مستمر مع المدافعات عن حقوق الإنسان والفاعلين المدنيين والممارسين العاملين في مجال مجتمع الميم-عين، من خلال جلسات عمل تدريبية للتحقق عُقدت في لبنان في منتصف عام 2026، ويعكس الأنماط التي حدّدها والشغرات التي أشاروا إليها والحمايات التي رأوا أنها الأكثر إلحاحاً في البيئة الراهنة.

يتطور المشهد السياسي والقانوني والرقمي في لبنان باستمرار، وتعمل منظمة هيومينا على مراجعة هذا الدليل وتحديثه مع تغيّر الأوضاع. للاستفسارات والشراكات، تواصلوا عبر البريد الإلكتروني: lebanon@humena.org.

وإذا كنت تستخدم هذا الدليل في خضمّ حادثة، فتصرّف أولاً وفق التوجيهات الأكثر إلحاحاً وتواصل للحصول على الدعم بعد ذلك.

شكر وتقدير

استفاد دليل السلامة في الفضاء العام من الوقت والخبرة والتجارب المعاشة للمدافعات عن حقوق الإنسان وناشطي مجتمع الميم-عين والفاعلات المدنيات والممارسين الحلفاء الذين شاركوا في جلسات العمل التدريبية للتحقق التي نظمتها منظمة هيومينا في لبنان. وبناءً على طلبهم الصريح، لم تُذكر أسماء المشاركين بصورة فردية. فالأنماط التي حدّدها والشغرات التي صوّبها والحمايات التي أولوها الأولوية شكّلت كل قسم من أقسام هذه الوثيقة.

جرى تطوير الدليل وتحريره على يد كريستي إسكندر (المؤلفة والباحثة الرئيسية) مع فريق منظمة هيومينا، تحت إشراف مصطفى فؤاد (المدير التنفيذي). وأنجز الإنتاج بدعم من مركز الابتكار — شبكة الابتكار للتغيير في منطقة الشرق الأوسط وشمال أفريقيا ومنظمة سيفيكوس في إطار مبادرة الديمقراطية الرقمية.

المصطلحات الرئيسية

مسرد المصطلحات

تعريفات موجزة للاختصارات والمصطلحات المرتبطة بالسياق اللبناني المستخدمة في هذا الدليل.

PSEA — الوقاية من الاستغلال والاعتداء والتحرش الجنسي

مجموعة من المعايير المطبقة على موظفي وشركاء المنظمات الإنسانية والمدينة.

CLDH — المركز اللبناني لحقوق الإنسان

منظمة غير حزبية لتوثيق الحقوق وتقديم الخدمات القانونية.

نشر البيانات الشخصية دون إذن (Doxxing)

الكشف المتعمد عن معلومات شخصية أو تعريفية عن شخص ما عبر الإنترنت، بهدف التمكين من المضايقة أو التهريب أو الأذى خارج الفضاء الرقمي.

ISF — قوى الأمن الداخلي

الشرطة الوطنية اللبنانية، وتضم وحدة جرائم الأمن السيبراني. راجعوا القسم 9.2 اعتبارات السلامة الموهقة قبل طلب المساعدة.

+LGBTQI — مجتمع الميم-عين

المثليات والمثليون ومزدوجو الميل الجنسي والعاثرون/العاثرات جندياً وحاملو صفات الكوير وثنائيو الجنس وغيرهم من الأقليات الجنسية والجنسية.

NCII — الصور الحميمة المنشورة دون موافقة

مشاركة صور أو مقاطع فيديو جنسية صريحة أو التهديد بمشاركتها دون موافقة. راجعوا القسم 3.6 الصور الحميمة المنشورة دون موافقة والتزييف العميق.

NSSF — الصندوق الوطني للضمان الاجتماعي

مؤسسة الضمان الاجتماعي اللبنانية.

الفضح (Outing)

الإفصاح عن التوجه الجنسي لشخص ما أو هويته الجندرية أو غيرها من المعلومات الحساسة المرتبطة بالهوية دون موافقته.

StopNCII.orgخدمة مجانية لمطابقة البصمة الرقمية تديرها خط مساعدة ضحايا الانتقام الإيجابي، تحجب مسبقاً الصور الحميمة المعروفة على المنصات الكبرى المشاركة. stopncii.org**TFGBV — العنف المبني على النوع الاجتماعي الميسر بالتكنولوجيا**

أي فعل يُرتكب أو يُدعم أو يتفاقم عبر التقنيات الرقمية ويتسبب بأذى جسدي أو جنسي أو نفسي أو اجتماعي أو سياسي أو اقتصادي على أساس النوع الاجتماعي.

WHRD — المدافعة عن حقوق الإنسان

امرأة تدافع عن حقوق الإنسان، أو مدافع/ة عن حقوق الإنسان يعمل على حقوق النساء والحقوق الجندرية.

المادة 534

المادة 534 من قانون العقوبات اللبناني، استُخدمت تاريخياً لتجريم العلاقات المثلية واحتجاز أفراد مجتمع الميم-عين. يُشار إليها في هذا الدليل كعامل خطر عند التفكير في اللجوء إلى مؤسسات الدولة.

المادة 582

المادة 582 من قانون العقوبات اللبناني (الذم/التشهير الجزائي). تُستخدم لملاحقة من ينتقدون المسؤولين أو الشخصيات السياسية علناً، بما في ذلك بيانات الرّد على العنف الرقمي. راجعوا القسم 5.5 تحديد مسار الاستجابة التالي.

القسم 1

نبذة عن هذا الدليل

تتميز فترات الانتخابات في لبنان بارتفاع المخاطر ومستويات العنف الرقمي في الفضاء العام، لا سيما بالنسبة للنساء في الحياة العامة، والمدافعين والمدافعات عن حقوق الإنسان، والمدافعين عن حقوق مجتمع الميم-عين. وغالباً ما تُستخدم هذه الهجمات لمعاكبة الظهور العلني، وردع المشاركة المدنية والسياسية، وفرض الرقابة الذاتية والانسحاب، وتقويض التمثيل في الفضاء العام.

استجابةً لذلك، تم تطوير دليل السلامة هذا كمورد عملي وموجه نحو العمل يوفر أدوات لدعم المشاركة الأكثر أماناً في الحياة المدنية والعامّة خلال الفترات ذات التوتر السياسي والانتخابات. وهو مصمم ليكون مرجعاً موجزاً وقابلًا للتكيف، يقدم إرشادات مُتاحة للجميع يمكن للمستخدمين تطبيقها بناءً على احتياجاتهم عند مواجهة العنف المبني على النوع الاجتماعي الميسّر بالتكنولوجيا (TFGBV) في لبنان، ونشر البيانات الشخصية دون إذن، والفضح، وانتحال الهوية، والتحرّش المنشق.

تم تطوير الدليل من خلال عملية قائمة على الممارسة والمشاركة، تستند إلى الخبرات المعيشة للعنف القائم على النوع الاجتماعي التيسّر تكنولوجياً في لبنان. ولتنقيح محتواه، من المقرر عقد جلستين مغلقتين مع المدافعات عن حقوق الإنسان، والفاعلات في المجال المدني، والمدافعين عن حقوق مجتمع الميم-عين. تهدف الجلسة الأولى إلى مراجعة نتائج الدليل وتوجيهاته وتقديم معلومات عنها؛ على أن تليها جلسة ثانية مع الأطراف نفسها لتأكيد ملاءمة المحتوى ودقته وسلامته. سيتم مراجعة الدليل بعد هاتين الجلستين وإصدار نسخة نهائية منه خلال فترة إعداد التقرير القادمة.

الغرض من الدليل

1.1

يهدف دليل السلامة في الفضاء العام إلى تعزيز الجاهزية العملية والاستجابة الأولية الفعّالة للعنف القائم على النوع الاجتماعي التيسّر تكنولوجياً، ودعم مشاركة أكثر أماناً في الفضاء العام خلال الفترات السياسية عالية الخطورة. كما يسعى إلى تعزيز الممارسات الرقمية الآمنة وتحسين الاستجابة للتهديدات الرقمية، للحد من تأثير العنف الرقمي على المشاركة المدنية.

وتهدف إلى تعزيز الجاهزية وتمكين استجابات أكثر أماناً ووعياً تجاه العنف الرقمي خلال الفترات السياسية الحساسة. ويمكن استخدامه كدليل مرجعي سريع وأداة وقائية لتحديد المخاطر عند التعرّض للعنف القائم على النوع الاجتماعي التيسّر تكنولوجياً أو توقّع حدوثه.

لمن هذا الدليل؟

1.2

هذا الدليل موجه إلى: المدافعين/المدافعات عن حقوق الإنسان، والنساء في الحياة العامة والمدنية بمن فيهن المرشحات والفاعلات المدنيات، ومدافعي ومدافعات مجتمع الميم-عين ونشطاته ونشاطاته. كما تستهدف الحلفاء وشبكات الدعم لمجتمعات الميم-عين، فضلاً عن الفاعلين المدنيين ومنظمي المجتمعات والقائمين على إدارة الفضاءات الرقمية، بمن فيهم المشرفون ومديرو الصفحات المجتمعية ومديرو المجتمعات الرقمية الذين يواجهون مخاطر مرتبطة بالانتخابات. وبشكل أوسع، يُعدّ هذا الدليل مرجعاً مفيداً للمجموعات المدنية والأفراد المنخرطين في العملية الانتخابية في لبنان، ممن قد يتعرضون لأشكال مماثلة من الهجمات الرقمية ويحتاجون إلى أدوات عملية تدعم مشاركتهم بأمان.

— كذلك موجه إلى

- الفاعلون المدنيون ومنظمو المجتمعات
- المشرفون ومديرو الصفحات المجتمعية
- مديرو المجتمعات الرقمية الذين يواجهون مخاطر مرتبطة بالانتخابات
- المجموعات المدنية والأفراد المنخرطون في العملية الانتخابية في لبنان

— الجمهور الرئيسي

- المدافعات عن حقوق الإنسان (WHRDs)
- النساء في الحياة العامة والمدنية، بمن فيهن المرشحات والفاعلات المدنيات
- المدافعون والناشطون من مجتمع الميم-عين
- الحلفاء وشبكات دعم مجتمعات الميم-عين

ما يتضمنه هذا الدليل وما لا يتضمنه

1.3

يوفر هذا الدليل أدوات عملية وميسّرة لدعم الجاهزية الأساسية، والتعرف المبكر على المخاطر، واتخاذ إجراءات الاستجابة الأولى في مواجهة المضايقات الإلكترونية خلال فترات الانتخابات. وتركّز على استراتيجيات يفوقها المستخدم بموارد محدودة، يمكن تطبيقها من قِبل الأفراد والفاعلين المدنيين والقائمين على إدارة الفضاءات الرقمية، بهدف تعزيز السلامة وتقليص التعرض للأذى.

غير أنها لا تُشكّل بديلاً عن الدعم القانوني أو النفسي-الاجتماعي أو الأمني الرقمي المتخصص، ولا تقدّم حلولاً شاملة أو مخصصة لحالات بعينها. وعلى الرغم من أن الدليل يتضمن إرشادات للإحالة، إلا أنه يُعدّ مورداً تكميلياً يساهم في ترسيخ الممارسات الأكثر أماناً، مع الإقرار بأن بعض الحالات قد تستوجب تدخلاً أو دعماً متخصصاً.

القسم 2

لماذا تزيد الفترات السياسية والانتخابية من المخاطر الرقمية؟

صدر هذا الدليل عام 2026، في أعقاب الحرب الغاشمة وعلى خلفية الأزمة الاقتصادية اللبنانية المستمرة والتحولت في التحالفات السياسية وبيئة تضيق فيها الحيز المدني وأعاد تنظيم نفسه في آن واحد. ولا يتصاعد العنف الرقمي في هذه المرحلة في المحيط بالانتخابات المجدولة فحسب، بل في كل لحظة من لحظات الحضور العلني — الاحتجاجات، وشهادات أمام البرلمان، والتصريحات العامة بشأن مسار إعادة الإعمار، والمناصرة من أجل الوصول الإنساني، وأي فعل تنظيمي يغدو مرئياً للجهات المعارضة. ويعكس التركيز على فترة الانتخابات في هذا الدليل النمط الأكثر دراسةً وتوثيقاً، غير أن القراء ينبغي أن يتعاملوا مع الأدوات ذاتها باعتبارها قابلةً للتطبيق على مدار العام، إذ تتناسب حدّتها مع مستوى ظهور الشخص المستهدف لا مع التقويم الزمني.

غالباً ما تترافق فترات النشاط السياسي المكثّف، ولا سيّما الانتخابات، مع زيادة الحملات الرقمية وارتفاع مستوى الظهور العلني. ومع انخراط المرشحين والناشطين والمواطنين بشكل أكبر على الإنترنت، يصبحون أكثر عرضة لخطاب الكراهية والمضايقات والهجمات الإلكترونية المنسقة، خصوصاً عند تعارض التوجهات السياسية والقيم الثقافية. تتسم هذه الفترات بتصاعد الاستقطاب، حيث تتحول المجالات الرقمية إلى ساحات للتنافس والمراع، مما يؤدي إلى تضخيم التوترات وزيادة احتمالية وقوع الانتهاكات.

علاوةً على ذلك، يُقاوم كلّ من إخفاء الهوية والنطاق الواسع لوسائل التواصل الاجتماعي حدّة هذه المشكلة، إذ يُتيحان للمعتدين شنّ هجمات منسقة واسعة النطاق في ظل غياب شبه تام للمساءلة. وقد أسهمت التحولات الأخيرة في سياسات الإشراف على المنصات، ولا سيما منصتي ميتا وإكس (X)، في إضعاف الضمانات المتعلقة بخطاب الكراهية، مما أفضى إلى بيئة إلكترونية أكثر تساهلاً تتكاثر فيها ظاهرتا المضايقات القائمة على النوع الاجتماعي وكراهية النساء تحت ذريعة حرية التعبير. وتجدر الإشارة إلى أنه في غضون ثلاثة أشهر فحسب من تغيير سياسات تويتر، تضاعفت الهجمات الموجهة ضد الصحفيات ثلاث مرات مقارنةً بالفترة ذاتها من السنوات السابقة. وهذه الأوضاع مجتمعةً تُشجّع المعتدين وتقلّص فرص المساءلة^[1].

وتعمّق الثغرات الهيكلية في آليات الحماية هذه المشكلة وتنخر في منظومة المساءلة. فبين عامي 2020 و2023، شكّلت النساء 80% من الناجيات من العنف الرقمي في لبنان فيما يُقدّر أن ما بين 30 و40% من حالات المضايقات الإلكترونية تتصاعد لتتحول إلى تهديدات جسدية أو أشكال أخرى من الأذى خارج المجال الرقمي^[2]. وعلى الرغم من خطورة هذه الحالات، تبقى الحماية القانونية محدودة، في ظل غياب آليات فعّالة لمعالجة الإساءة الإلكترونية ومحاسبة المعتدين. يعود ذلك بشكل أساسي إلى إطار قانوني متقادم لا يستجيب بصورة كافية لجرائم المجال الإلكتروني، بما في ذلك القصور في تجريم الابتزاز الجنسي، وملاحقة مرتكبي الإساءة الإلكترونية، وضمان حماية فعّلية للناجيات^[3] وبناءً عليه يجد المستهدفون، ولا سيما الناشطات السياسيات، أنفسهم في مواجهة تصاعد مستمر للأذى مع محدودية سبل الانتصاف القانونية أو تحقيق العدالة.

تُساهم الأعراف الثقافية والاجتماعية في لبنان أيضاً في تشكيل مستوى التعرّض للمخاطر الرقمية خلال الفترات السياسية. إذ لا تزال المواقف الأبوية المتجذّرة تواصل تصوير السياسة والقيادة باعتبارهما مجالات يهيمن عليها الرجال، وغالباً ما تُقدّم النساء كفاعلات أقل شرعية، في حين لا تزال القضايا المرتبطة بالميل الجنسي والهوية الجندرية شديدة الحساسية في الخطاب العام. وفي هذا السياق، يكون الأفراد الذين يتحدّون هذه الأعراف، ولا سيّما النساء وأفراد مجتمع الميم-عين، أكثر عرضة للاستهداف عبر هجمات جندرية وأخلاقية وتشويهية، تهدف إلى تقويض مصداقيتهم وإضعاف مشاركتهم في الفضاء العام.

ونتيجةً لذلك، تُهيئ فترات التنافس والتوترات السياسية بيئةً مواتيةً لتفشّي العنف الرقمي، وقد تدفع النساء وغيرهن من الفئات المهقشة إلى الانسحاب من المشاركة العامة أو إثنائهن عن دخول الحياة السياسية برقتها. ولا يقتصر أثر ذلك على ترسيخ التفاوتات الجندرية في القيادة السياسية، بل يسهم أيضاً في التقلص التدريجي للحيز المدني وإقصاء الأصوات المتنوعة من الفضاء العام^[4].

2.1 العنف الرقمي بوصفه تكتيكاً لإسكات المشاركة

2.1

يستخدم العنف الرقمي خلال الفترات السياسية الحساسة كتكتيك متعمّد لتقويض الخصوم والنيل من مصداقيتهم، وقمع المشاركة، وتوجيه الخطاب العام. وتهدف الهجمات مثل التشهير وحملات التشويه والتهديدات والمضايقات إلى معاقبة الظهور العلني ونزع الشرعية عن الأفراد، ولا سيما من يعبرون عن آراء مخالفة أو يتحدّون الفاعلين السياسيين الراسخين.

شهدت الانتخابات البرلمانية اللبنانية لعام 2022 تصاعداً في العنف الرقمي المنهجي الذي استهدف في كثير من الأحيان النساء المشاركات في الحياة العامة. وفي معظم الحالات، قامت الأحزاب السياسية والشبكات بشن مثل هذه الهجمات المنظمة والحملات المنسقة، غالباً من خلال «جيوش إلكترونية» من الحسابات الموجهة، بهدف النيل من مصداقية المرشحات والتأثير على الرأي العام. وترتبط هذه الممارسات ارتباطاً وثيقاً بالمنافسة السياسية الأوسع نطاقاً، حيث تُستخدم الهجمات الرقمية لإضعاف الخصوم بشكل استراتيجي وتشكيل الروايات السائدة.^[1] وتُستهدف المرشحات، ولا سيما اللواتي يتنافسن ضد الأحزاب الراسخة ويروجن لآراء مختلفة، على نحوٍ غير متكافئ كوسيلة لتقويض مصداقيتهن. ويشكل انتشار هذه الهجمات الرقمية تحدياً للمواقف السياسية، وينزع الشرعية عن وجود النساء في الفضاء السياسي، ويعزز القيم المعادية للمرأة المتأصلة ثقافياً. كما أنها تضخم المحتوى الجنساني والجنسي الذي يرسخ المواقف التمييزية ويجعل الإقصاء أمراً عادياً.^[2]

على سبيل المثال، واجهت المرشحة ديماء أبو ديه، التي ترشحت عن المقعد الشيعي على قائمة «الزحطة من أجل السيادة» في عام 2022، حملة مستمرة ومنسقة من الإساءات عبر الإنترنت بعد أن تحدت الفاعلين السياسيين المهيمنين في منطقتها.^[3] وأفادت بتلقيها تهديدات خطيرة من حسابات مجهولة ومزيفة، شكلت تهديدات مباشرة لسلامتها وأجبرتها على مغادرة مسقط رأسها مؤقتاً. كما عملت العديد من المنصات والمواقع الإلكترونية على تضخيم الروايات التشهيرية التي تستهدفها شخصياً وسياسياً. ومع تصاعد الهجمات وانتشارها لتصل إلى الأذى خارج المجال الرقمي، أصدر والداها بياناً عاماً ينكران فيه ترشحها ويبرران أنها.^[4]

توضح حالة ديماء أبو ديه بوضوح كيف يمكن للعنف الرقمي أن يكون منسقاً ومستمراً ومدمراً للغاية. فهو يؤثر على السلامة الشخصية عبر الإنترنت وخارجه، ويؤثر على المكانة الاجتماعية، ويعطل المشاركة السياسية. في الواقع، تتمتع الأحزاب السياسية المهيمنة، التي غالباً ما تقوم على أيديولوجيات أبوية، بنفوذ كبير على الفضاءات الرقمية والخطاب العام. ويتم توظيف هذا النفوذ لتنسيق وتضخيم المضايقات الموجهة، ومن خلال شبكات منظمة ومؤيدين عبر الإنترنت، يمكن لهذه الجهات مواصلة حملات الترهيب والهجمات على السمعة التي تتجاوز المنافسة السياسية لتستهدف الأفراد بشكل مباشر. وبذلك، يعاقب العنف الرقمي الظهور العلني ويدفع الأفراد إلى الخروج من النقاش العام.

2.2 لماذا تواجه النساء والمدافعات عن حقوق الإنسان ومدافعو ومدافعات مجتمع الميم-عين تعرضاً متصاعداً للخطر؟

2.2

إن الأوضاع القانونية والاجتماعية المتغيرة التي تواجه مجتمعات الميم-عين في منطقة الشرق الأوسط وشمال أفريقيا، والتحول الخاص الذي شهده لبنان بين عامي 2020 و2023، موثقة في أبحاث منظمة هيومينا المنشورة^[5]. The political pressure on women in public life and on LGBTQI+ defenders described in the rest of this section sits within that broader pattern.

يؤثر التعرض للعنف الرقمي خلال الفترات السياسية الحساسة في النساء أكثر من غيرهنّ، وفي المدافعات عن حقوق الإنسان ومدافعات مجتمع الميم-عين، وذلك نتيجة تشابك عوامل النوع الاجتماعي والأعراف الاجتماعية والظهور السياسي العلني. إذ كثيراً ما تتحدى مشاركتهم في الحياة العامة الأعراف السائدة وبني السلطة القائمة، مما يجعلهم أكثر عرضة للاستهداف عبر هجمات ممنهجة قائمة على الهوية.

وتُعدّ النساء الأكثر هشاشة أمام هذه الأشكال من الإساءة، بفعل الأعراف الجندرية المتجذّرة التي تُصوّرهن فاعلات سياسيات غير شرعيات. ونتيجةً لذلك، يغدون أكثر عرضة للهجمات الجندرية والشخصية والتي تستهدف سمعتهم، بهدف النيل من مصداقيتهم وردعهم عن المشاركة في الحياة العامة.^[1] وكثيراً ما تتخذ الإساءة الإلكترونية الموجهة ضد النساء طابعاً جنسياً واستباحياً، إذ تنصبّ على مظهرهن وسلوكهن وأخلاقهن الفتوّرة، بدلاً من مواقفهن السياسية أو كفاءاتهن. وفي حالات كثيرة، تتعرض المرشحات لتعليقات تتناول مظهرهن الخارجي وملابسهن وحياتهن الشخصية، مما يحوّل الأنظار عن الجدارة والكفاءة ويُرسّخ الصور النمطية الضارة التي تُضيّق دورهن في الحياة العامة.

تشكل الأعراف الثقافية والاجتماعية في لبنان الطريقة التي يُنظر بها إلى النساء ويُعاملن بها في الحياة العامة. وتُصوّر القيم الأبوية المتجذّرة النساء على أنهن غير مؤهلات أو أقل قدرة على تولي مناصب السلطة. وخلال الفترات السياسية الحادة، تتضخم مثل هذه الروايات ويتم توظيفها لإضعاف مشاركة النساء وتشويه سمعتهم وتقويض شرعيتهم، لا سيما أولئك اللواتي يتحدّين الهياكل السياسية الراسخة. تُطّيع هذه الثقافة الأبوية الإساءة الجندرية في الفضاءات الرقمية، كما أنها تترع الشرعية عن قدرة النساء على المشاركة في الحياة العامة، مما يحدّ بشكل أكبر من التمثيل السياسي العادل.

تواجه المدافعات عن حقوق الإنسان مستويات إضافية من المخاطر بسبب طبيعة عملهن، لا سيما عند مناصرة قضايا حساسة مثل المساواة والحوكمة والمساواة الجندرية والدفاع عنها. وغالباً ما يضعهن نشاطهن في مواجهة مباشرة مع جهات فاعلة ذات نفوذ، مما يزيد من احتمالية تعرضهن لهجمات منسقة ومراقبة وترهيب. وينعكس هذا النمط في جميع أنحاء منطقة الشرق الأوسط وشمال أفريقيا. وقد وجدت دراسة أجرتها منظمة Fe-Male حول العنف الرقمي ضد المدافعات عن حقوق الإنسان في منطقة الشرق الأوسط وشمال أفريقيا (53 من أصل 115 مشاركة كنّ ناشطات لبنانيات) أن **78.3% من المشاركات أفدن بتعرضهن للعنف عبر الإنترنت**. وغالباً ما كان ذلك في شكل رسائل جنسية أو عنصرية أو معادية للمثليين.^[2] بالإضافة إلى ذلك، تعرضت 97.4% منهن لشكل واحد على الأقل من أشكال التمييز القائم على النوع الاجتماعي، بما في ذلك التعليقات على المظهر أو نمط الحياة، والتهديدات ذات الطابع الجنسي.^[3] تكشف هذه الأنماط عن المدى الذي بلغه العنف الرقمي ضد المدافعات عن حقوق الإنسان، إذ تتسم هذه الظاهرة بالانتشار الواسع والطابع الجندري العميق الجذور، مما يُعزّز المساعي الرامية إلى إسكات مشاركتهن في الحياة العامة.

في ظل هذه الأعراف الثقافية، يظل التوجه الجنسي والهوية الجندرية من المسائل بالغة الحساسية في لبنان، ولا سيما في السياقات السياسية، حيث قد يترتب على الظهور العلني تبعات اجتماعية وشخصية وقانونية جسيمة. وعلى الرغم من أن العلاقات المثلية بالتراضي لا تُجرّم صراحةً في قانون العقوبات اللبناني، فقد جرى توظيف المادة 534 تاريخياً لملاحقة هذه العلاقات، وذلك على الرغم من صدور عدة أحكام قضائية بين عامي 2007 و2018 أكدت أن العلاقات المثلية بالتراضي ليست مخالفة للقانون. وفي يوليو 2023، تقدّم عدد من أعضاء البرلمان بمقترح قانون لإلغاء المادة 534.

