INSI

الدفاع الرقمي

إدارة الإساءة الإلكترونية داخل غرف الأخبار وخارجها

JOURNALISM | SAFETY | RESPONSIBILITY | COMMUNITY

جَدْوَل مُحْتَوَياتٍ

مقدمة

يواجه قطاع الإعلام موجةً متواصلة من المضايقات الإلكترونية التي تستهدف الصحافيين، بدءًا من الجهات الحكومية وشبكات الجريمة المنظمة وصولاً إلى الروبوتات وأفراد الجمهور الذين يشجعهم على ذلك إمكانية إخفاء الهوية. وقد اصبح خطاب الكراهية والتضليل الإعلامي والتهديدات بالعنف الجسدي واقعاً يومياً يعيشه العديد من الزملاء، يُجبر بعضهم على ترك المهنة، بينما يعاني آخرون من أذىً نفسي طويل الأمد، في وقتٍ تشتد فيه الحاجة إلى تغطية إعلامية مستقلة ومعمقة أكثر من أي وقت مضى.

ندرك جميعاً أن احتواء العنف الرقمي أمرٌ صعب. لكن الواضح أن الصحافيين يتوقعون من مشغليهم أن يتحملوا مسؤولياتهم قبل الهجمات والمضايقات الالكترونية وأثناءها وبعدها، مقدمين الدعم، بل ومتخذين إجراءات ملموسة ايضاً.

منذ عام ٢٠٢٠، تجتمع المنظمات الأعضاء في المعهد الدولي لسلامة الأخبار (INSI) لتبادل المناهج والدروس المستفادة. وقد دعمت هذه المنظمات مبادرتي «جوجل نيوز» و«فيسبوك» وشاركت في مراحلها الأولى ، ونحن نثمن عالياً مساهمتها.

هذا الدليل، الذي كتبه مايك كريستي، أحد المساهمين الرئيسيين في تلك الجهود، لصالح المعهد الدولي لسلامة الأخبار (INSI)، يستند إلى تلك الحوارات وما تلاها. وبصفته رئيساً عالمياً للسلامة في وكالة «رويترز»، ساهم كريستي في وضع معايير حماية المؤسسات الإخبارية لموظفيها في مواجهة التهديدات الجسدية والرقمية والنفسية. وكان لعمله دورٌ محوري في صياغة أفضل الممارسات على مستوى قطاع الإعلام.

تم تصميم هذا الدليل لمساعدة مسؤولي غرف الأخبار، العاملين في هيئات التحرير والأمن والموارد البشرية، لإنشاء إطار عملي من أجل التخفيف من تأثير الإساءة عبر الإنترنت والاستعداد إذا ما تصاعدت التهديدات الرقمية إلى خطر حقيقي على أرض الواقع.

لا شك أن لكل غرفة أخبار ملف خاص وآليات وموارد خاصة لمواجهة المخاطر. ولكن لا ينبغي لها أن تكافح العنف الرقمي بمفردها. فالتعاون على مستوى قطاع الإعلام، من خلال التعاون مع منصات في مجال الإنفاذ والمساءلة، ومع الحكومات في مجال التنظيم الهادف، سيُحدث أثراً أكبر من الجهود المنفردة. يشجع المعهد الدولي لسلامة الأخبار (INSI) جميع أعضائه على المشاركة الفعالة في هذه المبادرات المشتركة، وترسيخ روح الصمود الجماعي لاستجابة غرف الأخبار للمخاطر الالكترونية.

نُدرك أن العديد من غرف الأخبار على إلمام تام بحجم وطبيعة الإساءة الإلكترونية، ولكن الوقت المتاح لديها لمواجهة المخاطر الالكترونية قليل. لذلك، يبدأ هذا الدليل بالتدابير الأكثر إلحاحاً وقابلية للتنفيذ. ويستهل بإطار عملٍ عمليٍّ للتصدي للتحرش الرقمي، وهو مُوجّهٌ تحديداً إلى المدراء المسؤولين عن سلامة الموظفين ودعمهم، ثم ينتقل إلى السياق والخلفية الأوسع.

في ملاحق هذا الدليل، توجد قوائم مرجعية تغطي استراتيجيات التخفيف الرئيسية، بما في ذلك التوثيق الذاتي وتخطيط الاستجابة. نأمل أن يكون هذا الدليل مرجعاً مفيداً وسهل المنال للصحافيين والمدراء وخبراء السلامة على حدٍ سواء.