^[4] غير أن الموقعين على المقترح تعرّضوا لاحقاً لحملة تحرش إلكتروني من قِبل فاعلين سياسيين ودينيين، مما دفع أحد البرلمانيين إلى سحب توقيعه. ونتيجةً لذلك، لا يخوض معظم من قد ينتمون إلى مجتمع الميم-عين الانتخابات بشكل علني، وكثيراً ما تبرز النقاشات حول هوياتهم عبر التكهّنات لا من خلال التعريف الذاتي. بيد أن العنف الرقمي يتقاطع أحياناً مع التوجه الجنسي الفعلي أو الفُتوّرة خلال الفترات الانتخابية أو في أوقات التوترات السياسية المتصاعدة. وقد تعرّض مرشحون وناشطون من مجتمع الميم-عين في بعض الأحيان لإشاعات وتلميحات واتهامات تتعلق بميولهم الجنسية بهدف النيل من مصداقيتهم. ويُوظّف هذا النوع من الكشف التخميني بصورة استراتيجية لتحويل الأنظار عن البرامج السياسية، وتصوير المرشحين بوصفهم خارجين عن المعايير الاجتماعية أو غير مؤهلين أخلاقياً في السياق المحافظ اللبناني. وهكذا يُستخدم الكشف عن الهوية أداة للعنف الرقمي في الانتخابات لفرز من يُعدّون ثقافياً مقبولين في الحياة العامة، مما يُرسّخ الخطاب المعادي لمجتمع الميم-عين ويُكرّس إقصاءه من الفضاء السياسي.

في سياق سياسي تُقيد فيه حتى مشاركة النساء، يواجه أفراد مجتمع الميم-عين عوائق أكبر تحول دون دخولهم إلى الحياة السياسية. فالوصمة الاجتماعية والمخاطر القانونية المحتملة واحتمال التعرض لهجمات رقمية موجهة تجعل الترشح للمنصب السياسي بشكل علني أمراً مستحيلًا، مما يجبر الأفراد في كثير من الأحيان على إخفاء جوانب من هوياتهم أو الامتناع عن المشاركة في الحياة السياسية تماماً. وهذا يؤدي إلى مزيد من تقييد الحيز المدني والحد من المشاركة السياسية الشاملة.

أنواع الهجمات التي يغطيها هذا الدليل

يقدم هذا القسم للمستخدمين لغةً مشتركة لتوصيف الأذى الذي قد يتعرضون له. وتكتسب التسمية الدقيقة أهمية لأنها تؤثر في مسار الاستجابة، ومستوى الاستعجال، واحتياجات الدعم.

تشمل الأشكال الرئيسية للهجمات عبر الإنترنت التي يغطيها الحقيبة: العنف الرقمي، وكشف ونشر البيانات الشخصية دون إذن، والفضح وانتحال الهوية، والتحرش المنشق. يهدف هذا القسم إلى تعريف كل نوع من هذه أشكال العنف بما يتيح للمستخدمين تحديد التهديد، وتقييم مستوى الخطر، ودرجة الاستجابة المطلوبة، ونوع الدعم المحتمل. عملياً، من المهم الإشارة إلى أن التهديدات الرقمية غالباً ما تكون مترابطة وقد تحدث في الوقت نفسه.

العنف المبني على النوع الاجتماعي الميسر بالتكنولوجيا

3.1

يشير العنف الرقمي إلى أي فعل يُرتكب أو يُدعم أو يتفاقم من خلال استخدام تكنولوجيا المعلومات والاتصالات ووسائل الإعلام الرقمية، ويؤدي أو يُحتمل أن يؤدي إلى أذى جسدي أو جنسي أو نفسي أو اجتماعي أو سياسي أو اقتصادي، فضلاً عن انتهاك الحقوق والحريات.^[6] وبينما يرتبط هذا المفهوم في الأصل بالعنف الموجه ضد النساء، يُستخدم مصطلح العنف الرقمي اليوم على نطاق أوسع ليشمل الأذى الذي يستهدف الأفراد على أساس هويتهم الجندرية أو توجههم الجنسي.^[7]

في الفضاءات الرقمية، يتخذ العنف الرقمي أشكالاً متعددة ومتداخلة، بما في ذلك الإساءة الجندرية، والتهديدات ذات الطابع الجنسي، والإذلال، والترهيب، وهي ممارسات غالباً ما تحدث بالتزامن. وتتجلى هذه الأفعال في استخدام لغة مهينة تستهدف جنس الشخص أو هويته، أو في توجيه تعليقات أو تهديدات جنسية غير مرغوب فيها بهدف إثارة الخوف، أو في مشاركة المحتوى أو التلاعب به بغرض التشهير بالأفراد وتقويض سمعتهم علناً. وغالباً ما تتسم هذه الانتهاكات بالتردد أو التكرار أو التنسيق أو التضخيم عبر منصات متعددة، مما يتيح لها الانتشار السريع والوصول إلى جمهور أوسع. وقد يلجأ المعتدون إلى أساليب مختلفة، مثل التحرش والتعقّب أو نشر المحتوى الجنسي دون موافقة، لزيادة الضغط على الناجيات وفرض السيطرة عليهن. ونتيجة لذلك، يمكن أن تتصاعد هذه الأشكال من العنف بمرور الوقت، وأن تزداد حدتها وتأثيرها وانتشارها، مما يخلق بيئات مستدامة من الخوف تقي الأفراد عن المشاركة في الحياة العامة والمدنية.

العنف الرقمي في الممارسة العملية

- استخدام اللغة المهينة أو اللغة ذات الطابع الجندري والتحيز الجنسي.
- الرسائل الجنسية غير المرغوب فيها أو التهديدات، والتعليقات الموجهة على المظهر أو الأخلاق، و/أو
- محاولات استثارة الخوف أو الخزي أو الإسكات.

نشر البيانات الشخصية دون إذن

3.2

يشير مصطلح نشر البيانات الشخصية دون إذن إلى الكشف المتعمد عن المعلومات الخاصة أو التعريفية لشخص ما عبر الإنترنت دون موافقته. وقد يشمل ذلك تفاصيل مثل أرقام الهواتف، وعناوين المنازل، ومعلومات مكان العمل، والصلات العائلية، أو غيرها من البيانات الحساسة. ورغم أن بعض هذه المعلومات قد تكون موجودة بالفعل على الإنترنت، فإن الكشف عنها بشكل موجه في سياق عدائي يمكن أن يزيد المخاطر بشكل كبير، حيث يجعل من السهل تحديد مكان الأفراد أو الاتصال بهم أو مضايقتهم. يمكن أن يتصاعد نشر البيانات الشخصية دون إذن بسرعة ويمتد ليتحول إلى تهديدات وأضرار في العالم الواقعي. وتعد أنواع معينة من الإفصاح عن المعلومات، مثل عناوين المنازل المواقع الجغرافية الآنية ومعلومات الاتصال الشخصية، خطيرة بشكل خاص، لأنها تزيد من الضعف وتقوض قدرة الفرد على الحفاظ على سلامته وخصوصيته عبر الإنترنت وفي العالم الواقعي. ويزداد هذا الخطر بشكل خاص خلال فترات التوترات السياسية، مثل الانتخابات، حيث قد يؤدي إلى تكثيف الاستهداف وتفاقم شدة الهجمات.

نشر البيانات الشخصية دون إذن في الممارسة العملية

- مشاركة أرقام الهواتف وعناوين البريد الإلكتروني والمواقع المنزلية أو مواقع العمل أو المواقع الجغرافية الآتية دون موافقة، بهدف حشد الناس لإلحاق الضرر،
- مشاركة معلومات حساسة عن أفراد الأسرة،
- تلقي أعداد متزايدة من المكالمات والرسائل المجهولة التي تتضمن تهديدات أو مضايقات، و/أو
- تهديدات تشير إلى معرفة معلومات خاصة وشخصية.

الفضح

3.3

يُشير مصطلح «الفضح» إلى الإفصاح عن التوجه الجنسي لشخص ما أو هويته الجندرية أو غيرها من الجوانب الحساسة في هويته دون موافقته. وفي الممارسة العملية، قد يشمل ذلك مشاركة معلومات خاصة أو صور أو تفاصيل شخصية بطرق تكشف عن الأفراد أمام الآخرين قبل أن يكونوا مستعدين للإفصاح عن أنفسهم أو راغبين في ذلك. وفي لبنان، حيث قد تُوظف القوانين والأعراف الاجتماعية لاستهداف أفراد مجتمع الميم-عين، يمكن أن يُفضي الكشف عن الهوية إلى مخاطر فورية وجسيمة، تشمل الوصمة الاجتماعية والنابذ الأسري وفقدان العمل والتعرض لأذى قانوني أو جسدي محتمل. وقد تتفاقم هذه المخاطر خلال فترات الحضور العام المتصاعد، حيث يمكن توظيف الكشف الموجّه أداةً للترهيب بهدف إسكات الأفراد وإقصائهم من الفضاء العام.

والفضح في الممارسة العملية

- انتشار الإشاعات الإلكترونية أو التلميحات أو الادعاءات المباشرة بشأن الهوية الجنسية أو التوجه الجنسي لشخص ما،
- الضغط على الشخص لتأكيد هويته أو نفيها،
- تداول محادثات خاصة أو صور أو تفاصيل تتعلق بالهوية الجنسية أو التوجه الجنسي لشخص ما، و/أو
- الابتزاز والتهديد بالكشف عن هوية الشخص ما لم يمتثل أو يلتزم الصمت.

انتحال الهوية

3.4

يُشير مصطلح «انتحال الهوية» إلى إنشاء هويات مزيفة أو حسابات وهمية أو ملفات شخصية مُعدّلة، أو نسب أقوال كاذبة إلى شخص ما بهدف التظاهر بأنه الشخص المستهدف دون موافقته. وفي الممارسة العملية، يُوظف انتحال الهوية لنشر معلومات مضللة باسم الناجيات، بما يلحق الضرر بسمعتهنّ ويستثير المضايقات ضدّهنّ أو يُعرّضهن لمزيد من الإساءة أو المخاطر الأمنية. وقد يتجلى ذلك في صورة حسابات احتيالية تُنشأ لنشر محتوى مُضّر أو مُضلل، أو تصريحات وصور مُختلفة تُنسب زوراً إلى الشخص المستهدف، أو اتصالات خادعة تهدف إلى تضليل الآخرين أو النيل من الثقة بهم أو انتزاع المعلومات منهم تحت ادعاءات كاذبة. وخلال فترات التوترات السياسية المتصاعدة، قد يُستخدم انتحال الهوية لتقويض مصداقية الأفراد، أو تشويه توجهاتهم وانتماءاتهم السياسية، أو استثارة ردود الفعل العدائية ضدهم. وهذا من شأنه أن يخرق في السلامة الشخصية، ويلحق الضرر بالمكانة المهنية والسياسية، وصولاً إلى تقييد الأفراد عن المشاركة في الحياة العامة والمدنية.

انتحال الهوية في الممارسة العملية

- إنشاء حسابات وهمية تستخدم اسم شخص ما أو صورته أو هويته دون إذن،
- نشر تصريحات أو محتوى باسم شخص ما دون علمه أو موافقته،
- لقطات شاشة أو اقتباسات مُعدّلة تُنسب زوراً إلى الشخص المستهدف،
- تلقي معلومات من أصدقاء بشأن اتصالات ورسائل مريبة صادرة عن حسابات تنتحل هوية الشخص المستهدف، و/أو
- إرسال رسائل إلى أشخاص آخرين بانتحال هوية شخص ما بهدف انتزاع المعلومات منهم.

التحرش المنسق

3.5

يُشير مصطلح «التحرش المنسق» إلى الإساءة الموجهة التي ينفذها أفراد أو مجموعات أو شبكات متعددة بشكل متعمّد ومنظّم، بهدف ترهيب شخص ما أو إسكاته أو النيل من مصداقيته أو إرهابه. وخلافاً للحوادث الفردية المعزولة، ينطوي التحرش المنسق على هجمات متكررة أو متزامنة قد تتضاعف عبر حسابات ومنصات وقنوات تواصل متعددة، مما يزيد من نطاق الأذى وحدّته. وقد تتجلى هذه الهجمات في صورة استهداف جماعي عبر رسائل مسيئة أو حملات الاستفزاز الإلكتروني أو النشر المتعمّد لمحتوى ضارّ يهدف إلى إثارة الخوف. وكثيراً ما تتقاطع هذه الهجمات مع التضليل الإعلامي وانتحال الهوية والتهديدات والمراقبة، وقد تتصاعد بسرعة من خلال التضخيم عبر شبكات منظّمة أو حسابات آلية. وفي حالات التحرش المنسق، يتولّد الأذى بشكل جماعي لا من خلال معتدٍ واحد، وغالباً ما يتجاوز ذلك قدرة الاستجابات الاعتيادية على التعامل معه. وهذا ما يغيّر في الغالب مستوى الاستجابة المطلوبة، إذ يستلزم إجراء تقييم سريع للمخاطر، وتوثيق الأنماط، واتخاذ تدابير حماية جماعية، والتصعيد نحو الدعم المؤسسي أو القانوني أو الأمني متى أمكن ذلك. ونتيجةً لذلك، يمكن أن يفضي التحرش المنسق إلى خلق بيئة مستدامة من الترهيب تُرغم الأفراد على فرض رقابة ذاتية على أنفسهم أو الانسحاب من الحياة العامة، مما يُلقي بظلاله على السلامة الشخصية والحياة المدنية والسياسية الشاملة.

التحرش المنسق في الممارسة العملية

- ارتفاع مفاجئ في التعليقات أو الرسائل العدائية الصادرة عن حسابات أو أشخاص مختلفين،
- نشر محتوى متشابه أو متطابق عبر حسابات متعددة،
- هجمات وحملات منظّمة تقع في آن واحد عبر منصات وحسابات متعددة،
- توظيف حسابات تبدو آلية أو مجهولة الهوية أو حديثة الإنشاء لنشر محتوى ورسائل عدائية، و/أو
- تحريك أفراد أو مجموعات لآخرين لمهاجمة شخص ما أو الإبلاغ عنه أو النيل من مصداقيته في الوقت ذاته.

الصور الحميمة المنشورة دون موافقة والتزييف العميق

3.6

يُشير مصطلح الصور الحميمة المنشورة دون موافقة إلى مشاركة صور حميمة أو جنسية أو عارية لشخص ما أو توزيعها أو التهديد بتوزيعها دون موافقته.

تُعَدّ الصور الحميمة المنشورة دون موافقة، بما فيها الصور الحقيقية والمحتوى الجنسي المُولّد بالذكاء الاصطناعي أو المُعدّل، من أشد أشكال العنف الرقمي الذي تواجهه النساء في الحياة العامة. وهي مصقّمة لإلحاق الأذى النفسي والإضرار بالسمعة وممارسة ضغط اجتماعي يدفع إلى الانسحاب من المشاركة العامة. وفي منطقة الشرق الأوسط وشمال أفريقيا، يزايد توثيق هذا التكتيك الموجه ضد السياسيات والمرشحات والمدافعات عن حقوق الإنسان، بما في ذلك عبر محتوى التزييف العميق المُولّد بالذكاء الاصطناعي الذي ينشئ صوراً حميمة لأشخاص حقيقيين دون أن تكون ثمة صورة حقيقية قد وُجدت أصلاً. وكثيراً ما يكون التهديد بالكشف بالغ الضرر بقدر الكشف ذاته.

ويمكن أن تستهدف الناشطات والمرشحات من النساء ومجتمع الميم-عين بالصور الحميمة المنشورة دون موافقة المُختلقة، ولا يُقلّل طابعها المُختلّق من حجم الضرر الناجم عنها. بل إن محتوى التزييف العميق ينتشر بسرعة، ويصعب دحضه بشكل قاطع دون إجراء تحليل جنائي رقمي، ويُلاحق الأضرار النفسية والسمعة والاجتماعية ذاتها التي تُلاحقها الصور الحقيقية.

مشاركة الصور الحميمة المنشورة دون موافقة ومحتوى التزييف العميق في الممارسة العملية

- صور أو مقاطع فيديو حقيقية أنشئت أصلاً بموافقة أصحابها لكنها سُوركت دون موافقتهم.
- صور أو مقاطع فيديو حُصل عليها عبر اختراق الأجهزة أو المساس بها أو الإكراه.
- محتوى مُولّد بالذكاء الاصطناعي أو مُعدّل، بما في ذلك التزييف العميق، يُصوّر شخصاً حقيقياً في مشاهد جنسية أو حميمة لم تقع قط.
- محتوى مُعدّل يجمع بين صور حقيقية للشخص المستهدف ومحتوى جنسي مُفبرك.
- التهديد بمشاركة هذا المحتوى وسيلةً للابتزاز أو الإكراه، حتى حين لا تكون أي صورة قد انتشرت بعد.

IMPORTANT ▲

ملاحظة مهمة: قبل تقديم شكوى قانونية رسمية إلى المؤسسات الحكومية (كقوى الأمن الداخلي)، راجعي قسم «تقديم شكوى جنائية بشأن الصور الحميمة المنشورة دون موافقة»، وتواصلي مع المنظمات المتخصصة قبل اللجوء إلى السلطات [انظري: 9.4 قائمة الموارد].

اعتبارات خاصة بلبنان

ينطوي تقديم شكوى جنائية تتعلق بالصور الحميمة المنشورة دون موافقة في لبنان على المخاطر ذاتها التي نوقشت في القسم 9.2 اعتبارات السلامة الموهقة قبل طلب المساعدة، أدناه: إذ قد لا تكون المؤسسات الحكومية، بما فيها قوى الأمن الداخلي، آمنة أو يسهل الوصول إليها، ولا سيما بالنسبة لأفراد مجتمع الميم-عين أو النساء اللواتي يمكن أن تُستخدم صورهن ضدهن في ظل الأعراف الاجتماعية السائدة. استشاري منظمة Legal Agenda أو المركز اللبناني لحقوق الإنسان أو منظمة أبعاد قبل النظر في أي شكوى رسمية، ولا تتوجهي إلى المؤسسات الحكومية حاملة أدلة حميمة دون وجود مستشار قانوني.

أولويات الاستجابة الفورية

- **احتفظي بجميع الأدلة** — بما فيها المحتوى المسيء ذاته، حتى وإن كان مؤلماً — قبل تقديم بلاغات للمنصات، إذ كثيراً ما يزال المحتوى بسرعة عقب الإبلاغ وقد يكون ضرورياً لاتخاذ إجراءات قانونية أو توثيق الأنماط.
- في حالات التزييف العميق أو المحتوى المُؤلّد بالذكاء الاصطناعي، **وثّقي التناقض مع أدلة حقيقية وقابلة للتحقق** (صور أصلية من الفترة ذاتها، وسجلات الموقع، وشهادات الشهود) لدعم طلبات الإزالة وأي توضيح علني.
- **أبلغِي عبر مسار إزالة الصور الحميمة المنشورة دون موافقة المخصص لكل منصة.** توفر المنصات الكبرى عمليات مراجعة مُعجّلة لهذه الفئة من المحتوى، وإن تفاوتت أوقات الاستجابة.
- استخدم [StopNCII.org](https://stopncii.org)، وهي خدمة مجانية تعتمد على مطابقة البصمة الرقمية وتديرها خط مساعدة الناجيات من الصور الحميمة المنشورة دون موافقة، لمنع مسبقاً مشاركة الصور الحميمة المعروفة على منصات مثل ميتا وتيك توك وإكس (X) وريديت وأولني فانز وبامبل وغيرها من المنصات الرئيسية. وتعمل هذه الخدمة حتى في حال لم يُنشر المحتوى علناً بعد.

الهجمات المتداخلة والمتصاعدة

3.7

لا تقع هذه الأشكال من الإساءة الإلكترونية دائماً بوصفها حوادث معزولة أو منفصلة بشكل واضح. ففي الممارسة العملية، كثيراً ما تتداخل أوجه الأذى وتتعرّض بعضها بعضاً وتتطور بمرور الوقت، إذ قد يُهبى شكل واحد من أشكال الإساءة الظروف لظهور شكل آخر أو تصاعده. فما قد يبدأ على سبيل المثال كمضايقات موهجة، قد يتصاعد ليتحول إلى هجمات منسقة وانتحال للهوية وحتى نشر للبيانات الشخصية دون إذن، مما يزيد من التعرض للخطر والهشاشة. وعلى نحو مماثل، قد تُوظّف هذه التكتيكات في آن واحد، إذ يلجأ المعتدون إلى توليفة من الأساليب المتعددة لتكثيف الضغط وتعظيم الأذى.

وخلال الانتخابات وفترات التوترات السياسية المتصاعدة، قد تتصاعد هذه الأنماط بسرعة. ويمكن أن يزيد تراكم أوجه الأذى من حدة التهديدات وعدم قابليتها للتنبؤ، لا سيما حين تُفرز الإساءة الرقمية مخاطر على السلامة خارج المجال الرقمي، وتشويهاً للسمعة، وعقبات أمام مواصلة المشاركة. ولهذا السبب، ينبغي فهم الحوادث وتقييمها باعتبارها متشابكة ومتراصة في ما بينها، لا معالجتها بوصفها أحداثاً منفردة. والإدراك بأن هذه الحوادث ذات طبيعة متراكبة ومتعددة الأبعاد من شأنه أن يدعم تقييماً أكثر فعالية للمخاطر وتوثيقها والاستجابة لها.

الهجمات المتداخلة والمتصاعدة في الممارسة العملية

- تحوّل المضايقات إلى نشر البيانات الشخصية دون إذن وتهديدات في المجال الرقمي،
- انتحال الهوية مقروناً بهجمات منسقة بهدف تضخيم الأذى، و/أو
- قيام هجمات منسقة بتسريب معلومات شخصية، مما يؤدي إلى نشر البيانات الشخصية دون إذن وتهديدات خارج الإنترنت تستهدف الشخص المعني وأفراد أسرته.

استهداف الصحفيات

3.8

- تُعدّ الصحفيات في لبنان — ولا سيما اللواتي يُغطين الشأن السياسي والفساد والقضايا الجنديرية والديناميكيات الطائفية وحقوق مجتمع الميم-عين — من أكثر الفاعلين المدنيين استهدافاً بصورة منتظمة في الفضاء الرقمي اللبناني. وقد وثّقت كلّ من منظمة مهارات وسكايز ومؤسسة سمير قصير أنماطاً مستدامة من المضايقات ونشر البيانات الشخصية دون إذن وانتحال الهوية الموجهة ضد الصحفيات العاملات في المطبوعات والإذاعة والمنافذ الإعلامية الرقمية المستقلة. وتختلف هذه الأنماط عن تلك التي تواجهها المرشحات والمدافعات عن حقوق الإنسان في عدة جوانب:
- كثيراً ما تصدر الهجمات عن شبكات موالية للجهات التي تتناولها تقاريرهن — أحزاب سياسية وأجهزة أمنية ومصالح تجارية — لا عن جماهير مجهولة الهوية.
 - التبعات المهنية أكثر مباشرة: إذ يتعرض المدرون والمعلنون والمنافذ الإعلامية لضغوط مصقمة للحدّ من مهام الصحفيات أو إجبارها على التراجع عن تقاريرها.
 - كثيراً ما يُستهدف أفراد أسرة الصحفيات ومصادرها بالتوازي مع استهدافها، مستغلّين شبكتها المهنية.
 - ينبغي أن تكون منظمات حرية الصحافة (مهارات، وسكايز، ومنظمة مراسلون بلا حدود) المرجع الأول للإحالة إلى جانب منظمات حقوق المرأة والأمن الرقمي المشار إليها في أقسام أخرى من هذا الدليل.

الاستهداف العابر للحدود والجاليات اللبنانية في الخارج

3.9

- يواجه المدافعات عن حقوق الإنسان، والمرشحات، والناشطات من مجتمع الميم-عين بشكل متكرر أشكالاً من العنف الرقمي ذات بُعد عابر للحدود. وتبرز ثلاثة أنماط شائعة في هذا السياق: نساء لبنانيات داخل لبنان يتعرضن لهجمات من شبكات تعمل من خارج البلاد (مثل دول الخليج أو أمريكا الشمالية أو أوروبا)؛ ونساء لبنانيات في الاغتراب يتعرضن لهجمات من شبكات تنشط من داخل لبنان؛ وحملات منشقة تمتد عبر كلا النطاقين الجغرافيين، مستفيدة من القيود العملية لإنفاذ القانون على المستوى الوطني.

انعكاسات ذلك على الاستجابة:

- يصبح الإبلاغ عبر المنصات الرقمية أكثر أهمية من تقديم الشكاوى القانونية، لأن المنصات تعمل عبر الحدود بينما تظل المحاكم محصورة بالنطاق الوطني.
- ينبغي أن يتضمن التوثيق تسجيل الأصل الجغرافي الظاهر للحسابات عند توفره (مثل لغة إنشاء الحساب، وأنماط المنطقة الزمنية، ومؤشرات البلد)، لأن ذلك يساعد في تحديد الجهات أو المنظمات القادرة على تقديم استجابة فعّالة.
- بالنسبة للمستخدمين في الاغتراب، قد تكون منظمات حقوق المرأة ومنظمات مجتمع الميم-عين في بلد الإقامة مساراً أسرع للحصول على الدعم مقارنة بالمنظمات اللبنانية التي تعمل عن بُعد وعبر المسافات.

التعرّف السريع على المخاطر وتصنيفها حسب درجة الخطورة

يمكن أن تتصاعد الهجمات الرقمية بسرعة، لا سيّما خلال فترات التوتر السياسي المرتفع عندما يكون العنف الرقمي مدفوعاً باعتبارات سياسية. ويُعدّ التعرّف المبكر على المخاطر أمراً بالغ الأهمية لمنع وقوع الأذى، وتقليل التعرّض له، وتحديد مسار الاستجابة المناسب وفقاً لدرجة خطورة الحالة.

الأسئلة التي يجب طرحها على الفور

4.1

عند مواجهة هجوم محتمل، يمكن أن تساعد الأسئلة التالية في تحديد مستوى الخطر ومدى إلحاح الاستجابة المطلوبة. هذه الأسئلة ليست شاملة، ولكنها تهدف إلى توجيه الوعي الفوري بالوضع:

ما نوع الهجمات التي تحدث؟

يساعد ذلك في تحديد طبيعة التهديد والاتجاه المحتمل لتصاعده.

- هل يتعلق الأمر بمضايقات، أو عنف قائم على النوع الاجتماعي الميسّر تكنولوجياً، أو نشر البيانات الشخصية دون إذن، أو انتحال الهوية، أو الفضح، أو التحرش المنشق؟ [راجعوا القسم 3: أنواع الهجمات التي يغطيها الدليل]

- هل تحدث أنواع مختلفة من الهجمات في آنٍ واحد؟

- هل هذه حادثة منفردة أم أنها متكررة؟

أين يحدث الهجوم؟

يساعد ذلك في تقييم مستوى التعرّض واتساع نطاق الانتشار. فالهجمات العلنية والمتعددة المنصات تميل إلى التصاعد بشكل أسرع والوصول إلى جمهور أوسع، مما يزيد من المخاطر الأمنية.

- هل يحدث على منصات عامة وعبر حسابات متعددة؟
- هل يتم عبر رسائل خاصة ويتضمن ابتزازاً؟
- هل يحدث داخل مجموعات مغلقة؟

هل تم نشر أي معلومات شخصية أو حساسة بشكل علني؟

يساعد ذلك في تقييم مستوى الخطر الفوري على السلامة، لا سيّما احتمال وقوع أذى خارج الإنترنت أو التواصل المباشر.

- هل تم نشر أو ذكر أرقام الهواتف، أو العناوين، أو مكان العمل، أو تفاصيل العائلة، و/أو محتوى خاص؟
- هل تم تلقي مكالمات أو رسائل مزعجة ومتكررة من أرقام غير معروفة؟

هل الهجوم منشق أم متكرر؟

يساعد ذلك في التعرف على الاستهداف المنظم والمضايقات. إذ يكون التحرش المنشق أصعب في السيطرة عليه، وأسرع في التصاعد، ويستلزم في الغالب تدابير استجابة أكثر صرامة.

- هل تنشر حسابات متعددة رسائل متشابهة؟

- هل يظهر المحتوى ذاته عبر منصات مختلفة؟

هل توجد تهديدات، سواء كانت صريحة أو ضمنية؟

يساعد ذلك في تحديد درجة الخطورة. فوجود التهديدات، لا سيما تلك المؤنقة أو المتكررة، يشير إلى تصعيد الموقف.

- هل تتضمن الرسائل عبارات تشير إلى إيذاء جسدي و/أو تهديدات بالقتل؟

- هل تشير الرسائل إلى العنف الجنسي؟

- هل تلمح الرسائل إلى الإضرار بالسمعة؟

- هل تهدف الرسائل إلى التهريب؟

هل يتصاعد الوضع؟

يساعد ذلك في تتبع تطور الأحداث، وضمان أن تكون الاستجابة متناسبة مع مستويات المخاطر الفعلية.

هل هناك أي مؤشرات على وجود خطر خارج الإنترنت؟

يساعد ذلك في تحديد الخطر المباشر. فأى صلة بين الأنشطة عبر الإنترنت وخارجها ترفع مستوى الخطورة بشكل كبير.

- هل حاول أي شخص الاتصال مباشرةً بالهدف أو تحديد مكانه؟
- هل تم ذكر تحركات الشخص المستهدف أو الإيحاء بوجود قرب جسدي منه؟

- هل تزايدت وتيرة الهجوم وحدته؟
- هل أصبحت اللهجة أكثر عنفاً؟
- هل تزايدت التهديدات والابتزاز؟

هل يمكن تحديد هوية الشخص أو المجموعة التي تقف وراء الهجمات؟

يساعد ذلك في تقييم القدرة والنية. إذ قد تكون الهجمات المرتبطة بجهات فاعلة أو شبكات منظمة أكثر استمرارية واستراتيجية وأصعب في الاحتواء.

- هل ثمة حسابات مجهولة الهوية أو حديثة الإنشاء ضُقت خصيصاً لتنفيذ هذه الهجمات؟
- هل ثمة حسابات آلية؟
- هل ثمة حسابات مرتبطة بأفراد أو مجموعات أو جهات فاعلة سياسية معروفة؟

هل يشمل الهجوم أشخاصاً آخرين من حولك؟

يساعد ذلك في تقييم اتساع نطاق التأثير. فعندما تمتد الهجمات لتشمل أشخاصاً آخرين، تزداد المخاطر بشكل كبير، ويتطلب ذلك تغييراً في أسلوب الاستجابة.

- هل يتم ذكر أفراد العائلة أو الزملاء أو المعارف؟
- هل يتم التواصل معهم؟
- هل يتم استهدافهم في الرسائل أو المحتوى؟

ينبغي النظر في الإجابات على هذه الأسئلة مجتمعة لا منفردة. فحتى إذا بدا أن تأثير الوضع محدود، فإن وجود مؤشرات خطر متعددة، كالحضور العلني أو التنسيق أو التعرض لنشر البيانات الشخصية دون إذن، قد يشير إلى مستوى أعلى من الخطر ويستوجب استجابة أكثر إلحاحاً.

4.2 حين تصدر الهجمات عن شركاء حميمين أو أفراد الأسرة

4.2

قد تصدر الهجمات الرقمية الموجهة ضد المرشحات والمدافعات عن حقوق الإنسان ومدافعي ومدافعات مجتمع الميم-عين والفاعلين المدنيين، أحياناً ولا سيما خلال الفترات السياسية النشطة، عن شركاء حميمين حاليين أو سابقين، أو عن شبكات تتصرف نيابة عنهم.

وتستوجب الهجمات الصادرة عن شركاء حميمين استجابات وتقييمات مختلفة. وتشمل المخاطر المرتبطة بالعنف الأسري والعلاقات الحميمة ما يلي:

- **معرفة عميقة بالروتين اليومي والحياة الخاصة.** يمتلك الشريك الحالي أو السابق معرفة مباشرة بعنوان منزلك وجدولك اليومي ومكان عملك والأماكن التي تتردد عليها وأفراد عائلتك وعلاقاتك الشخصية. مما يزيد بشكل واضح من خطر التعرض للأذى خارج المجال الرقمي.
- **الوصول إلى وسائل الإعلام الخاصة والاتصالات.** قد يكون المعتدون في سياق العنف العشير قد حصلوا أو سبق لهم الحصول على صور خاصة أو اتصالات شخصية أو معلومات حساسة يمكن توظيفها في الابتزاز أو مشاركة الصور الحميمة غير المتوافق عليها أو الكشف الموجه. وقد يسبق هذا الوصول وقوع الهجوم بأشهر أو سنوات.
- **دوافع مختلطة ومتشابكة.** غالباً ما تتبع الهجمات الصادرة عن العنف العشير من تضافر الشكوى الشخصية والرغبة في السيطرة والدوافع السياسية أو المتعلقة بالسمعة. ويجعل هذا التشابك الهجمات أكثر استمرارية وأشد تخطيطاً في مضمونها وأصعب في الاحتواء.
- **الوصول عبر الحسابات المشتركة أو المترابطة.** إذا سبق مشاركة الأجهزة أو الحسابات أو التخزين السحابي أو أنظمة المشاركة العائلية مع الشريك أو إتاحتها له، فقد يظل بإمكانه الوصول إليها وقد يستغلها بنشاط. راجعوا القسم 5.3 تقليل التعرض الفوري للاطلاع على خطوات أمان الحساب الفورية.

تدابير التخفيف

تستلزم توصيات الاستجابة القياسية الواردة في هذا الدليل تكيفاً دقيقاً حين تصدر الهجمات عن شريك حميم أو في سياق العنف الأسري. وفيما يلي الخطوات المناسبة للتابع:

- **انتقي من تُفصحين له، ولا سيما أفراد الأسرة.** قبل الإفصاح لأفراد الأسرة، قَيِّمي ما إذا كانوا على الأرجح سيقدمون الدعم، وما إذا كانت تربطهم علاقات قائمة بالمعتدي، وما إذا كانوا قد يمارسون ضغطاً للمصالحة. أفصحوا فقط لأفراد الأسرة الذين تتيقنين من أنهم آمنون وقادرون على دعمك دون إشراك المعتدي.
- **تواصلوا أولاً مع منظمة كفى أو منظمة أبعاد،** فكلتا المنظميتين تستطيعان تقديم الدعم والمشورة بشأن الخطوات التالية. راجعوا إلى القسم 9.4 قائمة الموارد.
- **افتراضوا أن المعتدي يعرف روتينك اليومي بالتفصيل.** قد لا تكون التغييرات البسيطة في الروتين كافية. فُكِّروا في: تجنّب الأماكن التي يعلم المعتدي أنك تتردد فيها؛ وعدم الإعلان عن أماكن وجودك علناً حتى لمن تثقين بهم، إلى أن تقيّمي من في دائرتك المقربة قد يكون على تواصل مع المعتدي.
- **لا تتوجهوا إلى المؤسسات الحكومية الرسمية دون استشارة منظمة كفى ومنظمة أبعاد أولاً** لتقييم ما إذا كان الإبلاغ الرسمي آمناً. إذ كثيراً ما لا توفر الاستجابات المؤسسية الحماية الكافية للشخص المستهدف، وقد تستغرق وقتاً طويلاً للاستجابة.
- **قيّدوا من في شبكتك يعلم بالوضع.** في سياقات العنف العشري، يمكن أن تصل المعلومات المتداولة داخل المجتمع إلى المعتدي عبر الدوائر الاجتماعية المشتركة أو جهات الاتصال المتبادلة أو أشخاص حسبي النية لا يدركون حجم الخطر. قد لا تشمل شبكة الدعم الخاصة بكم في هذا السياق العائلة والأصدقاء، بل قد تقتصر على منظمات قادرة على تقديم الدعم وتقليل المخاطر.

4.3 حالات منخفضة ومتوسطة وعالية الخطورة

يبين هذا القسم على أداة تحليل المخاطر، ويشرح معنى كل مستوى من مستويات الخطورة عملياً، ونوع الاستجابة التي يتطلبها. يجب التعامل مع مستويات الخطورة كإرشادات لاتخاذ التدابير، وليس كتصنيفات ثابتة. يمكن أن تتغير الأوضاع بسرعة، لذلك ينبغي إعادة التقييم بشكل مستمر مع تطور الظروف.

● خطورة منخفضة — تعرض محدود، وخطورة طفيفة، ولا تهديد فوري.

عادةً ما تتضمن حالات الخطورة المنخفضة حوادث معزولة ذات انتشار محدود، ودون مؤشرات على التصعيد أو امتداد الأذى خارج الفضاءات الإلكترونية. وقد تشمل هذه الحالات حوادث مضايقة فردية، أو محتوى منخفض التفاعل، أو تفاعلات محصورة في الرسائل الخاصة أو ضمن مجموعات صغيرة. ولا يكون هناك كشف لمعلومات شخصية حساسة، أو استهداف منسّق، أو تهديد مباشر أو ضمني.

في الممارسات العملية: يمكن مراقبة الوضع، ولكن لا ينبغي تجاهله، إذ قد تتصاعد الحوادث منخفضة الخطورة إذا لم يتم التعامل معها.

التدابير الموصى بها

- **اقطعوا التواصل مع المعتدي (إن وُجد)** وتجنّبوا التفاعل مع المحتوى المسيء. واحجبوا المعتدي على جميع المنصات التي يمكن استخدامها للتواصل المحتمل (مثل: جي ميل، وإنستغرام، وفيسبوك، وإكس، وتيك توك، وتيليجرام، وواتساب). *يساعد ذلك الناجية على استعادة شعور الأمان ومنع استمرار الإساءة.*
- **وثّقوا كل شيء لحفظ الأدلة،** ويشمل ذلك أي محتوى يدل على العنف أو الإساءة أو الاستغلال: لقطات شاشة، رسائل بريد إلكتروني، رسائل نصية، أو صور مستلمة. *يساعد ذلك في توثيق التجربة، ويدعم إمكانية اللجوء إلى مسارات قانونية أو تقديم بلاغات.*
- **استخدموا أدوات المنصات للتقييد أو الإبلاغ عن الحوادث.** على فيسبوك وإنستغرام وتيليجرام وواتساب وتيك توك يمكن الإبلاغ عن أي مستخدم أو محتوى [راجعوا القسم 8. إرشادات الإبلاغ عبر المنصات]. *يساعد ذلك على الحدّ من التفاعل والتواصل المحتمل مع المعتدي.*
- **راجعوا إعدادات أمان حسابك الأساسية وعدّلوها** من خلال التحقق من: من يمكنه رؤية منشوراتكم ومعلوماتكم الشخصية، ومن يمكنه التواصل معكم أو مراسلتكم، وأذونات وضع العلامات والتعليقات، وتفعيل المصادقة الثنائية إن لم تكن مُفعّلة بعد. *يساهم ذلك في حماية المعلومات الحساسة، وتقليل مخاطر اختراق الحساب، أو انتحال الهوية، أو الوصول غير المصرح به.*
- **اطلبوا المساعدة،** لأن العزلة كثيراً ما تُفاقم العنف الرقمي. ومن المهم كسر هذه الحلقة والتحدث إلى شخص موثوق: صديق أو فرد من الأسرة أو متخصص. ^[9] *يساهم ذلك في بناء نظام دعم يخفف شعور الناجية بالعزلة ويقلل من الأثر النفسي للإساءة.*

ملاحظة خاصة بالمدافعين/ات من مجتمع الميم-عين: حتى في الحالات منخفضة الخطورة التي تتضمن شائعات أو تلميحات أو محتوى مرتبط بالهوية، ينبغي تقييم الوضع مع منظمات متخصصة قبل تحديد مسار الاستجابة، نظراً للمخاطر القانونية والاجتماعية الخاصة بهذا السياق [راجعوا 9.4 قائمة الموارد].

• متوسط الخطورة — حضور علني متصاعد، واستمرارية، ومؤشرات مبكرة على التصاعد.

تنطوي الحالات متوسطة الخطورة على هجمات مستدامة أو متوسعة قد تشمل مضايقات متكررة أو هجمات منشقة ناشئة أو انتحالا للهوية أو كشفاً جزئياً للبيانات الشخصية. وفي هذه المرحلة، يكتسب المحتوى حضوراً علنياً أوسع ويتنشر عبر المنصات ويستقطب التفاعل. وقد لا تكون التهديدات بالغة الخطورة أو فورية بعد، غير أن الوضع يُظهر مؤشرات على التطور والتصاعد.

في الممارسة العملية: يستوجب الوضع استجابةً فغالة ومراقبةً واحتواءً دون تأخير، إذ يمكن أن يؤدي الانتظار إلى تعزيز التعرض للخطر وتقليص السيطرة على الوضع.

التدابير الموصى باتخاذها: (إضافةً إلى التدابير المذكورة في قسم الخطورة المنخفضة)

- **وتّقوا أنماط الإساءة بصورة منهجية** (لا الحوادث الفردية فحسب) مع الاحتفاظ بسجل بما يجري بمرور الوقت. احتفظوا بملفات شاشة للرسائل والمنشورات، وأسماء المستخدمين لجميع الحسابات المعنية، وروابط URL، والتواريخ والأوقات. يساعد ذلك على إثبات أنماط الاستهداف ومراقبة مخاطر التصاعد وضمان الحفاظ على الأدلة في حال قررت الناجيات طلب المساعدة القانونية.
- **راقبوا أنماط التشابه** في الرسائل والتوقيات والحسابات التي تتصرف بشكل منشق. يساعد ذلك في تحديد ما إذا كان الوضع يتحول نحو التحرش المنشق.
- **تجنبوا الإجراءات التي قد تُضخم الأذى دون قصد** وشجّعوا شبكتكم على فعل الشيء ذاته. وتشمل هذه الإجراءات: إعادة مشاركة المحتوى العدائي، والتفاعل المباشر مع المنشورات أو الحسابات المسيئة، أو لفت الانتباه إلى الملفات الشخصية أو الوسوم الضارة. يُقلّص ذلك خطر زيادة الحضور العلني وتوسيع نطاق الحملات المنشقة أو تكثيف تأثيرها.
- **قلّصوا التعرض العلني** من خلال مراجعة المنشورات وخيارات الظهور ووضع العلامات للحدّ من حجم المعلومات الشخصية والتعريفية المتاحة على الإنترنت. راجعوا المنشورات الأخيرة وعدّلوا إعدادات الجمهور وقبّدوا من يمكنه وضع علامة عليكم أو التعليق. يُقلّص ذلك المعلومات المتاحة على الإنترنت التي يمكن توظيفها في الاستهداف المستقبلي.
- **إبلغوا الأشخاص والشبكات الموثوقة** لتلقّي الدعم وتقليص العزلة والسماح للآخرين بالمساعدة في مراقبة الوضع والاستجابة له. يُرسي ذلك شبكة دعم مع تصاعد الوضع ويتيح للآخرين مراقبة الأدلة وتوثيقها دون تعريض الناجية للمحتوى المسيء.
- **إبلغوا جمهوركم أو شبكتكم بأي حسابات وهمية** تنتحل هوية الناجيات بهدف تجريدن من مصداقيتهن والحدّ من الأضرار التي تلحق بسمعتن. يُقلّص ذلك من فعالية انتحال الهوية وانتشار التضليل الإعلامي.

• عالي الخطورة — تهديدات جسيمة، وتعرض للكشف، وتنسيق، أو احتمال وقوع أذى.

تنطوي الحالات عالية الخطورة على مؤشرات خطر بالغة الأثر، تشمل نشر البيانات الشخصية دون إذن، والتهديدات، وحملات التحرش المنشق واسعة الانتشار، والتهديد بالكشف عن الميول الجنسية، أو الصور الحميمة المنشورة دون موافقة ومحتوى التزييف العميق. ويتسم هذا المستوى من الحدة بالتصاعد السريع والانتشار الواسع والاستهداف الذي يتجاوز الفرد ليطال الأسرة والأصدقاء والزملاء، مع تداعيات تمتد خارج المجال الرقمي.

في الممارسة العملية: يجب أن تكون الاستجابة فورية، وتُعدّ السلامة الرقمية والجسدية أولوية قصوى.

التدابير الموصى باتخاذها: (إضافةً إلى التدابير المذكورة سابقاً)

- **أولوا السلامة الشخصية الأولوية وقلّصوا التعرض للخطر:** تجنّبوا النشر الآني (ولا سيما المنشورات التي تتضمن الموقع الجغرافي)، وأوقفوا مشاركة الموقع على جميع المنصات، وتجنّبوا التفاعل مع المعتدين، يساعد ذلك على تقليص الهشاشة الفورية والحدّ من فرص الاستهداف المستقبلي.
- **أبلغوا الجهات المختصة** (حيثما كان ذلك آمناً ومناسباً) أو المنظمات القادرة على تقديم الدعم. قيّموا ما إذا كان الإبلاغ الرسمي خياراً آمناً وقابلًا للتطبيق للحصول على الدعم القانوني والأمني وضمان الحماية من التهديدات والأذى خارج المجال الرقمي. يُسهم ذلك في السعي نحو العدالة والمساءلة مع ضمان السلامة الجسدية للناجيات.
- **فكّروا في تغيير رقم الهاتف** في حالات التعرض الشديد وحين تتلقّى الناجيات مضايقات مستمرة أو مكالمات ورسائل وتهديدات متكررة. إذ قد يساعد تغيير رقم الهاتف على استعادة السيطرة والحدّ من الأذى الفوري. وقبل القيام بذلك، أبلغوا جهات الاتصال الموثوقة وأقنوا الوصول إلى الحسابات الأساسية المرتبطة بالرقم القديم. يساعد ذلك على وقف الاستهداف المستمر ومنع التواصل المباشر المستقبلي.

إذا كنتم غير متأكدين من مستوى الخطورة، فمن الأكثر أماناً التعامل مع الوضع على أنه **عالي الخطورة** والانتقال إلى إجراءات الحماية.

علامات الخطر الفوري

4.4

- تشير بعض المؤشرات إلى أن الوضع قد يتصاعد بسرعة أو أنه تجاوز بالفعل نطاق الأذى الرقمي ليصبح خطراً أمنياً فورياً. عند وجود واحدة أو أكثر من هذه العلامات، يجب التعامل مع الحالة على أنها ذات خطورة عالية وعاجلة، وتتطلب اتخاذ إجراءات حماية ودعم فورية.
- **تهديدات مباشرة بإيذاء جسدي أو عنف** بما في ذلك التهديدات الصريحة بالاعتداء أو القتل أو العنف الجنسي ضد الناجيات أو غيرهنّ، سواء أرسلت بشكل خاص أو علني.
← أوقفوا التفاعل، واحفظوا الأدلة، وأبلغوا شخصاً موثقاً أو شبكة دعم موثوقة فوراً.
 - **امتداد المضايقات والتهديدات إلى أفراد العائلة أو الزملاء أو الأصدقاء** بما في ذلك محاولات التواصل مع الأشخاص في الحياة الشخصية أو المهنية للناجية أو كشف بياناتهم.
← أبلغوا الأشخاص المتضررين والمستهدفين ونشّقوا معهم للتوصل إلى استجابة مشتركة.
 - **نشر البيانات الشخصية دون إذن ومشاركة معلومات حساسة** مثل عنوان المنزل أو رقم الهاتف أو مكان العمل أو الموقع الجغرافي المباشر، بما يتيح للآخرين تحديد موقع الناجيات أو التواصل معهنّ.
← نّبّهوا جهات الاتصال المقربة واتخذوا الخطوات اللازمة لضمان السلامة الجسدية، سواء بالتواصل مع الجهات المختصة أو الانتقال المؤقت إلى مكان آمن.
 - **التعقّب والتتبع خارج الإنترنت والمراقبة أو الاقتراب المباشر** نتيجة نشر البيانات الشخصية دون إذن.
← تجنّبوا الروتين اليومي المتوقع، وتأكدوا قدر الإمكان من عدم بقاء الناجية وحيدة، وأبلغوا شخصاً موثقاً بالموقف.
 - **التهديدات أو نشر الصور الحميمة دون موافقة أو التزييف العميق.**
← لا تحذفوا المحتوى بأنفسكم قبل توثيقه [راجعوا 12.4 قائمة التحقق للتوثيق]، ولا تتفاعلوا مع المعتدي ولا تردّوا على التهديدات، وتواصلوا فوراً مع شخص موثوق أو منظمات الدعم [كفى/أبعاد — راجعوا 9.4 قائمة الموارد]. واستخدموا أدوات الإزالة الخاصة بالمنصات [راجعوا 8.4 الإبلاغ عن الصور الحميمة دون موافقة ومحتوى التزييف العميق].

مصفوفة التقييم السريع للمخاطر

قِيمُوا كل مؤشر استناداً إلى وضعكم الحالي، ثم اجمعوا النقاط الإجمالية وارجعوا إلى جدول تفسير النتائج أدناه. يُمنح 0 للحالات منخفضة الخطورة، و1 للحالات متوسطة الخطورة، و2 للحالات عالية الخطورة؛ بعد جمع النقاط، استخدموا جدول تفسير النتائج لتحديد مستوى المخاطر الذي تنتمي إليه الحالة.

مؤشر المخاطر	منخفض (0)	متوسط (1)	مرتفع (2)
نوع الهجوم	حادثة واحدة، مضايقة محدودة المستوى	مضايقات متكررة، أو انتحال هوية، أو هجمات متداخلة	تعدد أنواع الهجمات في الوقت نفسه مع مؤشرات على وجود تنسيق بينها
الظهور / الانتشار	جمهور محدود أو خاص	ظهور علني أو متزايد	انتشار واسع، وعبر منصات متعددة، مع إعادة نشر سريعة
نشر البيانات الشخصية دون إذن والكشف عن المعلومات الشخصية	عدم مشاركة أي بيانات شخصية	كشف جزئي أو غير مباشر للمعلومات	مشاركة بيانات حساسة مثل رقم الهاتف، وعنوان البريد الإلكتروني، وعنوان السكن، وموقع العمل
التنسيق	لا توجد مؤشرات على وجود تنسيق	مؤشرات على تكرار المحتوى وظهور أنماط متشابهة	هجوم منسق بوضوح عبر حسابات متعددة تستخدم الرسائل أو الأساليب نفسها
التهديدات	لا توجد تهديدات	تهديدات ضمنية أو غير مباشرة	تهديدات مباشرة بالعنف أو القتل أو الأذى الجنسي
التصعيد	الوضع مستقر ولا يزداد سوءاً	تزايد في وتيرة الهجوم وحدته	تصعيد سريع أو ارتفاع مفاجئ في الهجمات
التأثير على الآخرين	الاستهداف يقتصر على الناجية	ذكر أشخاص آخرين	استهداف أفراد العائلة أو الزملاء أو جهات الاتصال
المخاطر خارج الإنترنت	لا توجد تداعيات خارج الفضاء الرقمي	إشارات أو تلميحات غير مباشرة	مؤشرات واضحة على التتبع أو التواصل المباشر أو القرب الجسدي من الناجية
مصدر الهجوم	فرد معزول أو غير معروف	حسابات متعددة ومشبوهة	جهات فاعلة منظمة، أو شبكات أو مجموعات يمكن تحديدها بشكل محتمل
هل يتورط في الهجوم شريك حالي أو سابق أو شبكته؟	كلا	كلا	نعم
جرى تداول صور حميمة دون موافقة ومحتوى تزييف عميق	كلا	كلا	نعم
المجموع الكلي	20 / _____		

نطاق النقاط	مستوى الخطورة	ما يعنيه ذلك عملياً
6 – 0	منخفض الخطورة	تعرض محدود، لا يوجد تهديد فوري. راقبوا واطبقوا إجراءات الحماية الأساسية.
12 – 7	متوسط الخطورة	الوضع في تصاعد. استجيبوا واحتووه لمنع مزيد من التصعيد.
20 – 13	عالي الخطورة	خطر جدي من ضرر رقمي أو جسدي. يتطلب إجراءات حماية ودعم فورية.

فيما يتعلق بالتهديدات، أو نشر البيانات الشخصية دون إذن، أو المخاطر خارج الإنترنت، أو الصور الحميمة المنشورة دون موافقة، أو عنف العشير، تعاملوا دائماً مع الحالة على أنها **عالية الخطورة بغض النظر عن إجمالي التقييم**. وفي حال عدم التأكد من كفاءة تقييم الوضع، فاعتبروها عالية الخطورة وانتقلوا إلى إجراء وقائي.

مسار الاستجابة خلال أول 24 إلى 72 ساعة

خلال الانتخابات وفترات التوترات السياسية، يمكن أن تتصاعد الهجمات الرقمية بسرعة وتكتسب حضوراً علنياً واسعاً، إذ تهدف إلى تعطيل المشاركة العامة والضغط على الأفراد لإجبارهم على الصمت أو الانسحاب من الحياة العامة. وكثيراً ما تكون الـ 24 إلى 72 ساعة الأولى التي تعقب أي حادثة بالغة الأهمية في الحدّ من التصاعد والحفاظ على الأدلة وتقليل التعرض للخطر وحماية السلامة الرقمية والجسدية. ويقدم هذا القسم إجراءات استجابة فورية يمكن أن تساعد المستخدمين على تثبيت الوضع واتخاذ قرارات مستنيرة وتحديد الخطوات التالية المناسبة، مع مواصلة المشاركة العامة والسياسية بأكثر قدر ممكن من الأمان.

IMPORTANT ▲

ملاحظة مهمة: تنطبق الإرشادات الواردة في هذا القسم على جميع مستخدمي هذا الدليل. غير أن التطبيق المناسب لخطوات بعينها، ولا سيما تلك المتعلقة بالاستجابة العلنية والإبلاغ الرسمي والدعم الموثوق والتصعيد، يتفاوت بحسب السياق. إذ تواجه المرشحات والمدافعات عن حقوق الإنسان ومدافعو ومدافعات مجتمع الميم-عين مشهديات مخاطر مختلفة تُحدد المسارات الآمنة والفعّالة لكل فئة. وحيثما تستلزم توصية ما تكييفاً لجمهور بعينه، يُشار إلى ذلك مباشرة.