التدابير الوقائية الاستباقية

اليوم، في عالمنا المتصل بشبكة الإنترنت، يواجه الصحافيون مخاطر متزايدة، إذ يستغل المهاجمون الأجهزة المتصلة بالسحابة الإلكترونية والبيانات المشتركة عبر المنصات. يُعدّ التهديد المبهم مُقلقاً ولكن عندما يتضمن التهديد اسم مدرسة طفل أو صورة غرفة نوم نُشرت على الإنترنت من قِبل موقع عقارات، يُصبح الخطر أشدّ وطأةً. لذا، يُعدّ التخطيط الاستباقي بالغ الأهمية لضمان جاهزية غرف الأخبار. فيما يلي بعض التدابير الوقائية الاستباقية الواجب اتخاذها:

١. تحديد المشكلة

قم بإجراء استطلاع رأي في غرف الأخبار لفهم مدى ضخامة مشكلة التحرش الإلكتروني والإساءة المرتبطة به في مؤسستك الإخبارية. احرص على استطلاع آراء النساء والصحافيات من الأقليات، فهنّ الأكثر تضرراً من الإساءة الإلكترونية.

٢. توفير التدريب

قم بتضمين معلومات أساسية حول التحرش الإلكتروني وآثاره وطرق استجابة المؤسسة في جميع دورات التدريب الخاصة بالبيئات المعادية وأمن المعلومات. كما يمكن تنظيم ورش عمل خاصة تركز حصرياً على التحرش الإلكتروني.

٣. إنشاء قنوات للإبلاغ

قم بتعريف الموظفين بقنوات الاتصال المتاحة للإبلاغ عن التحرش الإلكتروني وانشرها لهم، ولا سيما التحرش الالكتروني عبر الرسائل الشخصية أو وسائل التواصل الاجتماعي. فكّر في إنشاء قناة للصحافيين لمشاركة تجاربهم مع التحرش الإلكتروني، مما قد يُحدد الاتجاهات الناشئة ويتيح لهم فرصةً لدعم بعضهم البعض. يمكن أن يشمل ذلك قناة Teams أو Slack، أو حتى البريد الالكتروني.

تأكد دائماً من أن فريق السلامة التحريرية على دراية مسبقة بأي بلاغ قد يؤدي الى إطلاق حملة إلكترونية ضد المؤسسة، بدلاً من انتظار التداعيات.

٤. التحقق الذاتي من المعلومات

اطلب من الصحافيين إجراء تمارين أساسية للتحقق الذاتي من المعلومات لمعرفة مقدار المعلومات الحساسة التي قد تُكتشف على الإنترنت. من المستحيل محو كل ما تراكم من معلومات على مدى سنوات من الاستخدام الرقمي لكن يمكن التقليل من المخاطر. على سبيل المثال، سيظهر عنوان أي شخص يملك عقاراً في بلد معَين في السجلات العامة. ولكن قد تتسرب المعلومات عبر حسابات على مواقع التواصل الاجتماعي التي لم يتم ضبط إعدادات الخصوصية فيها بشكل صحيح. لذا من الضرورة بمكان تحديث إعدادات الخصوصية في منصات التواصل الاجتماعي وحذف المعلومات القديمة وغير الضرورية. يُنصح بإدراج هذا ضمن عملية اعداد الموظفين الجدد.

٥. إجراء أبحاث معمقة حول الثغرات الرقمية

قم بإجراء بحث معمق حول الثغرات الإلكترونية للصحافيين البارزين والعاملين في مشاريع حساسة. قد تتمكن إدارات أمن المعلومات وإدارة المخاطر من القيام بذلك، أو يمكن الاستعانة بشركات خارجية متخصصة.

٦. استخدام خدمات الحذف عبر الإنترنت

قم بإرسال طلبات إلغاء الاشتراك التلقائية إلى وسطاء البيانات (الشركات الوسيطة) الذين يجمعون معلومات شخصية عن المستهلكين ويبيعونها. يمكن ان يتم ذلك باستخدام خدمات الحذف الإلكترونية مثل DeleteMe. ومع أن هذه الخدمة غير متوفرة في جميع الدول، إلا أنه يُنصح الاشتراك في خدمة على مستوى المؤسسات لغرف الأخبار أو الحصول على حسابات فردية. قد لا تعالج هذه الخدمات المصدر الأصلي للمعلومات التي يتم جمعها وبيعها، ولكنها قد تساعد في الحد من انتشارها.