تثبيت الوضع

5.1

- كثيراً ما تُصمّم الهجمات الرقمية خلال الحملات السياسية لاستثارة الخوف والإلحاح والارتباك والإضرار بالسمعة بهدف النيل من مصداقية المرشحين والناشطين والصحفيين. وقد تؤدي ردود الفعل الفورية الصادرة تحت الضغط إلى زيادة التعرض للخطر وتضخيم المحتوى الضار دون قصد. لذا فإن الخطوة الأولى هي إبطاء التصاعد وتقييم الوضع بوضوح لاستعادة السيطرة قبل اتخاذ قرار بشأن الخطوات التالية.
- **التوقف** قبل الرد علناً أو خصوصياً على الهجوم. تجنّبوا التفاعل مع المحتوى أو التواصل المباشر مع المعتدين أو محاولة الدفاع عن النفس فوراً في حالة الضيق.
- **إجراء تقييم فوري للمخاطر** باستخدام أداة التعرف السريع على المخاطر وتصنيف درجة خطورتها لتحديد مستوى خطورة الحادثة ونوع الاستجابة المطلوبة.
- **تحديد الشكل الرئيسي للهجوم** وما إذا كانت تكتيكات متعددة تُوظف في آن واحد، وتحديد ما إذا كان الهجوم معزولاً أم منسقاً.
- **عدم حذف الحسابات أو الرسائل أو الأدلة فوراً** ما لم تكن ثمة مخاوف أمنية عاجلة. احتفظوا بالمحتوى للمساعدة في الحفاظ على المعلومات والأدلة المهمة التي يمكن أن تدعم لاحقاً الإبلاغ أو الإجراءات القانونية أو الدعم المؤسسي أو التقييم الأمني.
- **الابتعاد مؤقتاً عن متابعة المحتوى المسيء** وطلب المساعدة من شخص موثوق لمراجعة الرسائل والتعليقات والمنشورات وجمع الأدلة. يساعد ذلك على تقليل الضغط النفسي والحدّ من التعرض المتكرر للمحتوى الضار.
- **في حال وجود مؤشرات على مخاطر خارج المجال الرقمي** وتهديدات تشير إلى الموقع الجغرافي أو التنقلات أو أفراد الأسرة أو مكان العمل أو محاولات إقامة تواصل مباشر، فأولوا السلامة الجسدية الأولوية:
- تجنّبوا مشاركة منشورات أو قصص أو محتوى يكشف عن الموقع الجغرافي الآتي.
- غيّرُوا الروتين اليومي وأنماط التنقل مؤقتاً حيثما أمكن. تجنّبوا الجداول الزمنية المتوقعة والروتين المتكرر. لا تعلنوا علناً عن الحضور في الاجتماعات أو الفعاليات أو الاحتجاجات أو أنشطة الحملات الانتخابية.
- لا تحضروا الاجتماعات الشخصية بمفردكم وأبلغوا شخصاً موثقاً بالمخاطر. وأبلغوا الجهات المختصة إن كان ذلك مناسباً.

الحفاظ على الأدلة

5.2

كثيراً ما يُحذف المحتوى العنيف رقمياً بسرعة أو يُنقل عبر منصات متعددة ومجموعات مغلقة. وكثيراً ما تعتمد الحملات المنسقة على حسابات مؤقتة وإعادة نشر جماعية وملفات شخصية مجهولة الهوية أو محتوى زائل. لذا يُعدّ الحفاظ على الأدلة مبكراً أمراً بالغ الأهمية لتوثيق أنماط الإساءة وتقييم التصاعد ودعم عمليات الإبلاغ والحصول على الدعم المؤسسي أو القانوني أو النفسي الاجتماعي أو الأمني حيثما كان متاحاً أو ضرورياً.

عند توثيق الحوادث، ينبغي التقاط المحتوى المسيء والسياق الأشمل المحيط به معاً. إذ كثيراً ما تبدو الحوادث الفردية طفيفة حين تُؤخذ بمعزل عن غيرها، غير أن أنماط التكرار والتنسيق والحضور العلني تتضح أكثر بمرور الوقت.

راجعوا القسم 12.4 قائمة التحقق للتوثيق لمعرفة ما ينبغي توثيقه.

تقليص التعرض الفوري

5.3

يزيد الحضور السياسي والمدني من الهشاشة خلال الهجمات الرقمية المنسقة. غير أن تقليص التعرض لا يعني بالضرورة الانسحاب من المشاركة، بل يعني الحدّ من فرص الاستهداف المستقبلي وحماية الحسابات في حين يجري تقييم الوضع وتثبيته. وفيما يلي الإجراءات الإلزامية الواجب اتخاذها فور التعرف على العنف الرقمي والمضايقات والاستهداف.

1. تأمين الحسابات وقنوات التواصل

- **تغيير كلمات المرور فوراً لجميع الحسابات المهمة:** إنشاء كلمات مرور جديدة وطويلة وفريدة لكل حساب، وتجنّب إعادة استخدام كلمات المرور ذاتها عبر المنصات المختلفة:
 - حسابات البريد الإلكتروني
 - حسابات وسائل التواصل الاجتماعي (فيسبوك، وإنستغرام، وواتساب، وإكس، وتيك توك)
 - الحسابات المصرفية
- **تفعيل المصادقة الثنائية (2FA)** على جميع الحسابات الرئيسية ومنصات التواصل لجعل الوصول غير المصرح به أمراً بالغ الصعوبة في حال تعرّض كلمات المرور للاختراق.
- **تأمين حسابات البريد الإلكتروني،** ولا سيما عناوين البريد الإلكتروني المرتبطة باسترداد كلمة المرور أو التحقق من الحساب: تأكدوا من وجود كلمة مرور فريدة عالية الأمان، وحدّثوا خيارات الاسترداد.
- **مراجعة الجلسات النشطة وتسجيل الخروج عن بُعد من المتصفحات والأجهزة:** استخدموا قسم «إعدادات الأمان» أو «الجلسات النشطة» على منصات مثل Google و Facebook و Apple لتسجيل الخروج من جميع الأجهزة وجلسات المتصفح.

2. تأمين الأجهزة وإعدادات الخصوصية

● مراجعة إعدادات الخصوصية والظهور عبر جميع المنصات والتطبيقات، تقييد:

- من يمكنه التواصل معكم،
- من يمكنه إرسال رسائل مباشرة،
- من يمكنه وضع علامة على الحساب أو الإشارة إليه،
- من يمكنه مشاهدة القصص والمنشورات،
- من يمكنه الوصول إلى المعلومات الشخصية.

- **تعطيل مشاركة الموقع الجغرافي الآني** ومراجعة أذونات الموقع على الأجهزة والتطبيقات. أوقفوا مشاركة GPS حيثما لم تكن ضرورية وراجعوا التطبيقات التي تملك صلاحية الوصول إلى الموقع والكاميرا والميكروفون وجهات الاتصال والملفات.
- **تعطيل خاصية تحديد الموقع الجغرافي** في تطبيقات الكاميرا ومنصات التواصل الاجتماعي لتفادي الكشف عن معلومات الموقع.
- **تحديث أنظمة التشغيل والتطبيقات وبرامج الأمان** إلى أحدث الإصدارات المتاحة لضمان الحماية من الثغرات الأمنية.
- **مراجعة الحسابات المشتركة والأجهزة المرتبطة والخدمات المتصلة.** ألغوا الوصول غير الضروري إلى التخزين السحابي المشترك وحسابات البث (إن كانت مرتبطة بحساب غوغل) والتقاويم المشتركة ومزامنة الأجهزة أو أنظمة المشاركة العائلية.
- **تجنّب ربط التطبيقات** عبر أدوات تسجيل الدخول بوسائل التواصل الاجتماعي كـ«تسجيل الدخول عبر Facebook»، للحدّ من انتشار الاختراق بين المنصات.
- **استخدام منصات تواصل آمنة ومشفّرة من طرف إلى طرف** (مثل «سيغنال»).
- **حذف بيانات EXIF من الصور:** بيانات EXIF (تنسيق ملف الصور القابل للتبادل) هي بيانات وصفية تُضخّن تلقائياً في الصور ومقاطع الفيديو من قبل جهازك عند التقاطها. وقد تحتوي على: إحداثيات GPS لمكان التقاط الصورة، وتاريخ ووقت الالتقاط، وطرز الجهاز وموديله، وإعدادات الكاميرا.

● كيفية حذفها:

- **على iPhone:** يتيح نظام iOS 13 وما فوق حذف بيانات الموقع عند المشاركة. اذهبوا إلى الصور ← اختاروا الصورة ← مشاركة ← اضغطوا على علامة الموقع في الأعلى ← اختاروا «عدم التضمين» قبل الإرسال. ولحذف بيانات EXIF بالكامل، استخدموا تطبيقاً مثل Metapho أو Photo Investigator.
- **على Android:** اذهبوا إلى معرض الصور ← اختاروا الصورة ← التفاصيل ← تعديل (أيقونة القلم) ← احذفوا معلومات الموقع. أو استخدموا تطبيقاً مثل Photo Exif Editor أو Exif Eraser.
- **على الحاسوب:**
 - **Windows:** انقروا بزر الفأرة الأيمن على الملف ← خصائص ← تبويب التفاصيل ← «إزالة الخصائص والمعلومات الشخصية» ← تحديد الكل ← موافق.
 - **Mac:** استخدموا Preview أو أداة مجانية مثل ImageOption التي تحذف البيانات الوصفية تلقائياً.

تحديد شبكة الدعم الموثوقة

5.4

IMPORTANT ▲

يستخدم هذا القسم عبارة «جهات الاتصال الموثوقة» بصورة مقصودة. إذ يدرك هذا الدليل أنه بالنسبة لكثير من المدافعات عن حقوق الإنسان، ولا سيما ناشطي ومدافعي مجتمع الميم-عين في لبنان، قد تكون الأسرة ذاتها جزءاً من الخطر — فالكشف عن الهوية أمام أفراد الأسرة والعنف القائم على الشرف وإجبار الأسرة على الانسحاب من الحياة العامة، كلها أضرار حقيقية تعقب كثيراً من الهجمات الرقمية. إذا كانت أسرته جزءاً من الخطر، استبدلوا كل إشارة إلى «الأسرة» أدناه بـ«جهات الاتصال الموثوقة المختارة». وأولوا منظمات مجتمع الميم-عين («حلم» و«موزاييك»)، ومجموعات حقوق المرأة (منظمة أبعاد، ومنظمة كفى) الأولوية على الإفصاح للأسرة حيثما كان الكشف عن الهوية أو ردود الفعل القائمة على الشرف احتمالاً وارداً. راجعوا 9.4 قائمة الموارد.

إن التعرف المبكر على شبكة الدعم الموثوقة يُقلّص حتماً تأثير العنف الرقمي على العزلة والصحة النفسية. إذ يمكن لشبكات الدعم المساعدة في التوثيق وتخفيف الضغط العاطفي وتعزيز اتخاذ القرار وتحسين التخطيط للسلامة. ولا يشترط أن يكون الدعم رسمياً بالضرورة، فحتى شخص واحد موثوق يمكنه المساعدة في تثبيت الوضع وتقليل الضغط. ومن المهم تحديد شبكة الدعم في أقرب وقت ممكن بدلاً من انتظار تصاعد الوضع.

يمكن أن تتألف شبكة الدعم الموثوقة من

- أصدقاء وأفراد أسرة يمكنهم المساعدة في مراقبة الرسائل وتوثيق الإساءة وتقديم الدعم العاطفي.
- زملاء وفرق الحملات وموظفون موثوقون في المنظمات يمكنهم المساعدة في التواصل والإبلاغ والتنسيق لوضع خطط الاستجابة.
- منظمات السلامة الرقمية والأمن السيرانّي التي يمكنها دعم أمان الحسابات وتقييم المخاطر.
- منظمات المساعدة القانونية وحقوق الإنسان عند حدوث التهديدات القانونية أو نشر البيانات الشخصية دون إذن أو التشهير.
- مقدمو الدعم النفسي الاجتماعي وخدمات الصحة النفسية الذين يمكنهم تقديم المساعدة في حال تسببت الهجمات في ضيق أو قلق أو خوف أو إرهاق.
- منظمات مجتمع الميم-عين ومجموعات حقوق المرأة التي تفهم المخاطر المحددة المرتبطة بالكشف عن الهوية والإساءة الجندرية والمضايقات الموجهة.
- صحفيون موثوقون ومشرّفون وجهات اتصال في المنصات حيثما يكون التوضيح العلني أو الإبلاغ العاجل ضرورياً.

يمكن لشبكة الدعم الموثوقة المساعدة في

- توثيق الأدلة وتنظيمها.
- مراقبة المحتوى المسيء حتى لا يتعرض الشخص المستهدف باستمرار للمواد الضارة.
- المساعدة في الإبلاغ عن الحسابات المسيئة أو انتحال الهوية.
- المساهمة في تقييم المخاطر والتصعيد.
- دعم القرارات المتعلقة بالردود العلنية وبيانات التوضيح، لضمان أن يكون التفاعل موضوعياً لا انفعالياً مع الاستعانة برأي طرف ثالث محايد.
- المساعدة في تنسيق تدابير السلامة ومرافقة الناجيات في الأماكن العامة في حال وجود مخاطر خارج المجال الرقمي.
- مرافقة الشخص المستهدف عند طلب المساعدة القانونية أو الدعم المؤسسي أو المنظمات.

اعتبارات مهمة عند تأسيس شبكة الدعم

- التحقق من أن الشخص أو المنظمة يمكن الوثوق بهم للحفاظ على السرية.
- تجنّب مشاركة المعلومات الحساسة على نطاق واسع أو علنياً.
- استخدام قنوات تواصل آمنة ومشفّرة من طرف إلى طرف لتنسيق الاستجابة.
- توجّي الحذر عند إعادة توجيه لقطات الشاشة أو الأدلة التي تحتوي على معلومات شخصية.
- إيلاء الأولوية للأشخاص والمنظمات الذين يفهمون الأبعاد السياسية والجندرية ومتعلقات مجتمع الميم-عين في الهجمات الرقمية في لبنان.

لا يُفترض بالمرشحات والناشطين التعامل مع العنف الرقمي خلال الفترات السياسية الحساسة بمفردهم كلياً. إذ يمكن للدعم المنسق أن يُساعد على تقليص الأذى وتحسين السلامة وتعزيز القدرة على الاستجابة بفعالية وروية، كما يسهم في الحفاظ على المشاركة السياسية الآمنة دون زيادة التعرض للخطر أو العزلة.

تحديد مسار الاستجابة التالي

5.5

الخطوة التالية بعد التثبيت الفوري هي تحديد كيفية الاستجابة في المرحلة القادمة. لا تتطلب جميع الحالات نفس أسلوب الاستجابة. لذا ينبغي في البيئات السياسية الحساسة أن تُولي قرارات الاستجابة الأولوية للسلامة والاستدامة واتخاذ القرارات المستنيرة. ويستعرض هذا القسم مسارات الاستجابة المحتملة التي يمكن توظيفها بصورة منفردة أو مجتمعة بحسب الوضع.

مواصلة المراقبة دون التفاعل العلني

قد يكون هذا المسار مناسباً في الحالات منخفضة الخطورة حيث يكون للهجوم حضور علني محدود، ولا تهديدات مباشرة، والمحتوى لا ينتشر بسرعة، ولا مؤشرات على التصاعد. تتضمن الاستجابة:

- مواصلة توثيق الأدلة ومراقبة الوضع بمساعدة شبكات الدعم.
- حجب الحسابات المسيئة وتقييدها.
- الإبلاغ عن المحتوى الضار عبر المنصات حيثما كان ذلك مناسباً.
- تجنّب التفاعل المباشر مع المعتدين.
- إعادة تقييم المخاطر بصورة منتظمة للكشف عن مؤشرات التصاعد.

التصعيد نحو الدعم المؤسسي أو القانوني أو الأمني

قد يكون التصعيد مفيداً في الحالات متوسطة إلى عالية الخطورة، ولا سيما في حالات التهديدات المباشرة ونشر البيانات الشخصية دون إذن والكشف عن الهوية والتحرّش المنشقّ المستدام التي تستهدف أفراد الأسرة والزملء ومحاولات الوصول إلى الحسابات.

- إبلاغ أصحاب العمل والمنظمات وفرق الحملات الانتخابية وأفراد الأسرة.
- طلب دعم الأمن الرقمي.
- التواصل مع منظمات المساعدة القانونية أو حقوق الإنسان.
- الإبلاغ عن التهديدات للجهات الحكومية كوحدة جرائم الأمن السيبراني في قوى الأمن الداخلي ينطوي على مخاطر حقيقية في لبنان، ولا ينبغي القيام به دون استشارة مسبقة مع منظمة مستقلة من منظمات المجتمع المدني (انظروا القسم 9.4 قائمة الموارد).
- طلب دعم طارئٍ للتخطيط للسلامة.

IMPORTANT ▲

ملاحظة مهمة — لمستخدمي مجتمع الميم-عين: لا تتواصلوا مع قوى الأمن الداخلي قبل استشارة «حلم» أو «موزاييك» أو Legal Agenda. فقد جرى توظيف المادة 534 من قانون العقوبات اللبناني لاحتجاز أفراد من مجتمع الميم-عين استناداً إلى أدلة رقمية سُوركت بحسن نية خلال مثل هذه الشكاوى. انظروا القسم 9.2 اعتبارات السلامة المهمة قبل طلب المساعدة للاطلاع على التحذير الكامل بشأن المؤسسات الحكومية، فالإبلاغ للجهات الحكومية ينطوي على مخاطر حقيقية في لبنان. استشيروا منظمة مستقلة من منظمات المجتمع المدني (انظروا 9.4 قائمة الموارد) قبل التوجه إلى قوى الأمن الداخلي.

التوضيح العلني والاستجابة

IMPORTANT ▲

قبل نشر أي توضيح يُسمّى فيه فرداً أو منظمة أو حزباً سياسياً، استشيروا مستشاراً قانونياً — إذ تُعدّ منظمة Legal Agenda أو المركز اللبناني لحقوق الإنسان جهتي الاتصال الأولى المناسبين. فقد جرى توظيف أحكام التشهير في لبنان (المادة 582 من قانون العقوبات والمرسوم الاشتراعي 2007/22 المتعلق بالإعلام المرئي والمسموع) بصورة اعتيادية لملاحقة الناجيات اللواتي يرددن علناً على معتديهم. إذ يمكن أن يُفسي بيان مضاد يهدف إلى الدفاع عن السمعة في حد ذاته إلى توجيه اتهامات جنائية بالتشهير، ولا سيما خلال الفترات السياسية الحساسة. لذا خظّطوا للاستجابة وتبعاتها القانونية معاً لا بصورة منفصلة، تفادياً لخطر التشهير المضاد.

وفي بعض الحالات، قد يرى الأفراد ضرورة إصدار استجابة علنية محدودة، ولا سيما في الحالات التي تتضمن: انتحال الهوية؛ والتضليل الإعلامي؛ والهجمات على السمعة؛ والادعاءات الكاذبة؛ وحملات التضليل المنسقة.

ويتوقف ما إذا كان التوضيح العلني مناسباً وآمناً وفغلاً بصورة جوهرية على هويتك والسياق الذي تعملين فيه. قبل اتخاذ قرار إصدار استجابة علنية، استخدموا المعيار التالي:

- **إذا كنت مرشحة أو فاعلة مدنية تحظين بدعم حزبي أو مؤسسي:** يُرجّح أن يكون التوضيح العلني الأكثر فعالية في سياقك. إذ تمتلكين دعماً مؤسسياً ومنبراً علنياً راسخاً وشرعية انتخابية تمنح استجابتك مصداقية. ويمكن لمسؤولي الحزب ومديري الحملات أو شركاء التحالف تضخيم توضيحك وإضفاء الثقل المؤسسي عليه (راجعوا الأسئلة الواجب أخذها بعين الاعتبار أدناه).
- **إذا كنت مدافعة عن حقوق الإنسان دون دعم حزبي أو مؤسسي:** توّتي الحذر الشديد قبل إصدار توضيح علني. فبدون دعم مؤسسي، يمكن أن يستقطب الرد العلني مزيداً من الاهتمام نحو الهجوم ويدعو إلى مزيد من التصاعد ويضعك بوصفك هدفاً فردياً دون حماية جماعية. وإن كان الرد العلني ضرورياً فعلاً، أصدره عبر قناة مؤسسية أو جماعية لا عبر حساب شخصي، واجعليه موجزاً وواقعياً، وفغلي شبكات دعمك واطلبي دعماً إضافياً [راجعوا 9.4 قائمة الموارد].
- **إذا كنت مدافعة أو ناشطة من مجتمع الميم-عين:** يحمل التوضيح العلني مخاطر محددة وجسيمة في السياق اللبناني ينبغي تقييمها قبل إصدار أي استجابة. فإذا تضمّن الهجوم الفضح أو إشاعات حول توجهك الجنسي أو هويتك، فقد يستقطب الرد العلني الانتباه نحو الادعاء ويدعو إلى مزيد من الاستهداف وقد يُفاقم المخاطر القانونية في بعض الحالات. لا تُصدري أي بيان علني قبل التواصل مع «حلم» أو Proud أو موزاييك [راجعوا 9.4 قائمة الموارد].

ينبغي دراسة أي استجابة علنية بعناية قبل النشر:

- تجنّبي الردود الانفعالية أو المتسرّعة الصادرة تحت الضغط؛ ابتعدي عن وسائل التواصل الاجتماعي والمحتوى الضار قبل الرد علناً.
- تجنّبي التفاعل المباشر مع المعتدين.
- تجنّبي مشاركة المحتوى الضار أو إعادة نشره.
- ركّزي على تصحيح المعلومات الكاذبة أو إيصال الحقائق الجوهرية.

أسئلة ينبغي مراعاتها: هل سيزيد الرد من الحضور العلني أو يطيل أمد الهجوم؟ هل سيؤدي الرد إلى دعوى تشهير مضادة؟ هل التوضيح ضروري للسلامة أو السمعة أو المسألة العامة؟ هل يمكن أن يظل الرد واقعياً وموجزاً وغير منخرط في الجدل؟ هل ثمة دعم مؤسسي أو موثوق متاح للمساعدة في صياغة الرد أو مراجعته؟ لا تستوجب كل هجمة رداً علنياً. ففي بعض الحالات، قد يكون الصمت والاحتواء والتوثيق أكثر أماناً وفعالية.

إعادة التقييم المستمرة

مسارات الاستجابة ليست ثابتة. إذ يمكن أن تتصاعد الأوضاع أو تستقر بسرعة، ولا سيما خلال الفترات السياسية الحساسة.

- هل لا تزال الهجمات تنتشر؟
- هل أصبحت التهديدات أكثر خطورةً وتكراراً؟
- هل تبرز مخاطر خارج المجال الرقمي، وهل جرى تداول معلومات شخصية؟
- هل ثمة حاجة إلى دعم إضافي أو تصعيد؟

القسم 6

6

خيارات المشاركة الأكثر أماناً

كثيراً ما تزيد فترات التوترات السياسية والانتخابات وتصاعد الحضور العلني من احتمالية الهجمات الرقمية وحدتها. غير أن المشاركة الأكثر أماناً لا تستوجب بالضرورة الانسحاب من الحياة العامة. ففي بعض الحالات، يمكن أن تؤدي تعديلات مؤقتة على مستوى الحضور العلني وعادات التواصل والتفاعل مع المنصات إلى تقليص التعرض للخطر مع إتاحة الاستمرار في المشاركة في الحملات الانتخابية والمناصرة والمشاركة المدنية. لذا ينبغي أن يهدف التخطيط للسلامة لا إلى تقليص الأذى فحسب، بل أيضاً إلى دعم استمرار المشاركة حيثما أمكن ذلك.

تعديل مستوى الحضور العلني دون الانسحاب الكامل

6.1

يستعرض هذا القسم طرقاً عملية للحدّ من التعرض للعنف الرقمي مع دعم استمرار الانخراط في الحياة العامة. وتركّز هذه الطرق على تعديلات مؤقتة على مستوى الحضور العلني وممارسات التواصل واستخدام المنصات، مما قد يُساعد على تقليص الاستهداف والتصاعد والتعرض للأذى دون الانسحاب الكامل.

تعديلات الحضور العلني

- تجنّبوا نشر تحديثات آنية أو بث مباشر أو مواقع جغرافية قابلة للتعرف عليها خلال الفعاليات أو الاجتماعات أو أنشطة الحملات الانتخابية. وشاركوا المحتوى بعد مغادرة الموقع.
- أوقفوا مؤقتاً المنشورات التي تحتوي على معلومات حساسة أو تعريفية أو أرشفوها أو قيّدوا الوصول إليها، بما في ذلك تفاصيل مكان العمل وأرقام الهواتف والروتين الشخصي ومعلومات الأسرة أو الأماكن التي تترددون عليها.
- راجعوا المنشورات القديمة والصور والمحتوى الذي وُضعت عليه علامات وسير المنصات الشخصية التي قد تكشف دون قصد عن تفاصيل أو أنماط تعريفية يمكن توظيفها في نشر البيانات الشخصية دون إذن أو المراقبة أو المضايقات الموجهة.
- انظروا في استخدام قنوات وحسابات تواصل قائمة على الصفحات أو الحملات الانتخابية أو المنظمات خلال فترات التصاعد بدلاً من الاعتماد على الحسابات الشخصية.

ممارسات التواصل

- إيلاء الأولوية للمحتوى المجدول أو المُعدّ مسبقاً خلال فترات التحرش المنسق المستدامة للحدّ من الضغط الناجم عن الحاجة إلى التواجد الدائم على الإنترنت أو الشعور بضرورة الرد على الهجمات.
- الحدّ من التفاعل المباشر مع المحتوى المسيء والوسوم العدائية ودورات الاقتباس والمشاركة أو حملات التحرش المنسق المصمّمة لاستثارة الحضور العلني أو الغضب أو التصاعد.
- تشجيع المؤيدين والزعماء والشبكات الموثوقة على تجنّب تضخيم المحتوى المسيء، بما في ذلك عبر إعادة نشر لقطات الشاشة أو الوسوم العدائية أو الهجمات المنسقة.
- تأسيس دعم إشراف موثوق (باستخدام الشبكات الموثوقة) حتى لا تضطري إلى إدارة التعليقات المسيئة أو الرسائل المباشرة أو عمليات الإبلاغ بمفردك.

استخدام المنصات

- تعطيل التعليقات مؤقتاً وتقييد الردود وتفعيل أدوات الإشراف على المنصات التي تتركز فيها الهجمات.
- تقييد من يمكنه وضع علامة على المحتوى أو الإشارة إليه أو دمج أو مزامته أو إعادة نشره أو تضخيمه بأي طريقة أخرى، حيثما تُوفّر ميزات المنصات سلباً لزيادة التعرض للخطر أو المضايقات.

خيارات المشاركة الفردية والجماعية

6.2

لا يستوجب الظهور العلني والتصريحات والتواصل دائماً نسبتها إلى فرد واحد. فخلال فترات الاستهداف المتصاعد، يمكن أن يُساعد توزيع الظهور عبر هيكل جماعي أو مؤسسي على تقليل تركّز الخطر على شخص واحد مع الحفاظ على تأثير الرسالة أو الحملة. بل إن الصوت الجماعي والتضامن ليسا استراتيجيتين وقائيتين فحسب، بل يمكنهما أيضاً المساعدة في دحض الرواية القائلة بأن الفرد قد أُسكت أو عُزل أو جُرّد من مصداقيته.

الصوت الجماعي والمؤسسي

- حيثما أمكن، ينبغي إصدار البيانات والتصريحات الصحفية ورسائل الحملات والمواقف العامة عبر حساب تابع للمنظمة أو صفحة اتّلافية أو ملف شخصي جماعي، بدلاً من نشرها عبر الحسابات الشخصية الفردية. يُحوّل ذلك الهدف العلني من فرد مُسمّى إلى كيان أوسع، مما يجعل التحرش المنسق أو نشر البيانات الشخصية دون إذن أصعب تركيزاً على شخص واحد.
- التناوب في الأدوار العلنية بين الزعماء الموثوقين أو أعضاء الفريق خلال فترات التصاعد، حتى لا يتحمّل شخص واحد كل التعرض المباشر الناجم عن الحملة. يشمل ذلك الظهور الإعلامي ذا الصلة والفعاليات العامة والردود على وسائل التواصل الاجتماعي وأي نشاط يستقطب تفاعل الجمهور.
- استخدام التأليف المشترك أو البيانات الجماعية غير المنسوبة حين لا تكون النسبة الفردية ضرورية لمصداقية الرسالة أو تأثيرها. النظر في الاتفاق مسبقاً مع المنظمة أو التحالف على متى تكون النسبة الجماعية مناسبة، حتى لا يُضطر إلى اتخاذ القرار تحت الضغط.
- تعيين نقطة اتصال للتواصل أو ناطق رسمي من داخل الفريق أو المنظمة يمتلك القدرة والاستعداد والموافقة لإدارة الظهور العلني خلال الفترات عالية الخطورة، بدلاً من الاعتماد تلقائياً على الفرد الأكثر حضوراً.

التواصل القائم على الصفحات والحملات الانتخابية

- إنشاء قنوات تواصل قائمة على الصفحات أو تفعيلها، كصفحات الحملات الانتخابية والملفات المؤسسية وحسابات المناصرة غير المرتبطة بهوية شخصية أو أرقام هواتف أو عناوين بريد إلكتروني، قبل فترات التصاعد المحتملة لا استجابةً للهجمات فحسب.
- الحفاظ على اتفاقيات داخلية واضحة بشأن من يملك صلاحية الإدارة على الصفحات أو الحسابات المشتركة، وكيفية اعتماد المحتوى ونشره، وما يحدث للصلاحيات إذا تعرّض أحد أعضاء الفريق للاستهداف أو تراجع مؤقتاً.
- مراجعة المعلومات التعريفية المتاحة عبر البصمة الرقمية العامة للمنظمة لحماية المعلومات الشخصية وبيانات الاتصال بالأعضاء المؤسسين والمسؤولين في أقسام «من نحن» أو التغطيات الإعلامية.

هياكل الشبكات

- بناء علاقات مع المنظمات المماثلة وشبكات المناصرة أو التحالفات قبل نشوء الأزمات، حتى يمكن تعبئة طلبات التضخيم الجماعي أو الرسائل المضادة أو بيانات التضامن العلني بسرعة عند الحاجة.
- الاتفاق المسبق على بروتوكولات الدعم المتبادل مع الحلفاء الموثوقين. كالاتفاق مثلاً على أنه إذا تعرّض أحد أعضاء الشبكة للاستهداف، يعمل الآخرون على تضخيم رسالته الأساسية والإبلاغ عن المحتوى المسيء أو إصدار بيانات دعم علنية دون انتظار الطلب.

حماية الدائرة المقرّبة

6.3

لا يمكن أن يقتصر التخطيط للمشاركة الأكثر أماناً على الشخص المستهدف وحده. إذ كثيراً ما تمتد الهجمات الرقمية، ولا سيما نشر البيانات الشخصية دون إذن والكشف عن الهوية وانتحال الهوية والتحرّش المنشق، لتطال أفراد الأسرة والشركاء العاطفيين والزلاء المقربين وغيرهم ممن ينتمون إلى الشبكة المباشرة للشخص المستهدف. وتُعَدّ حماية المحيطين بالشخص المستهدف ركيزة أساسية في التخطيط للسلامة.

إبلاغ الأسرة والأشخاص المقرّبين

- إبلاغ أفراد الأسرة الموثوقين والشركاء والأصدقاء المقربين بطبيعة المخاطر التي يواجهها الشخص فور بدء العنف الرقمي. يُتيح ذلك لهم الاستعداد في حال امتدت الهجمات إليهم، ودعم الشخص المستهدف.
- إبلاغ الزلاء الموثوقين بالتهديدات القائمة أو المتوقعة حيثما كان ذلك مناسباً وأماناً، حتى يتجنّبوا مشاركة المعلومات دون قصد، ويتمكّنوا من التعرف على محاولات انتحال الهوية، وتقديم الدعم المهني دون أن يؤخذوا على حين غرة.
- وضع حدود واضحة مع جهات الاتصال المهنية وفرق الحملات الانتخابية بشأن المعلومات المتعلقة بعمل الشخص المستهدف وجدوله الزمني أو موقعه التي يمكن مشاركتها خارجياً، ومراجعة ما تنشره المنظمة أو صاحب العمل عن الشخص المستهدف في أدلة الموظفين وقوائم الفعاليات أو المواد الصحفية.

تقليل البصمة الرقمية للدائرة المقرّبة

- تشجيع أفراد الأسرة والأشخاص المقرّبين على مراجعة إعدادات الخصوصية على حساباتهم الخاصة، ولا سيما حيثما قد تكون الصور التي وُضعت عليها علامات أو بيانات الموقع أو معلومات العلاقات أو تفاصيل مكان العمل مرئية ويمكن توظيفها لتحديد مكان الشخص المستهدف أو الضغط عليه من خلالهم.
- اطلبوا من الأشخاص المقرّبين إزالة أو تقييد المحتوى العلني الذي يكشف عن الأماكن المشتركة للشخص المستهدف أو روتينه أو ترتيبات سكنه أو هيكل أسرته، ولا سيما حين يتضمن المحتوى صوراً موسومة في المنزل أو مواقع مدارس الأطفال أو عناوين السكن المرئية.
- ينبغي التعامل مع المعلومات المتعلقة بالأطفال، بما فيها أسماؤهم أو مدارسهم أو مظهرهم أو روتينهم اليومي، بوصفها معلومات حساسة وإبقاؤها بعيدة عن المحتوى العلني، إذ يكون الأطفال عرضةً بشكل خاص للاستهداف غير المباشر.

الاعتبارات العاطفية والنفسية

- قد تعاني الدائرة المقرّبة من خوف أو ضيق أو صدمة ثانوية جراء الهجمات، حتى وإن لم تكن مستهدفةً بشكل مباشر. لذا تُعَدّ المحادثات المفتوحة والمريحة والمنتظمة ضرورية لتخفيف هذه المخاوف.
- حيثما أمكن، ينبغي تحديد الأشخاص ضمن الدائرة المقرّبة للمستهدف مسبقاً ممن يمكنهم تقديم الدعم العملي (مثل إدارة الحسابات أو تولّي الاتصالات)، ومن يمكنهم تقديم الدعم النفسي أو المعنوي، ومن قد يكون من الضروري حمايتهم من معرفة كامل تفاصيل ما يحدث.
- وضع حدود مع الأشخاص المقرّبين بشأن مقدار تفاعلهم مع المحتوى المسيء الموجه ضد الناجية، بما في ذلك طلب عدم اطلاعهم على تهديدات المضايقات أو لقطات شاشة الهجمات أو الرسائل المباشرة المسيئة نيابةً عن الشخص المستهدف، إذ يمكن أن ينقل ذلك الأذى إليهم.

ما الذي يجب على الآخرين القيام به؟

6.4

لا يمكن أن تقع مسؤولية المشاركة الآمنة في الفضاء العام على عاتق الشخص المستهدف وحده. فالمنصات الرقمية والأحزاب السياسية وأصحاب العمل والجهات المانحة جميعهم يتحملون مسؤوليات لا تتناولها الأقسام السابقة. ويحدد هذا الدليل هذه المسؤوليات هنا لتوزيع العبء بشكل أكثر عدلاً، ولتزويد الأشخاص المستهدفين وحلفائهم والمدافعين عنهم بمجموعة واضحة من المطالب التي يمكن توجيهها إلى المؤسسات المحيطة بهم.

— ما الذي يجب أن تفعله الأحزاب السياسية

- اعتماد مدونات سلوك تحظر صراحةً مشاركة الأعضاء المنتسبين أو دعمهم للعنف القائم على النوع الاجتماعي الميسر بالتكنولوجيا، مع تحديد عقوبات واضحة في حال المخالفة.
- إنشاء آليات شكاوى داخلية آمنة يمكن للنساء داخل الحزب وعلى قوائم الانتخابية استخدامها دون خوف من الانتقام.
- إصدار مواقف علنية تدين الهجمات المحددة التي تستهدف المرشحات والفاعلين من مجتمع الميم-عين عند وقوعها؛ فالصمت بحد ذاته يُعد موقفاً.
- الالتزام بشكل دائم بعدم الاستفادة من أعمال العنف القائم على النوع الاجتماعي الميسر بالتكنولوجيا الموجهة ضد الخصوم أو توظيفها في الحملات السياسية.

— ما الذي يجب أن تفعله المنصات الرقمية

- **إدارة محتوى شفافة:** نشر معايير المجتمع باللغة العربية وتطبيقها بشكل متسق بغض النظر عن الانتماء السياسي، مع توفير آليات استئناف تتلقى ردوداً ضمن الأطر الزمنية المعلنة.
- **جهات اتصال إقليمية محددة:** تعيين مشرفين بشريين معروفين للبنان ومنطقة الشرق الأوسط وشمال أفريقيا يمكن التواصل معهم في الحوادث عالية الخطورة دون الحاجة إلى المرور عبر نماذج الإبلاغ العامة.
- مسارات أسرع للتعامل مع نشر الصور الحميمية المنشورة دون موافقة، ونشر البيانات الشخصية دون إذن، وحملات التحرش المنشقة، بما في ذلك استخدام المطابقة الاستباقية للبصمات الرقمية.
- تقارير علنية حول قرارات إزالة المحتوى التي تؤثر على الجهات الفاعلة المدنية اللبنانية، مع مشاركة بيانات حالات مجهولة الهوية مع منظمات المجتمع المدني.

— ما الذي يجب أن يفعله المانحون والجهات الممولة

- الاعتراف بأن السلامة الرقمية بند مشروع ومؤهل للتمويل ضمن المنح، بدلاً من اعتباره تكلفة تشغيلية غير ممولة.
- تجنب فرض جداول زمنية تدفع الجهات المستفيدة إلى الظهور العلني المكثف خلال الفترات السياسية الحساسة دون توفير الدعم اللازم لمواجهة المخاطر الأمنية الناتجة عن ذلك.
- اعتبار الإبلاغ عن الحوادث مؤشراً على قوة أنظمة الرصد والمتابعة، وليس دليلاً على ضعف البرامج أو فشلها.

— ما الذي يجب أن يفعله أصحاب العمل والمنظمات

- منح إجازات مدفوعة الأجر للموظفين المتأثرين بحملات الهجمات الرقمية المستمرة، واعتبار ذلك خطراً مهنيّاً لا مسألة شخصية.
- توفير الدعم القانوني والنفسي والاجتماعي على نفقة جهة العمل، بدلاً من تحميل الناجية التكاليف.
- تعديل المهام ذات الظهور العام خلال فترات الخطر المرتفع دون أن يؤثر ذلك سلباً على تقييم الأداء.
- وضع بروتوكولات حماية واضحة للموظفين الذين تجعلهم طبيعة عملهم أكثر عرضة للاستهداف العلني.

الذكاء الاصطناعي والسلامة الرقمية

صارت أدوات الذكاء الاصطناعي حاضرة في تفاصيل الحياة الرقمية، كروبوتات المحادثة الآلية، ومولّدات الصور، وأنظمة الإشراف على المحتوى، وخوارزميات البحث، وبالنسبة للمرشحات والمرشحين من مجتمع الميم-عين والمدافعات والمدافعين عن حقوق الإنسان والفاعلين المدنيين، يفتح الذكاء الاصطناعي ثغرات عملية يفيد التعرّف عليها قبل وقوع الهجوم. ويتناول هذا القسم كيفية مساهمة الذكاء الاصطناعي في تضخيم الهجمات الرقمية، وكيف يمكن حماية المعلومات الشخصية عند استخدام أدوات الذكاء الاصطناعي، والخطوات العملية للحد من التعرض للمخاطر.

كيف يمكن للذكاء الاصطناعي أن يضخم العنف الرقمي؟

7.1

تُستخدم هذه الأدوات لتوسيع نطاق الهجمات الرقمية، وأتمتتها، وزيادة حدّتها، والتعرّف على هذه الاستخدامات هو نقطة البداية.

محتوى التزييف العميق والوسائط الاصطناعية

يمكن استخدام أدوات توليد الصور والفيديو بالذكاء الاصطناعي لإنشاء محتوى واقعي لكنه مُفبرك، ويشمل ذلك مقاطع فيديو مزيفة، أو صوراً مُعدّلة، أو تسجيلات صوتية مُصطنعة تنسب زوراً تصريحات أو ملامح أو أفعالاً إلى شخص مستهدف. وفي السياقات السياسية، تُستخدم تقنيات التزييف العميق لتصنيع محتوى مُحرّج أو ذي طابع جنسي، أو لنشر معلومات مضللة حول مواقف المرشحين، أو إنتاج مواد تهدف إلى الإذلال أو التشهير أو تقويض السمعة. ولا يشترط أن يكون المحتوى مقنعاً لیسبب ضرراً؛ إذ يمكن حتى للمحتوى المُعدّل بشكل واضح أن ينتشر بسرعة ويلحق الضرر بالسمعة قبل تصحيحه. وفي حالات الصور الحميمة المنشورة دون موافقة أو التزييف العميق، راجعوا 3.6 الصور الحميمة المنشورة دون موافقة والتزييف العميق.

ما الذي يجب الانتباه إليه

- صور أو مقاطع فيديو لشخص مستهدف في مواقف لم يكن فيها من قبل، حميمة أو غير ذلك.
- تسجيلات صوتية منسوبة إلى شخص مستهدف لم يتم بتسجيلها.
- لقطات شاشة مُعدّلة لمنشورات أو تصريحات لم يكتبها الشخص.
- محتوى مُصطنع يجمع بين وجه وصوت الشخص المستهدف وسيناريوهات مُخلقة.

تدابير التخفيف: إنشاء حضور موثوق وفتحّق منه عبر المنصات الرئيسية بحيث يكون لدى الجمهور مرجع موثوق يميز بين المحتوى الحقيقي والمحتوى المُفبرك. وفي حال ظهور محتوى مُولّد اصطناعياً، إصدار تصحيح واضح ومختصر وحقيقي عبر القنوات الموثقة الخاصة بك، وعدم مشاركة المحتوى المُفبرك حتى بهدف تفنيده أو نفيه. وطلب تحليل جنائي لتأكيد الأصل الاصطناعي وتعزيز أي بلاغ للمنصات أو شكوى قانونية. والإبلاغ عن المحتوى عبر المنصات باستخدام قنواتها الخاصة للإبلاغ عن الوسائط الاصطناعية أو المعدّلة إن وُجدت [راجعوا 8.4 الإبلاغ عن الصور الحميمة المنشورة دون موافقة ومحتوى التزييف العميق].

انتحال الهوية عبر الذكاء الاصطناعي وتوليد النصوص

يمكن لنماذج اللغة الكبيرة إنتاج كميات ضخمة من النصوص المقنعة بسرعة، مما يتيح إنتاج تصريحات مزيفة أو اقتباسات مختلفة أو رسائل منسّقة تبدو وكأنها صادرة عن أشخاص حقيقيين. وهذا يقلل تكلفة الجهود المنسقة للتحرش، ويسمح لمجموعات صغيرة أو أفراد بتصميم حملة تبدو وكأنها معارضة واسعة ومنظمة.

تدابير التخفيف: إعداد تنبيهات لاسمكم وتنوعاته لمراقبة الحسابات المزيفة أو التصريحات المُفبركة التي تستخدم اسمكم. والإبلاغ الفوري عن حسابات الانتحال للمنصات مع حفظ جميع الأدلة والوثائق.

التحرش الآلي واسع النطاق

يمكن استخدام أدوات الذكاء الاصطناعي لإنتاج ونشر محتوى مسيء بكميات وسرعة تفوق قدرة البشر على التعامل معها. تشمل بعض الأساليب إغراق التعليقات، أو إنتاج نسخ متعددة من نفس الهجوم لتجاوز أنظمة الحظر، أو إنشاء تحرش مخصص على نطاق واسع.

تدابير التخفيف: تفعيل فلاتر التعليقات، وحظر الكلمات المفتاحية، وأدوات الإشراف على المنصات التي يتركز فيها التحرش الآلي. وتقييد مؤقت لمن يمكنه التعليق أو الرد أو التفاعل مع المحتوى.

التعرّف على الوجه والمراقبة

يمكن لأدوات التعرف على الوجه المدعومة بالذكاء الاصطناعي تحديد الأشخاص من الصور أو مقاطع الفيديو المنشورة عبر الإنترنت وربطهم عبر منصات متعددة. وبالنسبة للأشخاص من مجتمع الميم-عين والناشطين ومن لم يُعلنوا هويتهم علناً، يُشكّل ذلك خطراً خاصاً يتمثل في كشف الهوية قسراً أو الفضح أو التعرض غير الطوعي.

تدابير التخفيف: تودّوا الحذر عند الإشارة إلى الآخرين في الصور أو السماح للآخرين بالإشارة إليكم. وعظّموا ميزات التعرف على الوجه في إعدادات الخصوصية عند توفرها على المنصات.

7.2 حماية المعلومات الشخصية عند استخدام أدوات الذكاء الاصطناعي

أدوات الذكاء الاصطناعي، بما فيها روبوتات المحادثة الآلية وأدوات الكتابة وموّدات الصور وأدوات الترجمة، قد تعالج وأحياناً تخزن المعلومات المُدخلة إليها. وخلال الفترات السياسية الحساسة أو عند التعرض لهجمات مستهدفة، يجب التعامل مع المعلومات المشاركة مع أدوات الذكاء الاصطناعي بنفس درجة الحذر كما في أي تواصل رقمي آخر.

ما الذي يمكن أن تحتفظ به أدوات الذكاء الاصطناعي وكيف يمكن استخدامه

- قد يتم تخزين المحادثات مع روبوتات المحادثة الآلية ومراجعتها من قبل المطورين أو استخدامها لتدريب نماذج مستقبلية حسب سياسة المنصة.
- قد يتم الاحتفاظ بالصور أو المستندات أو البيانات الشخصية المشاركة مع أداة ذكاء اصطناعي بعد انتهاء الجلسة.
- بعض منصات الذكاء الاصطناعي تعمل عبر نطاقات قضائية مختلفة ذات معايير حماية بيانات متفاوتة.

خطوات حماية معلوماتك

- قراءة سياسة الخصوصية وشروط الاحتفاظ بالبيانات قبل استخدام أي أداة ذكاء اصطناعي في أعمال حساسة. ابحثوا تحديداً عما إذا كانت المحادثات تُخزّن، ولكم من الوقت، وما إذا كانت تُستخدم للتدريب.
- عدم مشاركة معلومات تعريفية شخصية: الاسم الكامل، والموقع، ورقم الهاتف، ومكان العمل، أو أي تفاصيل محددة.
- عدم استخدام أدوات الذكاء الاصطناعي لمعالجة مستندات حساسة أو ملفات قانونية أو أدلة أو اتصالات سرية.
- استخدام أدوات الذكاء الاصطناعي عبر التصفح الخاص أو وضع التصفح الخفي عند الإمكان لتقليل الاحتفاظ ببيانات الجلسة.
- عند توفر الخيار، إلغاء مشاركة البيانات لتدريب النماذج (تتيح معظم منصات الذكاء الاصطناعي الكبرى ذلك في إعدادات الحساب).
- توجّي الحذر عند استخدام أدوات الذكاء الاصطناعي على أجهزة قد تكون مخترقة، إذ قد تكون البيانات المُدخلة في متناول جهات خارج منصة الذكاء الاصطناعي.
- إذا كنتم تستخدمون أدوات الذكاء الاصطناعي في العمل الحسّاس، فضعوا بروتوكول فريق يحدد ما يمكن وما لا يمكن معالجته عبر هذه المنصات.

IMPORTANT ▲

اعتبارات خاصة بالهجمات المعتمدة على الذكاء الاصطناعي: لا تشاركوا تفاصيل هويتكم أو علاقاتكم أو وضعكم القانوني أو مخاوف سلامتكم مع أدوات الذكاء الاصطناعي. حتى الإفصاح «الخاص» لأداة رقمية قد ينطوي على مخاطر إذا كانت هذه البيانات قابلة للوصول من قبل أطراف ثالثة.

إرشادات الإبلاغ عبر المنصات

توفر المنصات الرقمية آليات للإبلاغ يمكن أن تساعد، في بعض الحالات، على تقليل ظهور المحتوى الضار، أو إزالة المواد التي تنتهك سياسات المنصة، أو المساهمة في إنشاء سجل توثيقي أوسع للحادثة. ومع ذلك، فإن الإبلاغ عبر المنصات ليس حلاً مضموناً، وتختلف فعاليته بشكل كبير حسب المنصة وطبيعة الانتهاك وسرعة الاستجابة. ويوضح هذا القسم متى يكون الإبلاغ خياراً مناسباً، وأهمية توثيق الأدلة قبل الإبلاغ، وما الذي يمكن أن يحققه الإبلاغ فعلياً.

متى يكون الإبلاغ مفيداً

8.1

يكون الإبلاغ عبر المنصات أكثر احتمالاً لتحقيق نتيجة ملموسة عندما يكون المحتوى أو السلوك المُبلَّغ عنه مخالفاً بوضوح لسياسات المنصة، وعندما يُقدّم البلاغ مدعوماً بتوثيق كافٍ. الحالات التالية هي الأكثر احتمالاً لنجاح الإبلاغ:

إزالة المحتوى

- الصور الحميمية المنشورة دون موافقة، حيث توفر معظم المنصات الكبرى مسارات مخصصة وسريعة لإزالة هذا النوع من المحتوى [راجعوا 8.4 الإبلاغ عن الصور الحميمية المنشورة دون موافقة ومحتوى التزييف العميق].
- حسابات انتحال الهوية التي تستخدم أسماء أو صوراً أو هويات أشخاص آخرين بهدف الخداع أو التحرش أو الإضرار بالسمعة.
- التهديدات المباشرة والواضحة بالعنف أو التحرش المستهدف الموجه لشخص محدد بالاسم.
- نشر البيانات الشخصية دون إذن التي تنشر معلومات شخصية مع نية واضحة لتسهيل الإيذاء.
- السلوك المنسق غير الأصلي، مثل حملات الإبلاغ الجماعي أو الهجمات المدفوعة بالحسابات الآلية أو الحسابات التي تُنشأ فقط للتحرش، عندما يمكن توثيق نمط الإساءة.

تقليل الظهور

- قد يؤدي الإبلاغ عن المحتوى أحياناً إلى تقليل انتشاره تلقائياً أو خفض ظهوره خوارزمية أثناء المراجعة، حتى لو لم يتم حذفه فوراً.
- **منصة X/Twitter:** يمكن أن تضع الحسابات التي تتلقى بلاغات متكررة في وضع «القراءة فقط»، مما يحد من النشر وإعادة النشر والإعجاب. يحدث ذلك نتيجة قرار بعد المراجعة، وليس إجراءً وقائياً تلقائياً أثناء المراجعة، ويُطبق على مستوى المنصة بالكامل وليس بشكل خاص تجاه الأشخاص المستهدفين.
- **منصة Instagram:** لا تُفرض قيود أثناء مراجعة البلاغ. يتوفر فيها خيار «تقييد» يحد من تفاعل الحسابات غير المتابعة أو الحسابات الجديدة، لكن يجب تفعيله يدوياً من المستخدم.
- **منصات Facebookg YouTubeg TikTok:** لا تمتلك آلية مماثلة لهذا النوع من القيود.

يمكن أن تؤدي البلاغات المتكررة من عدة مستخدمين حول نفس المحتوى أو الحساب إلى زيادة احتمال مراجعته واتخاذ إجراء من قبل المنصات.

إنشاء سجل توثيقي

حتى عندما لا يؤدي البلاغ إلى إزالة المحتوى، فإن تقديمه يُنشئ سجلاً بأن الحادثة قد تم الإبلاغ عنها. يساعد ذلك في توثيق أنماط الإساءة في حال الرغبة في اتخاذ إجراءات قانونية أو طلب دعم من جهات تنظيمية أو مؤسسات مختصة. يكون الإبلاغ أقل فعالية عندما يقع المحتوى ضمن «المناطق الرمادية» في سياسات المنصات، ويزداد هذا التحدي عندما تكون معايير المجتمع ضعيفة أو غير مطبقة بشكل متسق، أو عندما يُنتج الضرر عبر عدد كبير من الحسابات في إطار حملات تحرش منسقة.

8.2 ما يجب توثيقه قبل الإبلاغ

8.2

تغطي الأقسام 12.4 من هذا الدليل ما يجب توثيقه بشكل كامل. قبل تقديم أي بلاغ عبر المنصة، يُنصح بالعودة إلى هذه الإرشادات [12.4 قائمة التحقق للتوثيق].

من المهم الإبلاغ عن الحالة بعد توثيق الأدلة، وليس قبل ذلك. تميل المنصات ومديرو الحسابات إلى إزالة المحتوى بسرعة بمجرد معالجة البلاغ، بما في ذلك المحتوى الذي لم يتم توثيقه بعد. لذلك يجب حفظ لقطات الشاشة والروابط وأوقات النشر وتفاصيل الحسابات قبل تقديم البلاغ، إذ قد يتم فقدان الوصول إلى المحتوى الأصلي بعد حذفه أو تعطيل الحساب.