٧. استخدام خدمات مراقبة التهديدات

تشترك العديد من المؤسسات الإعلامية في خدمات مراقبة العلامات التجارية للكشف عن انتهاكات حقوق النشر، والمواقع والحسابات المزيفة، أو التقارير والهجمات التي قد تضر بسمعة المؤسسة. كما تتوفر خدمات مماثلة لرصد التهديدات الأمنية التي تواجهها المؤسسات الإخبارية، والتهديدات الإلكترونية التي يتعرض لها الصحافيون، بعض هذه الخدمات تقوم بمراقبة الأنشطة في نطاق «الويب المظلم» dark web و«الويب العميق» deep web مثل مجموعات الدردشة على «تيليجرام».

٨. حذف المشاركات والمنشورات القديمة

يُنصح تنقيح التعليقات العامة الصادرة أيام الشباب الأكثر تهوراً إذا كانت قد تُعرّض سلامة الصحافي أو نزاهته للخطر. فالآراء السياسية، حتى لو لم تعد مُعتنقة، قد تمنع الصحافيين من تغطية الحملات الانتخابية على سبيل المثال. كما أن الصور والمشاركات المثيرة للجدل مجتمعيا قد تُشكّل مشكلة أمنية إذا كان الصحافي يتعامل مع مجموعات محافظة للغاية. يُنصح بإدراج هذه التعليمات ضمن عملية اعداد الموظفين الجدد.

٩. ملفات شخصية ذات تفاصيل قليلة

قد يكون وجه المراسل التلفزيوني المبتسم جزءاً مهماً من علامته التجارية، ولكن هل يحتاج مراسل الأخبار المالية الاستقصائي إلى نشر صورة شخصية على ملفه الشخصي «البروفايل»؟

يمكن للمهاجمين استخدام صور الملف الشخصي لتتبع الصحافيين عبر برامج التعرف على الوجوه. لذا، يُنصح تجنب نشر الصور الواضحة وتفاصيل الحياة الخاصة. وتزداد خطورة هذا الأمر لدى الصحافيات اللواتي يتعرضن للإساءة عبر الإنترنت أكثر بكثير من الرجال.

١٠. الفصل بين الحياة الخاصة والمهنية

يُنصح الفصل التام بين الحياة الخاصة والمهنية على الإنترنت من خلال إنشاء حسابات منفصلة، بحيث تقتصر الملفات الخاصة على الأصدقاء والعائلة، وأن تكون محمية بإعدادات خصوصية قوية مغلقة، وخالية تماماً من التواصل مع المصادر الصحافية والزملاء. اما الملفات المهنية، فيجب أن تحتوى على حد أدنى من المعلومات الشخصية، وأن تركز على العمل، وأن تراعي عدم نشر أية معلومات يمكن استغلالها ضد الصحافي أو المؤسسة الإعلامية.

١١. التدريب على الظهور العلني

من الأهمية بمكان تدريب الصحافيين على مهارات التعامل مع الجمهور والظهور العلني، فغالباً ما تحاول جماعات اليمين من الأهمية بمكان تدريب الصحافيين على مهارات التعامل مع الجمهور والظهور العلني، فغالباً ما تحاول جماعات اليمين المتطرف إيقاع الصحافيين في فخ الإدلاء بتعليقات محرجة أو مسيئة، وذلك بطرح أسئلة استفزازية عليهم علناً ثم نشر إجاباتهم على الإنترنت. فيما يدّعي آخرون بأن لديهم معلومات حصرية يقدمونها للصحافيين بهدف الحصول على أدلة او محادثات تشير الى تحيز الصحافيين حول قضية ما، الأمر الذي قد يستغله هؤلاء المدّعين ضد الصحافيين مما يضعف مصداقيتهم أمام الجمهور.