8.3 ما الذي يمكن للإبلاغ أن يفعله وما لا يمكنه فعله

8.3

من المهم فهم حدود عمليات الإبلاغ عبر المنصات لتحديد متى يكون استخدامها مناسباً.

ما يمكن للإبلاغ أن يفعله	ما لا يمكن للإبلاغ أن يفعله
بدء عملية مراجعة قد تؤدي إلى إزالة المحتوى أو تعليق الحساب أو تقليل انتشاره.	ضمان إزالة المحتوى أو تعليق الحساب أو أي نتيجة محددة، إذ إن المنصات تطبق سياسات الإنفاذ بشكل غير متسق ولديها تراكمات كبيرة.
إنشاء سجل زمني لواقعة داخل نظام المنصة نفسه.	تحديد الإجراء الذي تم اتخاذه — إن وُجد — بعد مراجعة البلاغ. فمعظم المنصات تكتفي بتأكيد أن البلاغ قد تمت «مراجعته» دون توضيح النتيجة.
التسبب في استجابات أسرع في بعض الحالات، عندما توفر المنصات مسارات مخصصة للفئات عالية الخطورة مثل الصور الحميمة المنشورة دون موافقة أو التهديدات الموثوقة والصريحة أو قضايا سلامة الأطفال.	إيقاف التحرش في الوقت الفعلي. إذ قد تستغرق عمليات المراجعة ساعات أو أياماً يظل خلالها المحتوى مرئياً وقد يزداد انتشاره.
المساهمة في بناء نمط من الأدلة إذا كانت الإساءة مستمرة وتم تقديم بلاغات متعددة مع مرور الوقت.	معالجة الإساءة عبر منصات متعددة. فالإبلاغ في منصة واحدة لا يؤثر على نفس الفاعلين أو المحتوى الذي يظهر في أماكن أخرى.
دعم الإجراءات القانونية أو التنظيمية عندما يعزز سجل البلاغات قضية ما.	أن يحل محل التدابير الوقائية الموازية مثل تعديل إعدادات الخصوصية أو الحظر أو توثيق الأدلة أو طلب الدعم القانوني عند الضرورة.
	معالجة الإساءة المنسقة أو ذات الدوافع السياسية بشكل موثوق، خاصة عندما يتم تسليح أدوات الإبلاغ نفسها عبر البلاغات الكاذبة الجماعية ضد النشطاء والمرشحين.

الإبلاغ المضاد

في بعض حملات التحرش المنسّق، يمكن للمهاجمين استخدام آليات الإبلاغ في المنصات ضد أهدافهم عبر تقديم بلاغات كاذبة بهدف تعليق الحسابات أو إزالة المحتوى. إذا تم تعليق حساب أو إزالة محتوى نتيجة بلاغات كاذبة، فإن معظم المنصات توفر عملية للاستئناف. احرصوا على توثيق إشعار التعليق والمحتوى الذي تمت إزالته وأي سياق يثبت أن البلاغ تم بسوء نية. كما يمكن للمنظمات القانونية الداعمة لحقوق رقمية أن تساعد في إجراءات الاستئناف.

8.4 الإبلاغ عن الصور الحميمة المنشورة دون موافقة والتزييف العميق

8.4

1. أداة الحظر المسبق StopNCII.org

StopNCII.org هي أداة مجانية تتيح للأفراد إنشاء بصمة رقمية (تسمى «هاش») لصورة أو فيديو حميم دون الحاجة إلى رفع الصورة نفسها. يتم مشاركة هذا الهاش مع المنصات المشاركة، والتي تستخدمه تلقائياً لاكتشاف ومنع رفع أو مشاركة الصورة عبر شبكاتها. يعمل StopNCII حالياً مع منصات Meta (فيسبوك وإنستغرام وثيريزد) وTikTok وSnapchat وReddit (وفق قائمة الشركاء). للمزيد من التفاصيل حول كيفية عمله والخطوات، يمكنكم زيارة: <https://stopncii.org/how-it-works/> (متوفر باللغة العربية).

2. قنوات الإزالة العاجلة الخاصة بالمنصات

معظم المنصات الكبرى لديها مسارات مخصصة لإزالة الصور الحميمة المنشورة دون موافقة تعمل بشكل أسرع من أنظمة الإبلاغ العادية. يُفضل استخدام هذه القنوات بدلاً من أدوات الإبلاغ العامة عن المضايقات:

- **ميثا (Facebook/Instagram):** لدى ميثا أداة مخصصة للإبلاغ عن الصور الحميمة المنشورة دون موافقة تتيح طلب إزالة عاجلة. اذهبوا إلى الصورة أو المحتوى المطلوب الإبلاغ عنه، اضغطوا على الخيارات (عادة في أعلى أو أسفل المنشور)، ثم «إبلاغ»، وابتحثوا عن قسم «الإبلاغ عن أضرار محددة» ثم اختاروا «تعبئة النموذج».
- **TikTok:** يوفر TikTok فئة مخصصة للإبلاغ عن الصور الحميمة المنشورة دون موافقة ضمن إرشادات مجتمعه، ويتم إعطاء الأولوية لهذه البلاغات. الإبلاغ يتم عبر: «إبلاغ» ← «العري والأنشطة الجنسية» ← «صور حميمة غير توافقية».
- **X/Twitter:** يوفر X مساراً خاصاً للإبلاغ عن الوسائط الحميمة المنشورة دون موافقة. اختاروا: «الإبلاغ عن المنشور» ← «يعرض صورة حساسة» ← «صورة أو فيديو غير مصرح به» ← «يحتوي على محتوى حميم غير مصرح به». مهم: *بعد التغييرات في سياسات الإشراف لدى X، أصبحت سرعة الاستجابة واتساق التنفيذ أقل. وتلقوا جميع البلاغات المقدمة واستخدموا StopNCII.org.*
- **YouTube:** أداة شكاوى الخصوصية في YouTube تغطي الصور الحميمة المنشورة دون موافقة.
- **أي خدمة من خدمات Google (بما فيها YouTube):** استخدموا [Google نموذج طلب إزالة المحتوى الصريح من](#).

إرشادات خاصة بتليجرام

8.4

يحتل تليجرام مكانة خاصة في المشهد الرقمي اللبناني. فالقنوات المغلقة وشبه العامة هي المكان الذي كثيراً ما تتداول فيه الصور المسربة والعناوين والمواد التشهيرية أولاً، قبل أن تنتقل إلى منصات أكثر خضوعاً للرقابة. يُعالج هذا الدليل تليجرام بشكل مستقل لأن نطاق التهديد فيه وخيارات الإبلاغ تختلف عن تلك الخاصة بالمنصات الكبرى المشمولة في القسم 8.4.

مراقبة القنوات المغلقة

- إذا كان الشخص المستهدف أو أحد طائفته عضواً في القناة التي يظهر فيها المحتوى الضار، يمكن التقاط لقطات شاشة مباشرة. وتلقوا اسم القناة وعدد الأعضاء ومشرفي القناة حيثما كان ذلك متاحاً.
- بالنسبة للقنوات التي لا يستطيع الشخص المستهدف الوصول إليها، يمكن للحلفاء الموثوقين الأعضاء فيها رصد المحتوى نيابةً عنه والإبلاغ بملاحظات بدلاً من إعادة توجيه المحتوى الضار مباشرةً، تفادياً لتعريض الشخص المستهدف لمزيد من الأذى.

الإبلاغ على تليجرام عملياً

- تقبل واجهة الإبلاغ على تليجرام الشكاوى المتعلقة بالبريد العشوائي والعنف وإساءة الأطفال والمواد الإباحية غير المشروعة والانتهاكات حقوقية. أما فئات المحتوى الضار الأخرى — كنشر البيانات الشخصية دون إذن والتشهير والتحرش المنسق — فلا تملك مسارات مخصصة وتستقطب استجابات غير منتظمة. توقعوا استجابة جزئية في أحسن الأحوال.
- القنوات (الفضاءات ذات البث الأحادي الاتجاه) خاضعة لشروط تليجرام؛ أما المجموعات الكبيرة والرسائل المباشرة فيخضعان لتطبيق أضعف. وحيثما ينتهك اسم القناة حقوق شخص ما أو ينتحل هويته، يكون الإبلاغ بوصفه انتحالاً للهوية هو فئة البلاغ الأكثر احتمالاً للنجاح.
- إن أكثر التدابير الوقائية موثوقيةً على تليجرام هي التدابير الخارجية: التوثيق للاستخدام القانوني والرسائل المضادة المنسقة عبر منصات أخرى والضغط على المنصة عبر منظمات الحقوق الرقمية ([سمكس، Access Now](#) — راجعوا 9.4). الإبلاغ المباشر وحده نادراً ما يحل مشكلة التحرش المستضاف على تليجرام.

مسارات الدعم والإحالة

يشكّل المشهد السياسي في لبنان عاملاً مؤثراً في سلامة جميع مسارات الدعم الواردة في هذا القسم. ففي فترات الانتخابات والتوترات السياسية المتصاعدة، قد تكون المؤسسات الرسمية مرتبطة بالأطراف نفسها المسؤولة عن الهجمات. كما تعمل بعض منظمات المجتمع المدني تحت ضغوط كبيرة، بـمـوارد محدودة، وفي بعض الحالات تحت تهديد مباشر. كذلك تمتلك الشبكات السياسية الطائفية القدرة والدافع لمراقبة الشكاوى الرسمية أو اعتراضها أو توظيفها لخدمة مصالحها. يعكس هذا القسم هذه الحقائق، ويوضح الحالات التي قد تتطلب دعماً إضافياً، وأنواع الدعم المتاحة، وكيفية الوصول إليها بأمان في السياق اللبناني.

لا يُعد هذا القسم آلية لإدارة الحالات، بل نقطة انطلاق لمعرفة الجهات التي يمكن اللجوء إليها والعوامل التي ينبغي أخذها في الاعتبار قبل القيام بذلك.

متى يجب طلب دعم إضافي؟

9.1

تغطي الإرشادات الواردة في هذا الدليل إجراءات يمكن اتخاذها بشكل مستقل أو بالاستعانة بشبكة موثوقة. إلا أن بعض الحالات تتطلب دعماً إضافياً. يُنصح بطلب المساعدة عند:

1. تتضمن الحالة أبعداً قانونية

- وجود تهديدات موثوقة بالعنف الجسدي أو الجنسي، ورغبة الشخص المستهدف في تقديم شكوى رسمية.
- نشر بيانات شخصية أو صور حميمة أو معلومات تعريفية، ورغبة الشخص المستهدف في معرفة خيارات إزالة المحتوى أو الانتصاف القانوني.
- اختراق حسابات أو أجهزة بطريقة قد تُعد جريمة جنائية.
- وجود مؤشرات على تورط جهات سياسية منظمة أو شبكات حزبية في الاستهداف.

2. يتطور الوضع إلى أذى خارج الإنترنت

- تصبح التهديدات الإلكترونية أكثر تحديداً أو شخصية أو مرتبطة بوقت معين.
- ظهور مؤشرات على مراقبة أو تتبع أو تهديدات تمس السلامة الجسدية.

3. يتطلب الأثر النفسي دعماً مهنيًا

- يؤثر التحرش المستمر على قدرة الشخص المستهدف على العمل أو النوم أو أداء دوره العام.
- المعاناة من ضغط نفسي حاد أو خوف أو إنهاك نتيجة التعرض المطول للإساءة.
- تأثر المحيطين بالشخص المستهدف نفسياً وعاطفياً.
- الحاجة إلى تحليل جنائي لتحديد مصدر الهجوم أو منشئه أو نمطه التقني، ولا سيما في الحالات التي تشمل اشتباهاً باختراق الحساب أو الجهاز.

4. تتجاوز الحالة التقنية القدرات المتاحة

- تعرض الأجهزة أو الحسابات أو الاتصالات للاختراق والحاجة إلى دعم تقني متخصص.
- إدارة هجمات منسقة واسعة النطاق عبر عدة منصات.
- الحاجة إلى تقييم أمني يتجاوز الخطوات الواردة في هذا الدليل.

اعتبارات السلامة الموهمة قبل طلب المساعدة

9.2

تشكل القنوات الرسمية للدولة مخاطر محددة قد تزيد من احتمالية الضرر. فالمؤسسات اللبنانية الرسمية، بما في ذلك قوى الأمن الداخلي والسلطة القضائية والهيئات ذات الصلة، ليست متساوية في مستوى الأمان أو سهولة الوصول للجميع. خلال فترات الحساسية السياسية، تعمل هذه المؤسسات ضمن بيئة سياسية طائفية قد تُعاد فيها توجيه الشكاوى أو يتم قمعها أو استخدامها كأداة ضغط، وذلك بحسب الانتماءات السياسية للأطراف المعنية. قد يكون الإبلاغ إلى السلطات الرسمية مناسباً في بعض الحالات، لكنه قد يكون خطيراً في حالات أخرى، اعتماداً على هوية الجهة التي تقف وراء الهجوم، وما إذا كانت هوية الشخص المستهدف ودوره العلني يجعله عرضة للاستهداف من قبل نفس الجهات التي يتم التبليغ إليها.

IMPORTANT ▲

قبل التوجه إلى أي جهة رسمية تابعة للدولة، استشيروا مستشاراً قانونياً موثقاً أو منظمة مجتمع مدني مستقلة سياسياً لتقييم ما إذا كان ذلك آمناً في سياق الهجوم.

في لبنان ينطوي ذلك على مخاطر حقيقية ينبغي الموازنة بينها بعناية.

- تتطلب الشكاوى الرسمية الإفصاح عن وجود صور حميمة أمام الشرطة أو القضاء، مما قد يؤدي إلى مزيد من التعرض وفقدان السيطرة على السردية.
 - في حالات العنف من الشريك الحميم أو السابق، قد تعطي الضغوط العائلية أو الوساطات أو الاستجابات المؤسسية الأولوية للمصالحة على حساب الحماية (تواصلوا مع «أبعاد» و«كفى» — راجعوا 9.4 قائمة الموارد).
 - يواجه أفراد مجتمع الميم-عين مخاطر قانونية إضافية بسبب المادة 534 من قانون العقوبات اللبناني (تواصلوا مع «حلم» أو Proud أو «موزاييك» قبل الإبلاغ الرسمي — راجعوا 9.4 قائمة الموارد).
 - قد تكون الإجراءات القانونية في لبنان بطيئة ونتائجها غير مؤكدة، خصوصاً في ظل محدودية الحماية الرقمية وعدم اتساق تطبيق الإجراءات.
- واجه مستخدمو ومستخدمات مجتمع الميم-عين مخاطر قانونية إضافية وخاصة. فالمادة 534 من قانون العقوبات اللبناني تجرم العلاقات المثلية، وقد استُخدمت لاحتجاز وملاحقة وإكراه أفراد من مجتمع الميم-عين. بالنسبة للمستخدمين والمستخدمات الكويريين، فإن الإبلاغ الرسمي إلى قوى الأمن الداخلي أو أي جهات رسمية أخرى قد يحمل خطر استخدام هويتهم ضدهم، بغض النظر عن طبيعة الهجوم الأصلي. لذلك يُفضّل عدم التواصل مع المؤسسات الرسمية قبل استشارة منظمات المجتمع المدني المعنية بحقوق مجتمع الميم-عين (مثل «حلم» أو Proud)، والتي تمتلك فرقة قانونية لديها خبرة في التعامل مع هذا النوع من المخاطر.
- إن عملية التواصل بحد ذاتها تترك أثراً. فالتواصل مع أي منظمة يُنشئ سجلاً يمكن تتبعه لاحقاً. لذلك تُعد قنوات الاتصال المشفرة من طرف إلى طرف ضرورة لحماية البيانات، ويُفضّل أن يتجنب الأشخاص المستهدفون استخدام بريدهم الإلكتروني المعتاد أو حساباتهم الشخصية على وسائل التواصل الاجتماعي عند طلب المساعدة. [راجعوا القسم 5.3 تقليص التعرّض الفوري للحصول على إرشادات حول الاتصالات الآمنة]. قبل التواصل مع أي جهة دعم، يجب التأكد من حفظ الأدلة وتوثيقها بشكل سليم وآمن. [راجعوا 12.4 قائمة التحقق للتوثيق].

أنواع الدعم التي قد تكون ذات صلة

9.3

— الدعم القانوني

يكون مناسباً عندما يفكر الأشخاص المستهدفون في تقديم شكوى رسمية، أو يحتاجون إلى فهم حقوقهم بموجب القانون اللبناني، أو يواجهون تشهيراً أو انتحال هوية ينعكس على حياتهم المهنية، أو يحتاجون إلى توثيق قانوني لتقديم طعن أو تعصيد. يُفضّل البحث عن منظمات لديها خبرة في حقوق الإنسان الرقمية وحرية التعبير والعنف القائم على النوع الاجتماعي أو القانون الانتخابي، وتعمل بشكل مستقل عن البنى السياسية الطائفية.

— الدعم في الأمن الرقمي

يكون مناسباً عندما تكون الحسابات أو الأجهزة قد تعرضت للاختراق، أو تكون هناك حاجة لإجراء تدقيق أمني، أو عند إدارة هجمات منسقة عبر عدة منصات، أو الحاجة إلى إرشادات حول وسائل تواصل آمنة تتجاوز ما هو وارد في هذا الدليل.

— الدعم النفسي والاجتماعي

يكون مناسباً عندما يؤثر التحرش المستمر أو الاستهداف العلني على الصحة النفسية أو العلاقات الشخصية أو القدرة على مواصلة العمل. يُفضّل البحث عن مقدّمي خدمات لديهم خبرة في التعامل مع الصدمات ومع المدافعات/ين عن حقوق الإنسان أو الناجين من العنف القائم على النوع الاجتماعي أو أفراد مجتمع الميم-عين.

— الدعم المجتمعي ودعم الأقران

يكون مناسباً عندما تكون هناك حاجة إلى مساعدة عملية في التعامل مع الإساءة، أو عندما يساعد التواصل مع أشخاص مرّوا بتجارب مشابهة في تقديم دعم معنوي. يمكن أن توقّر شبكات النساء في السياسة وتحالفات مجتمع الميم-عين وشبكات المدافعين/ات عن حقوق الإنسان دعماً من الأقران أو مناصرة جماعية أو تضامناً.

— الدعم الطارئ

يكون مناسباً عندما يكون الشخص المستهدف أو أحد أفراد دائرته المباشرة في خطر. في هذه الحالة يجب الاعتماد على شبكات الدعم الموثوقة.

قائمة الموارد

9.4

تم جمع بيانات الاتصال أذناه وقت إعداد هذا الدليل في عام 2026. قد تتغير أرقام الهواتف وساعات العمل وعناوين البريد الإلكتروني بشكل متكرر في بيئة التشغيل في لبنان. قبل الاعتماد على أي جهة من هذه القائمة في حالة طارئة، يجب التحقق من معلومات الاتصال الحالية عبر الموقع الرسمي للمنظمة أو حساباتها على وسائل التواصل الاجتماعي. إذا تبيّن أن أي وسيلة اتصال لم تعد تعمل، يُرجى الإبلاغ عنها عبر info@humena.org ليتم تصحيحها في النسخة القادمة.

دعم الطوارئ والحقوق الرقمية

طارئ · 24/7

فرونت لاين ديفنדרز (FLD)

+353 1 210 0489 (خط الطوارئ، 24/7 — دبلن)

منظمة دولية مخصصة لحماية وأمن المدافعين عن حقوق الإنسان المعرضين للخطر حول العالم. توفر دعماً سريعاً وعملياً يشمل منح طارئة وإعادة توطين مؤقتة وبناء قدرات في الأمن الرقمي ودعماً نفسياً. تدير خط طوارئ يعمل على مدار 24 ساعة باللغات العربية والإنجليزية والفرنسية. نموذج اتصال آمن متاح. البريد الإلكتروني: info@frontlinedefenders.org · الموقع الإلكتروني

الدعم القانوني

قانوني

المفكرة القانونية

+961 1 383 606

منظمة مستقلة متخصصة في البحث القانوني والدعوى الاستراتيجية. تعمل في مجالات حرية التعبير والعنف القائم على النوع الاجتماعي وحقوق مجتمع الميم-عين والمساءلة السياسية. مناسبة لجميع الفاعلين المدنيين والمدافعين/ات عن حقوق الإنسان والنساء المعرضات للخطر الذين يحتاجون إلى مساعدة قانونية. البريد الإلكتروني: info@legal-agenda.com · الموقع الإلكتروني

قانوني

المركز اللبناني لحقوق الإنسان (CLDH)

+961 1 24 00 23

منظمة حقوق إنسان غير حزبية تقدّم خدمات قانونية وتوثيق الانتهاكات. تعمل في قضايا الاحتجاز التعسفي والتعذيب وانتهاكات حقوق الإنسان بشكل عام. مناسبة للحالات التي تتضمن انتهاكات خطيرة للحقوق أو تهديدات أو مراقبة أو ترهيب من جهات حكومية أو غير حكومية. كما يمكن للمركز تقديم دعم نفسي أيضاً. البريد الإلكتروني: info@cldh-lebanon.org · الموقع الإلكتروني

دعم مناهضة العنف القائم على النوع الاجتماعي وحقوق المرأة

عنف النوع الاجتماعي / حقوق المرأة

منظمة أبعاد – مركز موارد المساواة بين الجنسين

+961 81 788 178 (خط المساعدة)

منظمة نسوية تعمل على قضايا المساواة بين الجنسين والعنف القائم على النوع الاجتماعي والمشاركة السياسية للنساء في مختلف أنحاء لبنان. تدير مساحات آمنة وخط مساعدة يعمل على مدار 24 ساعة. لديها خبرة موثقة في العمل ضمن سياقات الأزمات والطوارئ. مناسبة للمرشحات السياسيات والناشطات والفاعلين/ات المدنيين/ات الذين يتعرضون لاستهداف قائم على النوع الاجتماعي. البريد الإلكتروني: abaad@abaadmena.org · [الموقع الإلكتروني](#)

ج

المشاركة السياسية للنساء

التجمع النسائي الديمقراطي اللبناني (RDFL)

+961 71 500 808 (خط المساعدة)

منظمة نسوية علمانية تعمل على تعزيز المشاركة السياسية للنساء والمساواة بين الجنسين والقضاء على العنف ضد المرأة. لدى التجمع خمسة مكاتب في لبنان (بيروت وطرابلس وبعبك وكسروان وصيدا) مما يمنحها وصولاً جغرافياً خارج بيروت. كما تدير خط مساعدة يعمل على مدار 24 ساعة. مناسبة للمرشحات السياسيات والفاعلين/ات المدنيين/ات ولديها خبرة قوية في الإحالة إلى خدمات دعم النساء في المجال السياسي. [الموقع الإلكتروني](#)

دعم مناهضة العنف القائم على النوع الاجتماعي وحقوق المرأة (تابع)

حقوق المرأة

Women Alive

+961 78 842 090

منظمة معنية بحقوق النساء والفتيات تعمل على مناهضة العنف القائم على النوع الاجتماعي من خلال المناصرة والتدريب والتوعية. تقدم إرشادات في مجال العنف القائم على النوع الاجتماعي ودعمًا نفسيًا اجتماعيًا (خاصة في طرابلس). البريد الإلكتروني: info@womenalive.net

عنف النوع الاجتماعي / العنف العشير

كفى (عنف واستغلال)

+961 3 018 019 (خط المساعدة 24/7)

منظمة نسوية تعمل بشكل وثيق مع الناجيات من العنف القائم على النوع الاجتماعي والعنف العشير في لبنان. تقدم دعماً متكاملًا يشمل خدمات اجتماعية وقانونية ونفسية للناجين/ات عبر شبكة من المستشارين/ات والمحامين/ات والأخصائيين/ات الاجتماعيين. تدير خط مساعدة يعمل على مدار 24 ساعة لتقديم دعم فوري. البريد الإلكتروني: kafa@kafa.org.lb · [الموقع الإلكتروني](#)

دعم مجتمع الميم-عين

دعم مجتمع الميم-عين

حلم

+961 81 478 450 (خط المساعدة)

منظمة حقوقية معنية بمجتمع الميم-عين في لبنان، تقدم استجابة طارئة ومساعدة قانونية وإدارة حالات ودعمًا نفسيًا اجتماعيًا وخدمات مجتمعية للأفراد الكويريين. تدير خط طوارئ يعمل على مدار 24 ساعة (متاح عبر سيغنال). البريد الإلكتروني: info@helem.net · [الموقع الإلكتروني](#)

دعم مجتمع الميم-عين

موزاييك

+961 76 945 445 (خط المساعدة)

منظمة تعمل على إنهاء الكراهية ضد المثليين والمتحولين في لبنان من خلال تمكين المجتمع والمناصرة الجماعية وتقديم خدمات كريمة للأشخاص من مجتمع الميم والكويريين. البريد الإلكتروني: mosaic@mosaic-mena.org · [الموقع الإلكتروني](#)

الصحة الجنسية ومجتمع الميم-عين

مرسى

+961 1 380 515

مركز صحة جنسية وإنجابية في بيروت يقدم خدمات طبية ونفسية واجتماعية سرية تامة للأشخاص من مختلف الخلفيات، مع تركيز خاص على مجتمع الميم-عين. البريد الإلكتروني: visutus@marsa.me · [الموقع الإلكتروني](#)

دعم مجتمع الميم-عين

Proud Lebanon

+961 76 608 205

منظمة تقدم دعماً قانونياً وإدارة حالات ودعمًا نفسيًا وخدمات مجتمعية للأشخاص من مجتمع الميم والفئات المهمشة في لبنان. البريد الإلكتروني: Support@ProudLebanon.org · [الموقع الإلكتروني](#)

الأمن الرقمي والحقوق الرقمية

حقوق رقمية

سمكس (SMEX)

+961 81 633 133 (مركز المساعدة)

منظمة حقوق رقمية تعمل على حرية التعبير والخصوصية والسلامة على الإنترنت. تقدم سمكس دعماً على مستوى المؤسسات في مجال الحقوق الرقمية. تدير مركز مساعدة يوفر دعماً مباشراً في الأمن السيبراني للناشطين/ات والصحفيين/ات والمدافعين/ات عن حقوق الإنسان والفئات المهمشة الذين يواجهون تهديدات وهجمات رقمية. كما تقدم خدمات تحليل جنائي رقمي. البريد الإلكتروني: helpdesk@smex.org · [الموقع الإلكتروني](http://الموقع.الإلكتروني)

الأمن الرقمي · 24/7

أكسس ناو — خط مساعدة الأمن الرقمي

+1 888 414 0100 (24/7)

خط مساعدة عالمي مجاني يعمل على مدار 24/7، ويقدم استجابة سريعة للحوادث في مجال الأمن الرقمي للمدافعين/ات عن حقوق الإنسان، مع إمكانية الدعم باللغة العربية وخبرة في السياق اللبناني. يُوصى به كجهة اتصال أولى في حالات اختراق الحسابات أو الأجهزة أو الهجمات المنسقة عبر عدة منصات. يمكنه تقديم دعم تقني ومساعدة قانونية وإرشادات للتعامل الآمن مع الهجمات الرقمية. البريد الإلكتروني: help@accessnow.org / legal@accessnow.org · [الموقع الإلكتروني](http://الموقع.الإلكتروني)

الدعم النفسي والاجتماعي

الصحة النفسية · خط دعم 24/7

إمبرايس (Embrace)

1564 (خط الدعم)

منظمة للصحة النفسية تقدم علاجاً ميسور التكلفة ورعاية نفسية وطبية نفسية ودعماً نفسياً اجتماعياً وخدمات صحة نفسية مجتمعية. تدير خطاً وطنياً يعمل على مدار 24 ساعة يقدم دعماً عاطفياً مجهول الهوية وتدخلات في حالات الأزمات وإحالات إلى خدمات الصحة النفسية. البريد الإلكتروني: info@embracelebanon.org · [الموقع الإلكتروني](http://الموقع.الإلكتروني)

ب

القسم 10

توجيهات للحلفاء والصديقات والزملاء

حين تتعرض مرشحة أو ناشطون وناشطات من مجتمع الميم-عين أو مدافعة عن حقوق الإنسان أو ناشطة في الفضاء المدني للعنف الرقمي، تُسهم استجابة من حولها في تحديد مآل الهجوم. الزملاء وفِرَق الحملات وأعضاء الأحزاب والصديقات والشبكات التنظيمية كلهم جزء من المعادلة. شبكة حلفاء واعية ومنسقة تُخفّف الأذى وتُسوّع الضغوط وتدعم استمرار الشخص المستهدف في دوره العام. أما الدائرة غير الفهّية أو تلك التي تتحرك بردود فعلٍ متسرّعة فقد تُضخم الهجوم وتُجرّد الشخص المستهدف من فاعليّته وتولّد مخاطر جديدة.