١٢. تحديد الأشخاص أو المجموعات الأكثر عرضة للخطر

قد يحتاج بعض الصحافيين إلى تدريب أو دعم إضافي، مثل:

- المراسلون السياسيون ومدققو الحقائق بشكل عام.
- العاملون في البلدان التي استخدمت الدولة أو السلطات الحاكمة فيها التحرش الإلكتروني كسلاح.
- النساء، وصحافيو الأقليات، ومثليي الجنس ومزدوجو التوجه الجنسي والمتحولون جنسياً (مجتمع الميم).
- الصحافيون الذين يتمتعون بحضور بارز على الإنترنت، والذين تعرضوا لانتقادات علنية من زعماء أو قادة سياسيين، والذين قاموا بتغطية بؤر التوتر الجيوسياسية التي استقطبت الرأي العام وأثارت انقساماً حاداً.

١٣. إدارة التعليقات

من أكبر التحديات التي تواجهها المؤسسات الإعلامية، كيفية الحفاظ على سلامة الحوار الإلكتروني وتهذيبه في التعليقات، الأمر الذي يتطلب موارد مخصصة. بعض المؤسسات الإخبارية، ببساطة تُغلق التعليقات، بينما تستخدم أخرى مزيجاً من أدوات الذكاء الاصطناعي.

الجدير ذكره أنه يجب إدارة ومراقبة التعليقات المسيئة الموجهة للمؤسسة وليس الأفراد فحسب، لاحتمال احتوائها على تهديدات جسدية مبطنة لصحافي بعينه.

١٤. إنشاء فريق استجابة متعدد الأقسام

قد تشمل الاستجابة للتحرش الإلكتروني الشديد إدارات مختلفة. وعليه، يجب المبادرة الى التنسيق المسبق لضمان جاهزية استجابة شاملة. ويُنصح تشكيل فريق عمل أو مجموعة عمل لإدارة الحوادث الكبرى، والتي تشمل:

- **إدارة التحرير**: اتخاذ القرارات بشأن نقل الصحافيين إلى مكان أكثر أماناً، أو توظيف حراس أمن، أو الاستعانة بجهات إنفاذ القانون.
- **إدارة السلامة التحريرية**: إدارة جميع المخاطر التي تُهدد سلامة الصحافيين الجسدية والنفسية والرقمية.
- **دائرة أمن المعلومات**:للحد ومنع الهجمات، وتحديد مصدرها وخطورتها، وتسجيل الحوادث، وتحليل اتجاهاتها.
- **دائرة أمن المؤسسة**: منع الاشخاص المعروفين بتحرشهم وخطورتهم أو المشتبه بهم من دخول غرفة الأخبار أو مقراتها.
- **دائرة الشؤون القانونية**: اتخاذ الإجراءات القانونية ضد المتحرشين عبر الإنترنت، والنظر إذا ما كان ذلك يشكل انتهاكاً لحرية التعبير.
- **دائرة الموارد البشرية**: تقديم الدعم النفسي أو خدمات المشورة للصحافيين الذين يتعرضون للهجوم. تقديم المشورة بشأن كيفية إبعاد الصحافيين عن منطقة الخطر.
- **دائرة الاتصال التواصل**: للتدخل الفوري في حال هجوم إلكتروني، على سبيل المثال سلسلة تعليقات مسيئة أو تهديد أمن وسلامة الصحافيين والمؤسسة.
- **مجموعات دعم الأقران (الزملاء)**: لضمان حصول الصحافيين المتضررين على دعم زملائهم.

١٥. توفير إرشادات السلامة التحريرية

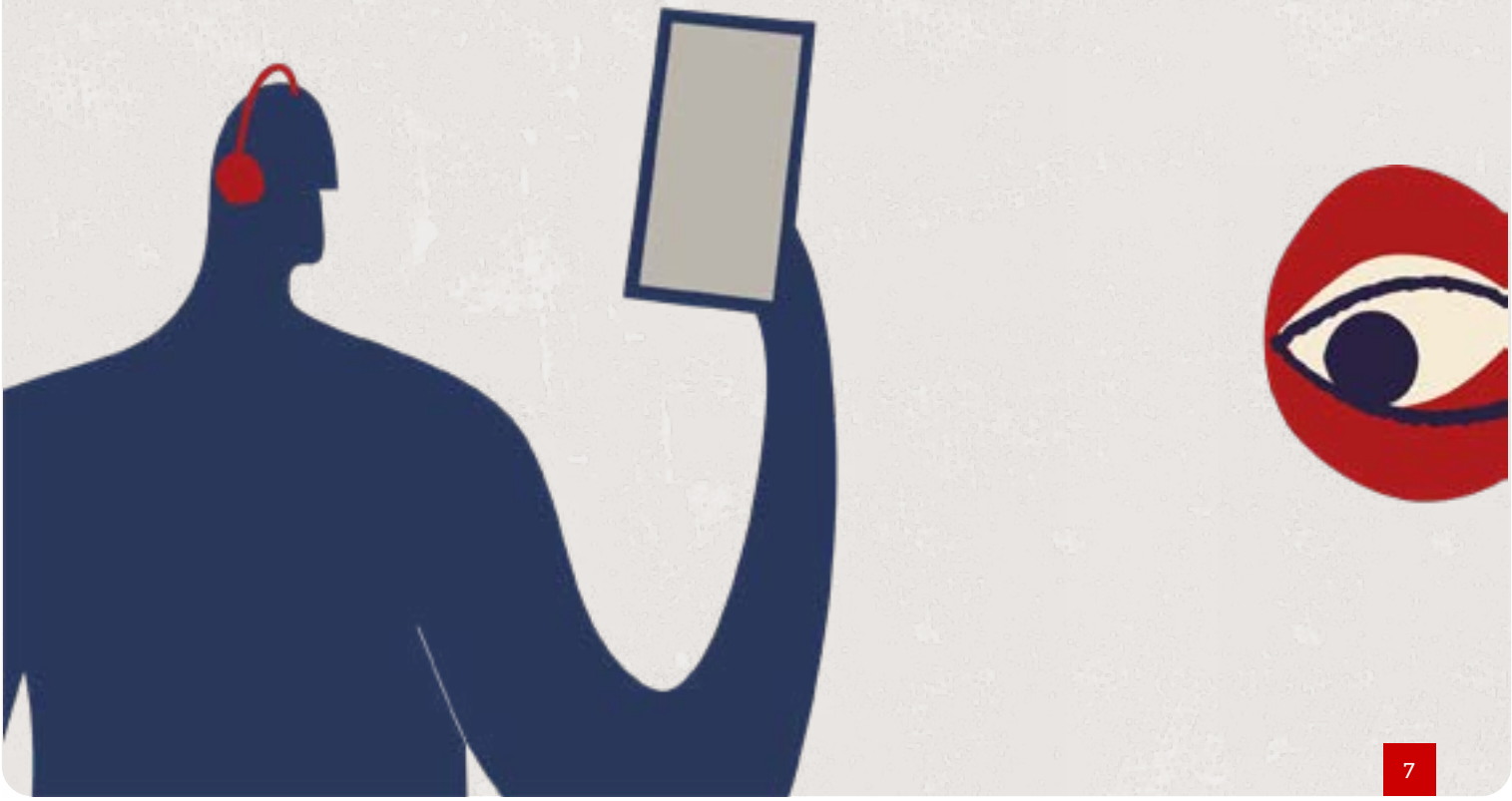
ينبغي أن تتضمن مكتبة إرشادات السلامة الخاصة بالمؤسسة الإخبارية مواد تتناول طبيعة التحرش الإلكتروني وآثاره وكيفية دعم المؤسسة للصحافيين. كما ينبغي أن تشمل إرشادات أمن المعلومات الأساسية للتحرش الإلكتروني.

١٦. الحد من المخاطر

تتبع الكثير من المؤسسات، التي تعتمد على الصحافيين والمساهمين المستقلين، سياسة «أحضر جهازك الخاص» (BOYD – Bring Your Own Device). هذا من شأنه أن يقلل ويصعّب الحماية من مخاطر الهجوم على غرف الأخبار والصحافيين. فعلى سبيل المثال، قد يكون التطبيق الآمن المُستخدم للدردشة مع مصدر حساس متاحاً على جهاز كمبيوتر شخصي أو خاص بالمؤسسة. وقد تُحفظ نُسخ احتياطية غير آمنة للمحادثات في السحابة الالكترونية إلى حسابات لا يُمكن لأمن معلومات المؤسسة الوصول إليها.