في الفترات السياسية الحساسة، تعمل الحملات ومنظمات المناصرة تحت ضغطٍ مرتفع وحضورٍ عامٍ واسع. كلّ قرار بشأن كيفية الاستجابة للهجوم يحمل تبعاتٍ سياسية وشخصية. وُضع هذا القسم ليساعد المحيطين بالشخص المستهدف على التصرف بطريقةٍ داعمة فعلاً تنطلق من مصلحته وتستند إلى فهمٍ لكيفية عمل العنف الرقمي.

ما الذي يفعله الحلفاء الداعمون

10.1

1. ابدأوا بالشخص المستهدف، لا بالهجوم

أهمّ خطوة يمكن لأيّ حليف أن يقوم بها هي التواصل مع الشخص المستهدف قبل أيّ تحرّك. اسألوه عمّا يحتاجه وعمّا قام به فعلاً وعن نوع الدعم الذي يريده. لا تفترضوا. قد يبدو الاندفاع إلى التحرك السريع مفيداً عبر منشور تضامني أو الإبلاغ عن المحتوى أو التواصل مع الإعلام، لكنّه قد يتجاوز استراتيجية الشخص نفسه ويكشف معلوماتٍ لم يختار الإفصاح عنها. كما قد يزيد ظهور الحادثة ويُكثّف الأذى بشكلٍ يستحقّ تجنّبه.

- اسألوا بشكل مباشر: «ما الذي تحتاجه/تحتاجينه مَيَّ الآن؟» و«هل ثمة شيء توذِّ/توذيْن ألا أفعله؟»
- اتركوا للشخص المستهدف أن يقرر ما إذا كان الوضع يستوجب معالجة علنية، أو يبقى داخلياً، أو يعالج بهدوء.
- احترموا قراره حتى لو لم تتفقوا معه: قد يختار ألا يرد علناً، أو ألا يبلغ، أو ألا يشارك منظمات خارجية، حتى وإن كنتم لا توافقون على هذا الخيار.

2. قدّموا دعماً عملياً قائماً على المهام

إدارة هجوم منشق أمرٌ فنيّ، ويزداد إنهماكاً مع استمرار الشخص المستهدف في حضوره العام. يستطيع الحلفاء تولّي مهام محدّدة تُخفّف عنه العبء من دون أن يضطرّ إلى البقاء متّصلاً بشكلٍ مستمرّ أو متفاعلاً عاطفياً مع المحتوى المُسيء. تشمل هذه المهام:

- توثيق الأدلّة على الإساءة عبر مختلف المنصّات والحسابات.
- متابعة منصّات أو وسوم أو حسابات معيّنة لرصد المستجدات، وتلخيص ما يحدث للشخص المستهدف بدلاً من إرسال لقطاتٍ مباشرة من المحتوى المُسيء.
- التعامل مع إجراءات الإبلاغ بموافقته، حتى لا يضطرّ هو إلى التعرّض المتكرّر للمحتوى الضارّ.
- إدارة الإشراف على الصفحات وحسابات الحملة والقنوات التنظيمية المشتركة: تصفية التعليقات وحظر الحسابات والردّ على الرسائل الواردة.
- المساعدة في صياغة الاتصالات والبيانات أو الردود عند الحاجة، لكن يجب أن يقرر الشخص المستهدف ما يُرسل ومتى.

3. قدّموا تضامناً ظاهراً

بالنسبة إلى قيادات الأحزاب ومديري الحملات ومسؤولي المنظمات: قدّموا دعماً ظاهراً عبر استجابة مؤسسية واضحة وسريعة تُركّز على استمرار الشخص المستهدف في عمله العام وتُعزّزه.

4. على الحلفاء أيضاً أن يعتنوا بأنفسهم

دعم شخصٍ يمرّ بعنفٍ رقميٍّ مستمرّ يستنزف العاطفة. الحلفاء الذين يستوعبون المحتوى المُسيء ويُدبرون المراسلات ويُقدّمون الدعم العاطفي قد يعيشون صدمتهم الخاصة وحالةً من الإنهاك. يكون الحليف أكثر فاعلية حين يحافظ على حدوده الشخصية ويتقاسم العبء مع آخرين في الشبكة ويلجأ إلى الدعم النفسي عند الحاجة.

10.2 ما الذي يتجنّبه الحلفاء

1. لا تُعيدوا نشر المحتوى المُسيء ولا تلتقطوا منه لقطات ولا تُضخّموه

من أكثر الأخطاء شيوعاً وأشدّها ضرراً أن يُعيد الحلفاء نشر المحتوى المُسيء لجذب الانتباه أو للتعبير عن الغضب. هذا الفعل يزيد مباشرةً انتشار الهجوم وظهوره.

2. لا تتصرّفوا من دون علم الشخص المستهدف وموافقته

التصرّف نيابةً عن شخصٍ مستهدفٍ يُقوّض استقلاليّته ويُربك استراتيجيّته وقد يُفاقم الوضع في بعض الحالات.

- لا تتواصلوا مع الصحفيين أو المنظمات القانونية أو الجهات الخارجية نيابةً عنه إلّا بعلمه وموافقته الصريحين.
- لا تُصدروا بياناتٍ علنية أو منشوراتٍ تضامنية ولا تنقلوا الحادثة إلى فضاءاتٍ جديدة من دون التحقق منه أولاً.
- لا تقرّروا نيابةً عنه كيف يجب أن يُؤمّر الهجوم أو يُوصف أو يُردّ عليه. هذا يشمل طبيعة الهجوم وتحديد هويّة المعتدين والتكهّن بدوافعهم. كلّ ذلك يحتاج إلى موافقته ومدخلاته.

3. لا تُقلّلوا من شأن الهجوم ولا تُبرّروه ولا تُعيدوا تأطيره

- الردود التي تهدف إلى الطمأنة قد تُقلّل من قدر مشاعر الشخص المستهدف وردود فعله تجاه الإساءة من دون قصد، فتُفاقم الأذى النفسي.
- ابتعدوا عن عباراتٍ مثل: «تجاهلوا الأمر»، أو «لا تعطيهما الانتباه الذي يريدونه»، أو «الأمر سيمرّ»، أو «هذا ما يحدث في السياسة». هذه العبارات مهما كانت نيتها حسنة تُقلّل من حجم الأذى الفعلي للعنف الرقمي المستمرّ وتُعيد عبء إدارته إلى عاتق الفرد المستهدف وحده.
 - لا تودحوا بأنّ سلوك الشخص نفسه أو حضوره العامّ أو تصريحاته هي ما يحتاج إلى تعديل لتخفيف الضرر. هذا شكّل من أشكال لوم الضحية شائع في الردود على العنف الرقمي وفؤؤد بشكلٍ خاصّ في السياقات السياسية حيث تتعرّض النساء وأفراد مجتمع الميم-عين أصلاً لضغوطٍ للحدّ من حضورهم العامّ.

4. لا تكشفوا الهوية ولا تُفصحوا عن معلومات ولا تنقلوها بلا موافقة

- في الهجمات التي تستهدف أفراد مجتمع الميم-عين أو في الحالات التي تتضمن مشاركة غير توافقية لصورٍ حميمة قد يكون لدى الحلفاء وصولٌ إلى معلوماتٍ حساسة عن هويّة الشخص المستهدف أو علاقاته أو حياته الخاصة. يجب التعامل مع هذه المعلومات بأقصى درجات الحذر.
- لا تُفصحوا عن التوجّه الجنسي للشخص أو هويّته الجندرية أو حالته العاطفية أو أيّ معلوماتٍ شخصية أخرى ولا تؤكّدوها ولا تناقشوها حتى في سياق الدفاع عنه.
 - لا تُشاركوا معلوماتٍ عن طبيعة هجومٍ يتضمّن صوراً حميمة أو فضحاً أو إساءاتٍ قائمة على الهوية خارج نطاق من يعلمون فعلاً ومن يحتاجون إلى المعرفة.
 - المعلومات المتعلقة بالتوجّه الجنسي والهوية والإفصاح عن صورٍ حميمة تُعرّض الأشخاص المستهدفين لمخاطر قانونية؛ إذ تُستخدم المادة 534 من قانون العقوبات اللبناني لتجريم المثلية الجنسية، كما تُعرّضهم لأضرارٍ اجتماعية تصل إلى جرائم «الشرف» بحق النساء.

5. لا تتعاملوا مع الوضع كفرصةٍ سياسية

- في فترات الانتخابات تتحوّل الهجمات على المرشّحات سريعاً إلى ورقةٍ سياسية مفيدة للمحيطين بهنّ — لجمع التبرّعات أو لتعزيز سرديّات الحملة أو لتحسين موقع الحلفاء أمام جمهورٍ معيّن. التصرّف على هذا الأساس من دون علم الشخص المستهدف وموافقته أمرٌ مؤذٍ مهما كانت النية.
- لا تؤمّروا الهجوم في المقام الأوّل على أنّه هجومٌ على الحزب أو الحملة أو القضية. سلامة الشخص المستهدف وتجربته تأتيان قبل أيّ سرديّة سياسية.
 - لا تفترضوا أنّ موافقة الشخص على بيان علني واحد أو على استخدام واحد لقصته تعني موافقته على كلّ ما يلي. طريقة الحديث عن تجربة الناجيات تتغيّر مع الوقت. تحقّقوا واسألوا ولا تفترضوا.

توجيهات لمشرفي الصفحات والمنصات المجتمعية والقائمين على الإشراف

يؤدي مشرفو الصفحات ومديرو المجموعات والقائمون على الإشراف على المحتوى الإلكتروني دوراً غالباً ما يُستهان به في أثناء الهجمات الرقمية. ليسوا مضيفين سلبين للمحتوى، بل صانعون فعليون لما تراه مجتمعاتهم وما يُضخم فيها وما يُطغى وما يُرَقَص. في الفترات السياسية المتوترة، تتوسّع حملات التحرش المنسّق والمعلومات المضلّة والهجمات القائمة على الفضح بسرعة كبيرة. كل قرار يتخذه مشرفو الصفحات والقائمون على الإشراف في هذه الفترات يحمل تبعات حقيقية على الأشخاص المستهدفين.

هذا القسم مخصّص لمن يديرون الفضاءات المجتمعية. يشمل ذلك صفحات الحملات وحسابات منظمات المناصرة ومنصات المجتمع المدني ومنتديات الدوائر الانتخابية وقنوات التواصل الحزبية وأي فضاء إلكتروني آخر فيه وظيفة إشراف. يُحدّد هذا القسم لماذا يهّم دور هؤلاء، وما الحدّ الأدنى من ممارسات عدم تضخيم المحتوى الضارّ، وكيف يكون الإشراف أكثر أماناً في الفترات المتوترة.

لماذا يهّم دور مشرفي الصفحات والقائمين على الإشراف

11.1

الإشراف على المحتوى ليس فعلاً مديداً. كل قرار يتخذه المشرف يُحدّد أي سلوك يُعتبر مقبولاً في الفضاء وأي ضرر يُسمح بانتشاره. لذا فإنّ القرارات كإبقاء تعليق أو حذفه، وإزالة منشور أو الإبقاء عليه، ووضع قواعد واضحة للمجتمع أو تركها مُبهمّة، تستحقّ تفكيراً جدياً في تبعاتها.

في الانتخابات وفترات الحراك السياسي المرتفع، تتحوّل صفحات المجتمعات إلى مواقع تنطلق منها الهجمات أو تُضخم فيها أو يتنازع بشأنها. التعليقات المُسيئة ونشر البيانات الشخصية دون إذن والشائعات والمحتوى القائم على الفضح لا تنشأ كلّها في المنصات العامة الكبرى. كثيرٌ منها يتنقل عبر صفحات المجتمعات المحلية ومجموعات الدردشة الحزبية والشبكات الأصغر. الانتشار الثانوي يُسبّب أحياناً ضرراً بقدر ضرر الهجوم الأصلي لأنّه يصل إلى جمهور يعرف الشخص المستهدف معرفةً شخصية أو مهنية. كما يُضفي على المحتوى مظهر المصادقية ويُجذّد الشخص من السيطرة على سرّيته داخل مجتمعه.

المشرفون الذين يسمحون بانتشار هذا المحتوى حتى بشكلٍ سلبيّ يصبحون جزءاً من آلية الهجوم. أمّا المشرفون الذين يتصرّفون بسرعة وتّساقٍ وشفافية فيقلّلون كثيراً من انتشار المحتوى الضارّ ويُرسلون رسالة واضحة لمجتمعهم بأنّ هذا السلوك لا يُحتفل.

الأمر بالغ الأهمية في الفضاءات المرتبطة بحملات سياسية أو أحزاب أو منظمات مجتمع مدني، حيث تعتمد ثقة المجتمع بالقيادة وسلامة الأشخاص الذين تخدمهم هذه المنظمات جزئياً على طريقة إدارة الفضاء الإلكتروني.

الحدّ الأدنى من ممارسات عدم تضخيم المحتوى

11.2

الممارسات التالية تمثّل المعيار الأساس لأيّ مشرف صفحة أو قائم على إشراف يتعلّق عمله بمحتوى سياسي أو مدني أو مرتبط بالمناصرة. تنطبق بشكلٍ خاص على من يديرون فضاءات تنضمّ إليها مرشّحات أو ناشطون/ات من مجتمع الميم-عين أو مدافعون/ات عن حقوق الإنسان، أو حيث يُناقش هؤلاء.

في ما يخص التعليقات والمحتوى المسيء

- احذفوا التعليقات التي تتضمن تهديدات أو شتائم أو معلومات تكشف بيانات شخص ما دون إذن أو لغة ذات طابع جنسي أو إساءات قائمة على الهوية موجّهة لأي فرد.
- لا تتركوا هذه التعليقات ظاهرة في انتظار البت في مدى انتهاكها لمعايير الصفحة: إذا كانت ضارّة بوضوح، تحرّكوا.
- لا تتفاعلوا علناً مع التعليقات المسيئة بطرق تزيد ظهورها، مثل اقتباسها في الرد، أو تثبيت ردّ يكرّر المحتوى الأصلي، أو مشاركتها بوصفها أمثلة على ما يَدان.
- طبّقوا معايير الإشراف بالتساق عبر الانتماءات السياسية والهويّات والمواضيع. الإشراف غير المتّسق يوحى بأنّ بعض أفراد المجتمع أقلّ حمايةً من غيرهم، خصوصاً حين تُحتفل الإساءة الموجّهة للنساء وأفراد مجتمع الميم-عين بينما يُزال محتوى آخر.

في ما يخص الشائعات والتسريبات والمحتوى القائم على الفضح

- لا تشاركوا ولا تُعيدوا نشر ولا تسمحوا بتداول محتوى يكشف معلومات شخصية عن أي فرد، بما في ذلك عنوان المنزل ومكان العمل وتفاصيل العائلة والتوجّه الجنسي والهويّة الجندرية.
- ينطبق ذلك أيضاً على المحتوى المؤمّر كأخبار أو ثرثرة أو تعليق سياسي أو شأن عام.
- تعاملوا مع الشائعات غير المؤكّدة عن الحياة الخاصة لشخص مستهدف كمحتوى ضار لا أسئلة مفتوحة للنقاش المجتمعي.
- استضافة هذا النقاش حتى من دون اتّخاذ موقف تُضخّم الضرر وتُعطيهِ منّة.
- إذا اتّضح أنّ محتوى منشوراً على الصفحة يتضمّن معلومات تكشف هويّة شخص ما دون إذن أو الفضح، احذفوه فوراً ولا تحفظوه ولا تُعيدوا نشره لأي غرض كان، بما في ذلك توثيق ما نُشر.

في ما يخص الإبلاغ والشفافية

- ضعوا آلية واضحة وميسّرة لأفراد المجتمع للإبلاغ عن المحتوى الضارّ إلى المشرفين واستجيبوا للبلغات في وقتٍ معقول (يمكن أن يكون ذلك عبر رابط في وصف الصفحة أو عبر رسائل خاصة موجّهة إلى حساباتٍ معيّنة للرد).
- حين تُزيلون محتوى، فكّروا في إصدار إشعارٍ موجز للمجتمع يُفيد بأنّ المحتوى أُزيل لانتهاكه معايير المجتمع، من دون تكرار المحتوى المُزال أو وصفه.
- احتفظوا بسجّلاتٍ داخلية لقرارات الإشراف خصوصاً في الفترات المتوتّرة؛ هذه السجّلات تُساعد في رصد أنماط الإساءة وتوثيقها عند الحاجة.

في ما يخص الوصول الإداري وأمان الحسابات

- راجعوا من يملكون صلاحياتٍ إدارية على الصفحة أو المنصة واسحبوا الصلاحيات ممّن لم يعد ناشطاً أو ممّن قد يكون حسابه قد تعرّض للاختراق أو ممّن تغيّر دوره داخل المنظمة.
- احرصوا على أن يبقى الوصول والنشر متمركزين في يد شخص واحد أو فريق تواصل صغير.
- استخدموا كلمات مرور قوية وفريدة وفعلّوا المصادقة الثنائية على كلّ الحسابات الإدارية.
- في فترة الانتخابات تزداد مخاطر اختراق الصفحات أو التسلّل إليها خصوصاً تلك المرتبطة بحملاتٍ أو منظماتٍ ناشطة سياسياً.
- اتّفقوا داخلياً على بروتوكول في حال اختراق حساب إداري، يُحدّد من يملك صلاحية سحب الوصول ومدى السرعة التي يمكن أن يحصل بها ذلك.

إشراف أكثر أماناً في الفترات المتوترة

11.3

الانتخابات والالتزامات السياسية وفترات الجدل السياسي المرتفع تخلق تحديات خاصة للإشراف. يزداد حجم المحتوى وتعلو رهانات كل قرار، وقد تستهدف جهات منسقة عمداً الفضاءات المجتمعية ضمن حملات أوسع للتحرش أو للتضليل. الإرشادات التالية مُصممة لتلك الظروف.

استبقوا التوتر وحضروا قبل بلوغ الذروة

- ضعوا معايير الإشراف قبل وقوع الهجوم. راجعوا توجيهات المجتمع وحدّثوها بحيث تتناول بوضوح التحرش ونشر البيانات الشخصية دون إذن والإساءة القائمة على الهوية ومشاركة المعلومات الشخصية.
- ثبّتوا توجيهات المجتمع بشكلٍ ظاهر بحيث يكون الأعضاء على دراية بالمعايير ولا يستطيعون ادّعاء الجهل بها لاحقاً.
- حدّدوا مسبقاً أيّ أعضاء الفريق يتولّى مسؤولية الإشراف وما هي صلاحياتهم وكيف تُتخذ القرارات بسرعة في حال ظهور محتوى ضارّ خارج ساعات العمل أو في خلال تصعيد متسارع.
- فكّروا في زيادة قدرة الإشراف مؤقتاً قبل الفترات التي يتوقّع فيها توتر.

تعرّفوا على بصمة الهجمات المنسقة

- الأنماط المعروفة للهجمات الرقمية المنسقة تشمل:
 - ارتفاعاً مفاجئاً في الحسابات الجديدة أو غير النشطة التي تتفاعل مع الصفحة.
 - تكرار العبارات نفسها أو الوسوم نفسها عبر تعليقاتٍ متعدّدة.
 - الإبلاغ الجماعي عن محتوى الصفحة.
 - الانتشار السريع لقطعة محدّدة من المحتوى كلقطة شاشة أو شائعة أو فيديو في فضاءاتٍ متعدّدة في الوقت نفسه.
- إذا رصدتم هذه الأنماط، لا تتعاملوا مع التعليقات الفردية وكأنّها مستقلة عن بعضها.
 - وثّقوا التحرش.
 - قيّدوا مؤقتاً من يستطيع التعليق أو النشر أو التفاعل مع الصفحة ريثما يجري تقييم الوضع.
- نّبّهوا الشخص المستهدف وفريقكم الأوسع إلى أنّ حملةً منسقة تبدو في طور الانتشار حتى يتّخذ كلّ منهم خطواته الوقائية.

أجبروا الظهور من دون نشر المحتوى الضارّ

- حين تُزيلون المحتوى الضارّ أو تردّون عليه، تجنّبوا أيّ فعلٍ يُنشئ ظهوراً جديداً للشخص المستهدف. يشمل ذلك:
 - كتابة منشوراتٍ علنية تصف طبيعة الهجوم بالتفصيل.
 - الإشارة إلى الشخص المستهدف في الردّ الإشرافي.
 - مشاركة لقطات شاشة لما نُشر حتى لو بهدف إظهار أنّه قد أُزيل.
- حين تتواصلون داخلياً بشأن حادثة سواء مع فريق الإشراف أو قيادة المنظمة أو المستشار القانوني، افعلوا ذلك عبر قناةٍ آمنة ومشفّرة من طرفي إلى طرف ولا تُحوّلوا المحتوى الضارّ نفسه ولا تشاركوه مع من لا يحتاج إلى رؤيته.
- اتّبهوا إلى أنّ إجراءات الإشراف ذاتها قد تتحوّل إلى هدفٍ للهجوم.
 - إزالة المحتوى قد تُثير اتّهاماتٍ بالرقابة أو الانحياز السياسي أو القمع خصوصاً في فترات النشاط السياسي المرتفع.
 - اعتمدوا معايير مجتمعية واضحة ومرئية للعامة صادرة قبل الحادثة.

ادعموا الأشخاص المستهدفين من دون السيطرة على وضعهم

- حين يُستهدف شخص مرتبط بالمجتمع من خلال منصّة بعينها أو في محيطها، ينبغي على المشرفين التواصل معه قبل أي إجراء علني.
- وثّقوا ما يحدث على المنصة بعناية (راجعوا القسم 12.4 قائمة التحقق للتوثيق)، واحرصوا على مشاركة هذا التوثيق مع الشخص المستهدف حتى يحتفظ بسجلّ الإساءة.

بعد انتهاء الفترات المتوتّرة

- أجروا مراجعةً داخلية موجزة لأداء الإشراف.
- ما القرارات التي اتخذت بسرعة وبشكل جيّد؟
- ما الذي استغرق وقتاً أطول من اللازم؟
- ما الثغرات التي ظهرت في معايير المجتمع أو في العمليات؟
- حدّثوا التوجيهات والبروتوكولات الداخلية بناءً على الدروس المُستفادة، حتى يكون المشرفون أكثر استعداداً للفترة المتوتّرة المقبلة.
- تواصلوا مع أعضاء فريق الإشراف الذين تعرّضوا لحدّ كبير من المحتوى الضارّ واحرصوا على أن يحصلوا على الدعم الذي يحتاجونه.

قوائم تحقق سريعة

تُتيح قوائم التحقق للمستخدمين/ات تحويل توجيهات الدليل إلى أدوات مرجعية سريعة وقابلة للتنفيذ. يمكن العودة إليها بسرعة تحت الضغط، أو في أثناء حادثٍ نشطة، أو استعداداً لفترة مرتفعة المخاطر كالانتخابات أو حملات المناصرة.

قائمة التحقق للاستعداد قبل التعرّض

12.1

- ☐ فغّلوا المصادقة الشّائبة على جميع الحسابات النشطة. أعطوا الأولوية للبريد الإلكتروني ووسائل التواصل الاجتماعي وأي حسابات مرتبطة بالحملة أو المنظمة.
- ☐ راجعوا أي الحسابات لا تزال نشطة وأغلقوا أو عطلوا ما لم تعودوا تستخدمونه.
- ☐ استخدموا كلمة مرور قوية وفريدة لكل حساب.
- ☐ راجعوا أي التطبيقات والخدمات الخارجية لديها وصول إلى حساباتكم واسحبوا الوصول من الحسابات التي لم تعودوا تستخدمونها أو لا تتعرّفون عليها.
- ☐ أنشئوا بريدًا إلكترونيًا منفصلاً للتواصل العام وتسجيلات الحملة، حمايةً لبريدكم الإلكتروني الأساسي.
- ☐ راجعوا إعدادات الخصوصية على جميع حسابات التواصل الاجتماعي النشطة.
- ☐ احذفوا عنوان المنزل ورقم الهاتف وموقعكم اليومي من جميع الملفّات الشخصية العامة والسير الذاتية المختصرة وأدلة المنصّات، أو قيّدوا الوصول إليها.
- ☐ حدّدوا أي معلومات شخصية متاحة للعامة وأين تظهر. ابحثوا عن اسمكم في غوغل وتحقّقوا ممّا إذا كان رقم هاتفكم وبريدكم الإلكتروني موجودين على الإنترنت.
- ☐ استخدموا تطبيق رسائل آمن ومشفّر من طرف إلى طرف للتواصل الحساس مع فريقكم والمقرّرين الموثوقين.
- ☐ أنشئوا أو فغّلوا صفحة حملة أو صفحة تنظيمية للتواصل العام، تفادياً لاستخدام الحسابات الشخصية في فترات الحضور المرتفع.
- ☐ حدّدوا شخصين على الأقلّ من شبكتكم المباشرة يعرفان وضعكم ويفهمان المخاطر المحتملة ووافقا على تقديم الدعم في حال وقوع حادث.
- ☐ احذفوا بيانات EXIF الوصفية من الصور قبل نشرها علناً، خصوصاً الصور الملتقطة في الفعاليات والاجتماعات والأنشطة الانتخابية أو في المنازل أو في أي موقع ترغبون في الإبقاء عليه خاصاً.