للحد من هذه المخاطر يمكن اتباع ما يلي:

- الاخذ بعين الاعتبار عدم ذكر اسم الصحافي عند نشر قصص مثيرة للجدل. غالباً ما يُعارض الصحافيون هذا، ويجب مراعاة تفضيلاتهم.
- مراجعة سياسات نشر ملفات تعريف مُفصلة للصحافيين على المواقع الإلكترونية وربط ملفاتهم الشخصية بالأخبار. قد تحظى هذه السياسات بشعبية لدى الصحافيين الذين يحرصون على بناء علاماتهم التجارية، ولكنها تزيد ايضاً من كمية المعلومات الشخصية التي يُحتمل أن تكون حساسة في المجال العام. تحتوي معظم الملفات الشخصية ايضاً على صور، مما يسمح للمنافسين بتتبع الصحافيين من خلال برامج التعرف على الوجه.
- يمكن للمسيئين ايضاً استخدام الإعدادات التي تتيح مشاركة المحتوى على نطاق واسع لأغراض التحرش. ويمكن لغرف الأخبار وضع إرشادات حول هذه الإعدادات والتفكير في كيفية استخدامها بشكل آمن واستراتيجي.



آليات الإبلاغ

بناء الثقة مع الصحافيين

من المعروف أن التحرش الإلكتروني لا يأتي دائماً من خلال قنوات الاتصال التي تتحكم بها المؤسسة، مثل المنشورات العامة أو رسائل البريد الإلكتروني، بل تتم عبر الرسائل المباشرة على حسابات التواصل الاجتماعي الشخصية.

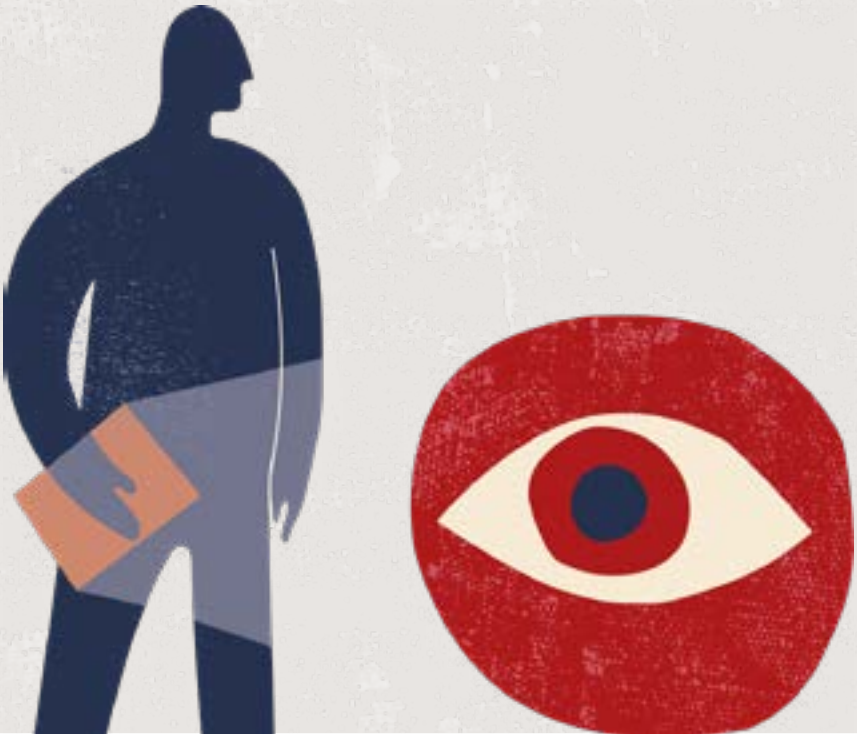
ينبغي على الصحافيين الإبلاغ عن هذه الإساءة، لكنهم غالباً لا يفعلون ذلك. قد يعتبرونها خطراً على عملهم، أو يعتقدون أنها تُلقي بظلال من الشك على نزاهتهم أو قدراتهم المهنية أو دقة تقاريرهم، خاصةً إذا ما شككت هذه الاساءة في مؤهلاتهم. وربما يشعرون بالقلق حيال إمكانية استبعادهم من التغطية الإخبارية. يجب تشجيع الصحافيين على الإبلاغ عن الإساءة. تشمل طرق تشجيع الإبلاغ ما يلي:

- **التدريب والتوعية** - يجب على الصحافيين عدم التقليل من خطورة التحرش الإلكتروني. يجب أن يوضح التدريب الممنوح لهم الطرق والآليات التي تعتزم المؤسسة استخدامها لوقف الإساءة، والتأكيد على دعم المؤسسة للصحافيين، وأن يؤكد التدريب أنه لن يتم استبعادهم من التغطية الإخبارية في حال ابلغوا عن الإساءة أو التحرش.
- **إنشاء قنوات للإبلاغ** - يمكن استخدام Teams أو Slack أو Forms أو البريد الإلكتروني، ويجب على الإدارة متابعة تقارير الإبلاغ والآليات، وإلا سيفقد الصحافيون ثقتهم بالعملية.

إبلاغ المنصات بحدوث الإساءة

أنشأت بعض شركات التواصل الاجتماعي بوابات شراكة خاصة أو جهات اتصال مخصصة للإبلاغ عن المشاكل. من المرجح أن تتضمن هذه البوابات خاصية الإبلاغ عن اختراق الحسابات، وسرقة بيانات الاعتماد، والإساءة عبر الإنترنت، وغيرها من المشاكل. قد يكون هناك ايضاً جهة اتصال مخصصة في شركة التواصل الاجتماعي يمكن لمستخدمي المؤسسات التواصل معها مباشرة في حال حدوث مشكلة.

في حالات أخرى، قد يتعين على المستخدمين الأفراد الإبلاغ عن التحرش أو أي مشاكل أخرى مباشرة إلى منصة التواصل الاجتماعي. لذا ينبغي على المديرين فهم المنصات التي يستخدمها صحافيوهم، وكيفية تعاملهم مع الشكاوى.



آليات الرصد والمتابعة

يمكن رصد التحرش الإلكتروني العلني من خلال أدوات تُمكّن المؤسسات الإخبارية من رصد التهديدات الأوسع نطاقاً التي تُهدد غرف أخبارها ومرافقها. العديد من هذه الأدوات مُصمم لحماية العلامات التجارية. قد يكشف الإنترنت المظلم والعميق بعضها، وربما الدردشات الجماعية على تطبيقات مثل «تيليجرام»، بالإضافة إلى الإنترنت العام.

يمكن استخدام بعض الأدوات الأحدث لرصد التهديدات أو الهجمات التي تُنقل عبر الرسائل المباشرة، ولكنها تتطلب موافقة الصحافي على تضمين حساباته الشخصية على مواقع التواصل الاجتماعي في هذا النوع من المراقبة.

الخيار الآخر هو استخدام أدوات فحص آلية تهدف إلى حماية الصحافيين (ومستخدمي الإنترنت الآخرين) من التأثير السام لرسائل الكراهية. يمكن استخدام هذه الأدوات لإخفاء الرسائل التي تحتوي على كلمات أو محتوى محدد.

قد يكون هذا النوع من إدارة المحتوى مفيداً لحماية المستهدفين من بعض الأضرار النفسية، ولكنه قد يمنع المؤسسة ايضاً من ملاحظة أو اكتشاف التهديدات الخطيرة التي تتطلب رداً. هناك بعض الإصدارات الجديدة المعتمدة على الذكاء الاصطناعي التي تفحص الرسائل المسيئة المستلمة وتراجع الرسائل لتحديد التهديدات التي يجب الإبلاغ عنها.

آليات الاستجابة

بمجرد إرساء آليات فعّالة للإبلاغ والرصد، قد تجد غرف الأخبار نفسها مضطرة لتحليل مئات الرسائل لتحديد ما إذا كان لأيٍّ منها عواقب وخيمة على أرض الواقع. إن فرز المضايقات الإلكترونية لتحديد المعتدين الخطيرين ممن لديهم سجل حافل بالإجرام أو العنف أشبه بالبحث عن إبرة في كومة قش.

عند اتخاذ قرار بشأن كيفية الرد، ضع في اعتبارك ما يلي:

١. تحديد هوية المهاجمين

غالباً ما يكون «جوجل» نقطة انطلاق جيدة، وقد يُظهر نتائج مفاجئة. تُستخدم أسماء المستخدمين أو الأسماء المستعارة غالباً في مواقع متعددة، مما قد يساعد في تحديد هوية المرسِل. يمكن استخدام خدمات الإنترنت، مثل Social Catfish، للبحث العكسي عن عناوين البريد الإلكتروني، بينما يمكن لـ PeekYou البحث من خلال أسماء المستخدمين.

قد يمتلك قسم أمن المعلومات في المؤسسات الإعلامية القدرة على تحديد مواقع بروتوكول الإنترنت (IP). إلّا أن العديد من مهاجمي الإنترنت يستخدمون الشبكات الافتراضية الخاصة (VPN) لإخفاء مواقعهم وفتح حسابات وهمية لمرة واحدة.