قائمة التحقق لفرز المخاطر

12.2

استخدموا هذه القائمة عند بداية أي حادثة أو عند الحاجة إلى إعادة تقييم وضع متطوّر. مؤشّر واحد قد لا يحدّد المستوى، لكنّ مزيجاً من عدّة إشارات في وضعٍ يبدو منخفض المستوى قد يدلّ على مخاطر أعلى ممّا تبدو عليه للوهلة الأولى. أعيدوا التقييم بهذه القائمة بانتظام مع تطوّر الوضع؛ مستويات المخاطر ليست ثابتة.

1. أسئلة تشخيصية سريعة

طبيعة الهجوم

- ☐ هل هذا تحرّش، أم العنف الرقمي، أم نشر للبيانات الشخصية دون إذن، أم فضح، أم انتحال هوية، أم تحرّش منسّق، أم مزيج من بعض هذه الأنواع أو كلّها؟
- ☐ هل تحدثت هجمات مختلفة في الوقت نفسه؟
- ☐ هل هي حادثة فردية، أم أنّها تكرّرت مع مرور الوقت؟

الموقع والانتشار

- ☐ هل يحدث الهجوم على منصّات عامة؟
- ☐ هل ينتشر عبر منصّات أو حسابات متعدّدة؟
- ☐ هل يحدث عبر الرسائل الخاصة، أو المجموعات المغلقة، أو التواصل المباشر؟
- ☐ هل يوجد ابتزاز أو تهديد بمشاركة محتوى خاص؟

نشر البيانات الشخصية دون إذن

- ☐ هل جرى نشر أو الإشارة علناً إلى رقم هاتف، أو عنوان منزل، أو مكان عمل، أو تفاصيل عائلية؟
- ☐ هل تعرّض محتوى خاص كالصور والرسائل والبيانات الشخصية للكشف؟
- ☐ هل تلقّيتكم مكالماتٍ أو رسائل مزعجة متكرّرة من أرقام مجهولة؟

التنسيق

- ☐ هل تنشر حسابات متعدّدة الرسائل أو المحتوى نفسه في الوقت نفسه؟
- ☐ هل يظهر المحتوى نفسه عبر منصّات مختلفة؟
- ☐ هل ثقة مؤشرات على حسابات آلية أو حسابات أنشئت حديثاً تعمل معاً؟
- ☐ هل ترتبط الحسابات بأفراد معروفين، أو فاعلين سياسيين، أو مجموعات منظّمة؟

التهديدات

- ☐ هل ثقة رسائل تتضمن لغةً توجي بالأذى الجسدي أو بالتهديد بالقتل؟
- ☐ هل ثقة إشاراتٍ إلى عنف جنسي؟
- ☐ هل ثقة تهديدات بالإضرار بالسمعة، أو الابتزاز، أو الفضح؟
- ☐ هل تهدف الرسائل إلى الترهيب أو إلى دفع الشخص إلى الانسحاب من الحياة العامة؟

التصعيد

- ☐ هل ازدادت وتيرة الهجمات أو حدّتها؟
- ☐ هل أصبحت اللهجة أكثر عنفاً أو تهديداً مع مرور الوقت؟
- ☐ هل ازدادت محاولات التهديد أو الابتزاز في تواترها؟

التأثير على الآخرين

- ☐ هل تُذكر أسماء أفراد من العائلة، أو الزملاء، أو المقرّبين في الهجمات؟
- ☐ هل يجري التواصل معهم مباشرةً أو استهدافهم؟
- ☐ هل بدأ أشخاص في دائرتكم المباشرة بتلقّي تحرّش؟

المخاطر خارج الإنترنت

- ☐ هل حاول أحد التواصل المباشر معكم أو تحديد موقعكم جسدياً؟
- ☐ هل ثقة إشاراتٍ إلى تحرّكاتكم، أو جدولكم، أو قُربكم الجسدي؟
- ☐ هل لاحظتم مؤشّراتٍ على مراقبةٍ خارج الإنترنت، أو تتبّع، أو اقتراب جسدي؟

2. حدّدوا مستوى المخاطر (في حال عدم اليقين، اعتبروه مرتفع المخاطر)

● منخفض الخطورة

تعرّض محدود، خطورة منخفضة، لا تهديد فوري

- ☐ حادثة فردية أو معزولة بحضور محدود
- ☐ لا تعرّض لمعلومات شخصية حسّاسة
- ☐ لا استهداف منشق عبر حسابات أو منصات متعدّدة
- ☐ لا تهديدات مباشرة أو ضمنية
- ☐ لا مؤشّرات على تصعيد
- ☐ لا انخراط لأفراد العائلة أو الزملاء

الإجراءات الفورية

- ☐ أوقفوا كلّ تواصل مع المعتدي واحظروه على جميع المنصّات التي يمكن أن يتمّ التواصل عبرها
- ☐ وثّقوا كلّ شيء
- ☐ استخدموا أدوات المنصة للحدّ من المحتوى المسيء أو للإبلاغ عنه وعن الحسابات
- ☐ راجعوا إعدادات الخصوصية الأساسية على الحسابات وأحكموها
- ☐ فغّلوا المصادقة الثنائية

● متوسط الخطورة

حضور متزايد، استمرارية، ومؤشّرات تصعيد ميّجرة

- ☐ تحرّش متكرّر أو مستمرّ
- ☐ محتوى يكتسب حضوراً أو ينتشر عبر منصات
- ☐ مؤشّرات ناشئة على التنسيق عبر حسابات متعدّدة
- ☐ كشف جزئي لمعلومات شخصية
- ☐ تهديدات موجودة، لكنّها ليست فورية ولا حادّة بعد
- ☐ زملاء أو مقرّبون بدأوا يتأثّرون

الإجراءات الفورية

- ☐ وثّقوا الأدلّة بشكلٍ منهجي
- ☐ ارصّدوا الأنماط المنسّقة: تشابه الرسائل، والتوقيات، ونشاط الحسابات
- ☐ قلّلوا الحضور العام: راجعوا المنشورات وعدّلوا إعدادات الجمهور وقبّلوا الإشارة والتعليقات
- ☐ تجنّبوا الإجراءات التي تُضخّم الأذى: لا تُعيدوا نشر المحتوى العدائي، أو تتفاعلوا مع المنشورات المسيئة، أو تجذبوا الانتباه إلى الوسوم أو الملقّات الضارّة
- ☐ نهبوا الجمهور والشبكات إلى الحسابات المزوّفة في حال انتحال الهوية

● مرتفع الخطورة

تهديدات جدّية، كشف بيانات شخصية، تنسيق، واحتمال أذى جسدي

- ☐ نشر بيانات شخصية دون إذن: عنوان منزل و/أو رقم هاتف و/أو مكان عمل و/أو موقع جري نشره علناً
- ☐ تهديدات مباشرة بالأذى الجسدي أو بالعنف الجنسي أو بالقتل
- ☐ حملات تحرّش منشق فيروسيّة أو تتصاعد بسرعة
- ☐ تهديدات بالكشف القسري عن الميل أو مشاركة غير توافقية لصورة حميمة
- ☐ الهجوم يمتدّ إلى أفراد العائلة أو الزملاء أو المقرّبين
- ☐ ابتزاز أو محاولات لإكراه الشخص على الانسحاب من الحياة العامة

الإجراءات الفورية: راجعوا القسم 12.3 قائمة التحقق للاستجابة للحوادث

3. خلاصة مستوى المخاطر

قارنوا وضعكم الحالي عبر كل مؤشر التقدير مكانه على مقياس المخاطر.

المؤشر	منخفض الخطورة	متوسط الخطورة	مرتفع الخطورة
الظهور	محدود	متنام	واسع ومنتشر
التحديات	لا يوجد	ضمنية أو ناشئة	مباشرة وذات مصداقية
البيانات الشخصية	غير مكشوفة	مكشوفة جزئياً	متداولة علناً
التنسيق	لا يوجد	مؤشرات مبكرة	مؤكد
تأثير الآخرين	لا يوجد	بدأ يظهر	نعم — استهداف فعلي
المخاطر خارج الإنترنت	لا يوجد	لا يوجد	قائمة أو وشيكة

أدنى خطورة أعلى خطورة

اقرأوا المؤشرات مجتمعة لا كل منها على حدة. مؤشر واحد قد يقع في مستوى المخاطر المنخفضة بينما يكون الوضع العام أعلى — فإذا أشارت عدة مؤشرات إلى مستوى متوسط أو مرتفع، فتعاملوا مع الوضع على المستوى الأعلى.

قائمة التحقق للاستجابة للحوادث

12.3

1. التوقّف والتقييم

☐	ابتعدوا عن الشاشة. لا تردّوا علناً أو بشكل خاص على الهجوم وأنتم تحت ضغط نفسي. لا تتفاعلوا مع المعتدين.
☐	حدّدوا الشكل الأساسي للهجوم. هل يُستخدم أكثر من تكتيك في الوقت نفسه؟
☐	احفظوا الرسائل والمحتوى والأدلة. لا تحذفوها، ولا تحذفوا الحسابات أو تُلغوا تفعيلها.
☐	وثّقوا كل المحتوى الفسّيء واحفظوه بشكل آمن ومرتبّ زمنياً.
☐	اطلبوا من شخص موثوق أن يتولّى رصد المحتوى الفسّيء بدلاً منكم.
☐	توقّفوا عن نشر المواقع الجغرافية الآنية أو القصص أو المنشورات.
☐	نوّعوا روتينكم وأنماط حركتكم قدر الإمكان تحسباً للمخاطر خارج الإنترنت.
☐	اصطحبوا شخصاً موثقاً معكم في الاجتماعات والفعاليات الشخصية.

2. تأمين الحسابات

☐	غيّروا كلمات المرور فوراً على جميع الحسابات الأساسية: البريد الإلكتروني ووسائل التواصل الاجتماعي والحسابات المصرفية والحسابات المرتبطة بالحملة.
☐	راجعوا الجلسات النشطة وسجّلوا الخروج عن بُعد من جميع المتصفّحات والأجهزة.
☐	عظّلوا مشاركة الموقع اللحظي على الأجهزة والتطبيقات. أوقفوا مشاركة الـ GPS.
☐	عظّلوا خاصية تحديد الموقع الجغرافي على الكاميرا وعلى تطبيقات التواصل الاجتماعي.
☐	راجعوا الحسابات المشتركة. احذفوا الوصول غير الضروري إلى التخزين السحابي المشترك والتقاويم ومزامنة الأجهزة.
☐	حدّثوا أنظمة التشغيل والتطبيقات وبرامج الأمان إلى أحدث إصداراتها المتاحة.

3. تفعيل شبكات الدعم الموثوقة

☐	أخبروا شخصاً موثقاً واحداً على الأقل بالوضع (صديقاً أو زميلاً أو أحد أفراد العائلة).
☐	اطلبوا من شبكتكم الموثوقة مساعدةً محدّدة: رصد المحتوى وجمع الأدلة وتوثيقها أو إدارة المراسلات.
☐	أبلغوا فريق الحملة أو زملاءكم في المنظمة أو صاحب العمل.
☐	تواصلوا مع منظمة أمن رقمي إذا اشتبهتم في اختراق حساب أو تسلّل إلى الجهاز أو هجمات تقنية معقّدة.
☐	تواصلوا مع منظمة قانونية أو منظمة لحقوق الإنسان عند تحديد تهديدات جذية بالكشف القسري عن الميل أو نشر البيانات دون إذن أو التشهير.
☐	تواصلوا مع مقدّم دعم نفسي-اجتماعي إذا تسبّب الهجوم بضائقة نفسية أو خوف أو إنهاك. راجعوا القسم 9.4 قائمة الموارد للمنظمات ذات الصلة.

4. اختاروا مسار الاستجابة (بناءً على مستوى المخاطر)

☐	الرصد من دون انخراط علني (للهجمات منخفضة المخاطر):
☐	استمرّوا في التوثيق والرصد بدعم من شبكتكم.
☐	احظروا الحسابات الفسّية وقيدوها.
☐	أبلغوا المنضّات عن المحتوى عند الاقتضاء.
☐	أعيدوا التقييم بانتظام بحثاً عن مؤشّرات التصاعد.
☐	التصعيد إلى دعم تنظيمي أو قانوني أو أممي (للمخاطر المتوسطة إلى المرتفعة):
☐	أبلغوا أصحاب العمل والمنظمات وفرق الحملات وأفراد العائلة.
☐	اطلبوا دعماً آمناً رقمياً.
☐	تواصلوا مع منظمات قانونية أو منظمات حقوق إنسان.
☐	أبلغوا السلطات حيثما كان ذلك آمناً ومناسباً.
☐	إصدار توضيح علني محدود (في حالات التضليل المنشق والادّعاءات الكاذبة وانتحال الهوية):
☐	لا تتفاعلوا مباشرة مع المعتدين ولا تُعيدوا نشر المحتوى الضارّ.
☐	لا تردّوا انفعالياً أو تحت الضغط.
☐	ركّزوا على تصحيح المعلومات الكاذبة ببلغ واقعية وموجزة وغير تفاعلية.
☐	أعيدوا تقييم الوضع بانتظام.

قائمة التحقق للتوثيق

12.4

وتُقوّم قبل الإبلاغ، فقد يُزال المحتوى فور تقديم البلاغ. اعملوا على كلّ فئة أدناه وضعوا علامةً على ما جرى توثيقه.

لقطات الشاشة

☐	المنشورات والتعليقات والردود والقصص المُسيئة
☐	الرسائل الخاصة أو الجماعية
☐	الصور والفيديوهات والملاحظات الصوتية أو البثّ المباشر المتضمّن لمحتوى ضارّ
☐	يجب أن يكون اسم المستخدم والتاريخ والوقت والمنصّة والمحتوى الكامل ظاهراً في كلّ لقطة شاشة
☐	المحتوى الذي يُعرض مرّة واحدة أو الذي يختفي يجب تصويره عبر جهازٍ ثانٍ
☐	التهديدات بالأذى الجسدي أو بالعنف
☐	استهداف أفراد العائلة أو الأصدقاء أو الزملاء
☐	الصور المُلتقطة من دون موافقتكم

الروابط وعناوين URL

☐	الرابط المباشر لكلّ منشور أو ملف شخصي أو حساب أو قناة أو مجموعة مُسيئة
☐	توثيق منفصل لكلّ منصّة يظهر فيها المحتوى

تفاصيل الحسابات

☐	أسماء المستخدمين والأسماء الظاهرة ومعرّفات الحسابات لجميع الحسابات المعنيةّة
☐	الصور الشخصية
☐	عدد المتابعين
☐	تواريخ إنشاء الحسابات
☐	أيّ انتماء حزبي ظاهر أو معلومات تعريفية

سجّل الحادثة

☐	تاريخ ووقت بدء الهجوم وعلى أيّ منصّة
☐	تاريخ ووقت تحديد التهديدات
☐	تاريخ ووقت مشاركة المعلومات الشخصية
☐	تاريخ ووقت انتشار التحرّش إلى منضّاتٍ أو جماهيرٍ إضافية
☐	أيّ نقاط تصعيد أخرى جرى رصدها لحظة وقوعها

المكالمات والتواصل المباشر

☐	الأرقام المجهولة التي اتّصلت أو راسلت بشكلٍ مزعج
☐	تسجيل تواتر المكالمات والرسائل
☐	تسجيلات الملاحظات الصوتية

تخزين الأدلّة والتعامل معها

☐	جميع الأدلّة محفوظة في مجلّد آمن وخاصّ
☐	نسخة احتياطية على قرص خارجي أو على تخزينٍ مُشفّر
☐	مرتبّة زمنياً
☐	محفوظة حتى إن لم يُحسم بعد قرار الإبلاغ

قائمة التحقق للمشرفين/ات على المحتوى ومديري الصفحات

12.5

للاستخدام من قبل أي شخص يدير صفحة مجتمعية أو حساب حملة أو منصة مدنية، خصوصاً في الانتخابات والفترات السياسية الحساسة.

☐	وثّقوا المحتوى المُسيء.
☐	احذفوا التعليقات التي تتضمن محتوى مُسيئاً.
☐	لا تقبّسوا المعتدين، ولا تُبلّغوا عنهم، ولا تنخرطوا معهم علناً.
☐	لا تُعيدوا نشر، ولا تُشاركوا، ولا تسمحوا بتداول المحتوى الضار.
☐	طبّقوا معايير الإشراف بالتساقٍ عبر جميع الهويات والانتماءات والمواضيع.
☐	تعاملوا مع الشائعات غير المؤكّدة عن حياة شخص ما الخاصة بوصفها محتوى ضارّاً لا مواضعاً للنقاش.
☐	احرصوا على أن تكون لدى أفراد المجتمع طريقة واضحة وميسّرة للإبلاغ عن المحتوى الضارّ إلى المشرفين.
☐	راجعوا وحدّثوا قائمة من يملكون الوصول الإداري.
☐	احرصوا على تمركز مسؤولية النشر لدى شخص واحد أو فريق صغير موثوق.
☐	استخدموا كلمات مرور قويّة وفريدة وفعلوا المصادقة الثنائية على جميع الحسابات الإدارية.

القسم 13

13

ملاحظات ختامية وموارد رئيسية

الخلاصات الجوهرية

13.1

الهجمات الرقمية في الفترات السياسية الحساسة والانتخابات مُصمّمة لتقييد المشاركة العامة وتستهدف على نحوٍ غير متكافئ النساء وأفراد مجتمع الميم-عين. حضورهم في الحياة السياسية يتحدّى المعايير الاجتماعية الراسخة ويترك ديناميكيات السلطة القائمة ويدفع باتجاه تغييراتٍ تقاومها الجهات المحافظة والأحزاب السياسية المهيمنة. لذلك يُستخدم العنف الرقمي لمعاقبتهن على هذا الحضور والانخراط. ضُقم هذا الدليل استجابةً لهذا الواقع؛ هدفه أن يُقدّم أدواتٍ عملية لمشاركة أكثر أماناً، حتى يبقى من يواجهون عنفاً إلكترونياً مستهدفين من خطرٍ في الحياة السياسية والمدنية من دون أن يُجبروا على الانسحاب التام.

بمجرّد تحديد العنف الرقمي، ينبغي على الأشخاص المستهدفين وشبكة دعمهم التوقّف قبل التحرّك. قيّموا الوضع وحدّدوا نوع الهجوم وانتشاره ومستوى مخاطره ومدى تنسيقه وما إذا كان يتصاعد. التصرّف تحت الضغط من دون هذا التقييم قد يُضخّم الأذى من دون قصد. وثّقوا أدلّة الهجمات الرقمية فوراً حتى إن لم تكونوا قد قرّرت بعد الإبلاغ عن الحادثة. المحتوى يختفي بسرعة لحظة تفعيل مراجعةٍ على المنصة أو تعطيل حساب. حفظ لقطات الشاشة والروابط وتفاصيل الحسابات والرسائل التهديدية أمرٌ جوهري.

مستويات مخاطر الهجمات الرقمية ليست ثابتة. تتطور الأوضاع بسرعة، خصوصاً في الحالات السياسية النشطة. لذلك من المهم إعادة تقييم الوضع بانتظام وتحديث استراتيجيات الاستجابة وتكييفها مع تغيّر الظروف. بحسب مستوى المخاطر، فإنّ الاستمرار في الانخراط قد يُضخّم الأثر على السلامة الجسدية والنفسية ويدفع الأشخاص المستهدفين إلى تقليل الحضور. لكنّ الحدّ من الحضور ليس انسحاباً من الحياة العامة. يدفع هذا الدليل باتجاه تعديلات مؤقتة على الظهور واستخدام المنصات وعادات التواصل تُعطي الأولوية للسلامة من دون أن تُلغي المشاركة. التخطيط للسلامة يهدف دائماً إلى إبقاء الناس منخرطين قدر الإمكان وفق شروطهم وبالإيقاع الذي يتحكمون به. الحملات الرقمية المنسقة لا ينبغي مواجهتها وحدنا. المقربون الموثوقون والحلفاء ودعم الإشراف وشبكات الأقران والعائلة والأصدقاء يستطيعون المساعدة في إدارة الهجوم وجمع الأدلة ودعم الصحة النفسية للأشخاص المستهدفين. تحديد شبكة الدعم وتجهيزها قبل وقوع الحادثة استراتيجية حماية جوهرية.

الإبلاغ عبر المنصات والقنوات الرسمية للدولة أدوات تحمل حدوداً حقيقية وفي السياق اللبناني تحمل مخاطر جسيمة. الإبلاغ عبر المنصات لا يضمن إزالة المحتوى الضارّ ولا يحمي من التهديدات الجسدية ولا يستطيع التصديّ للإساءة المنسقة عبر المنصات المتعدّدة. لكنّه قد يُساعد في الحدّ من الأذى والظهور وينبغي استخدامه إلى جانب تدابير سلامة أخرى. المؤسسات الرسمية، بما فيها وحدة الجرائم المعلوماتية في قوى الأمن الداخلي، قد تجعل الشكاوى الرسمية خطراً بدل أن تكون حماية، بحسب من يقف خلف الهجوم وهويّة الشخص المُهاجم. الأمر إشكاليّ بشكل خاصّ للمدافعين/ات من مجتمع الميم-عين. ينبغي التفكير في الإبلاغ بعناية والمضيّ به فقط حيث يكون آمناً ومناسباً.

لن تُلغي الأدوات الواردة في هذا الدليل هذه المخاطر. لكنّها حين تُستخدم باتّساق وعناية وبشكل جماعيّ تُقلّل الأذى وتدعم استمرار الانخراط وتمنع العنف الرقمي من إعاقه المشاركة العامة.

روابط الموارد الرئيسية

13.2

— أدلة للإبلاغ عبر المنصات

- TikTok
- Facebook
- Instagram
- X / Twitter
- WhatsApp

— أدلة للحماية على الإنترنت

- SMEX – كيف تستطيع النساء حماية أنفسهنّ على الإنترنت؟
- UNHCR – الاستجابة للأذى على الإنترنت وطلب المساعدة
- UNFPA – ورقة إرشادية حول الإبلاغ عن العنف الرقمي: دليل مرجعي عملي للصحفيين/ات والإعلام

جهات اتصال مفيدة

المفكرة القانونية	+961 1 383 606	حلم	+961 81 478 450
CLDH	+961 1 24 00 23	موزاييك	+961 76 945 445
أبعاد	+961 81 788 178	Proud	+961 76 608 205
RDFL	+961 71 500 808	سمكس	+961 81 633 133
Access Now	+1 (888) 414 0100	إمبرايس	1564

المراجع

المراجع

المراجع مرقمة بحسب ترتيب ورودها لأوّل مرّة في النّص. انقرّوا على أيّ رقم [N] في المتنّ للانتقال إلى المرجع المقابل أدناه.

Skeyes Media (2023, March). Representative of UN Women: Online Bullying discourages women in Lebanon from engaging in politics and skeyesmedia.org:running in elections. Retrieved from [1]

[fe-](https://fe-male.org/archives/13653) :Fe-male (2021, June). Online Violence Against Women Human Rights Defenders in the MENA: Experiences and Perceptions. Retrieved from [2]

Daraj Media (2024, November). Biased Algorithms: How Digital Platforms Reinforce Abuse Against Female Politicians in Lebanon. Retrieved [3]

Human Rights Watch (2023, September). Lebanon: Attack on Freedoms Targets LGBTI People. Repressive legislation; unlawful crackdown. hrw.org. Retrieved from [4]

HuMENA for Human Rights and Civic Engagement (2024). A Report on the Legal and Social Situation of the LGBTQI+ Community in the Middle humena.org :East and North Africa Region and its Radical Transformation Between 2020 and 2023 — Lebanon as a Model. Retrieved from [5]

amnesty.org :Amnesty International. Online Violence. Retrieved from [6]

:UN Women (2024, September). Technology Facilitated Gender-Based Violence: Developing a shared research agenda. Retrieved from [7]

unfpa.org :UNFPA (2024, December). An infographic guide to Technology-Facilitated Gender-Based Violence. Retrieved from [8]

icfj.org :New Research Illuminates Escalating Online Violence on Musk’s Twitter. International Center for Journalists (2023, July). Retrieved from [9]

للمطالعة الإضافية

للمطالعة الإضافية

مصادر إضافية أسهمت في البحث الذي يقوم عليه هذا الدليل، مُدرّجة هنا للقراء والقارئات الراغبين/ات في التعمّق. هذه المواد غير مُستشوّج بها داخل المتنّ.

- smex.org :SMEX (2024, March). 80% of Women in Lebanon Face Digital Violence. Retrieved from
- UN Women (2025, March). Shaping Perceptions: Media influence on women's political participation during and beyond elections in lebanon.unwomen.org :Lebanon. Retrieved from
- maharatfoundation.org :Maharat (2022, August). Media and Gender Monitoring of the 2022 Elections VAWP. Retrieved from
- arabnews.jp :Arab News (2022, April). Lebanese female candidates stand up to Hezbollah, are disowned by families. Retrieved from
- unfpa.org/TFGBV :UNFPA. Technology-facilitated Gender Based Violence: A Growing Threat. Retrieved from
- docs.un.org/en/A/HRC/44/52 :Human Rights Council (2020). Combating Violence Against Women Journalists. Retrieved from

ابقوا بأمان. وابقوا منخرطين.

لن تُلغى الأدوات الواردة في هذا الدليل هذه المخاطر. لكنّها حين تُستخدم بالتساق وعناية وبشكل جماعي، تُقلّص الأذى، وتدعم استمرار الانخراط، وتمنع العنف الرقمي من إعاقة المشاركة العامة.

لبنان: lebanon@humena.org

عام: info@humena.org

الموقع: humena.org

المناصرة: advocacy@humena.org



HuMENA For Human Rights and Civic Engagement
HuMENA pour les Droits de l'Homme et l'Engagement Civique
هيومنينا لحقوق الإنسان والمشاركة المدنية



INNOVATION
FOR CHANGE
MIDDLE EAST & NORTH AFRICA



CIVICUS



Digital Democracy
Initiative