٢. تحليل التهديدات

تشمل المؤشرات إلى أن التهديد عبر الإنترنت قد يتحول إلى عنف جسدي ما يلي:

- **يتضمن تهديداً مباشراً مثل «سأقتلك»**. في المقابل، قد يُنظر إلى التهديد غير المباشر مثل «يجب إعدامك بتهمة الخيانة» على أنه حرية تعبير وليس نية للإيذاء.
- **يُعرّض الصحافي لخطر متزايد**. هل تم الكشف عن عنوان منزله؟ هل سيكون غير آمن إذا تم الكشف عن موقعه الجغرافي؟
- **يخفي المهاجم هويته**. قد يُظهر هذا أنه يعلم أن أفعاله خاطئة. قد يشكّل المهاجمون الذين يستخدمون أسماءهم الحقيقية، على عكس المتوقع، تهديداً أكبر لأنهم قد لا يدركون أن ما يفعلونه خطأ.
- **الموقع**. قد يُشكّل شخص يعيش بالقرب من مكان الهجوم تهديداً أكبر من شخص يحتاج إلى السفر جواً حول نصف الكرة الأرضية للوصول إلى هدفه.
- **السجل الجنائي أو تاريخ العنف**. هل للمهاجم صلات بجماعات عنيفة أو لديه تصريح بحمل أسلحة؟
- **التصعيد**. هل انتقلت الهجمات من منصة إلى أخرى وازدادت في الحجم والحدّة؟
- **التهديدات المنظمة**. هل الحكومة أو جهة أخرى متورطة في الهجمات؟ هل سبق لها أن أبدت استعدادها لاستخدام العنف؟ هل يمكن للحكومة ايضاً اتخاذ إجراء قانوني أو احتجاز صحافي؟
- **روبوتات الإنترنت**. انتبه للحسابات الجديدة التي ليس لها تاريخ واضح، أو تلك التي شاركت في حملات مماثلة.

٣. حظر المهاجمين

قد يكون حظر المهاجمين عبر الإنترنت مغرياً لحماية الصحة النفسية للصحافيين. ومع ذلك، قد يؤدي الحظر ايضاً إلى تصعيد غير ظاهر. غالباً ما يُنشئ المهاجمون حسابات جديدة و يستأنفون المضايقات ببساطة.

كبديل، يمكن لفريق السلامة التحريرية أو قسم أمن المعلومات أن يتولى مراقبة حسابات التواصل الاجتماعي الشخصية. مع ذلك، قد يتردد الصحافيون في إعطاء كلمات المرور أو السماح بالوصول إلى الرسائل من مصادر حساسة. في هذه الحالة، يمكن لزميل أو مشرف تحريري مراقبة الرسائل، مع الاستعانة بخبراء السلامة وأمن المعلومات إذا لزم الأمر.

٤. اتخاذ الإجراءات

يجب على غرف الأخبار اتخاذ إجراءات سريعة إذا ثبت أن التحرش الإلكتروني قد يؤدي إلى أضرار جسيمة. تشمل الخيارات المتاحة ما يلي:

- **الاتصال بسلطات إنفاذ القانون**. ينبغي دائماً إحالة التهديدات المباشرة إلى الشرطة أو الوكالات الفيدرالية. قد يحتاج الصحافيون إلى الإبلاغ بأنفسهم.
- **إغلاق المكاتب**. قد يصل التهديد الى حد تتخذ فيه الإدارة اغلاق المكاتب لضمان سلامة الصحافيين والعاملين.
- **إضافة المهاجمين المعروفين إلى قوائم الأشخاص الممنوعين من دخول مكاتب المؤسسة** وإبلاغ الموردين الخارجيين وملاك العقارات.
- **ضمان أمن منزل الصحافي أو مكان إقامته المؤقت** من خلال توفير نظام أمن منزلي أو اشتراك في خدمة أمنية.
- **نقل الصحافي وعائلته** إلى فندق يتمتع بحماية أمنية جيدة أثناء تقييم التهديد.
- **تعيين حراس شخصيين** للصحافيين البارزين والأكثر عرضة للخطر.
- **إعادة توجيه البريد الإلكتروني للمؤسسة** وحظر الحسابات المسيئة على البريد الإلكتروني الشخصي.
- **تحديد من يتولى مراقبة التهديدات** الواردة نيابة عن الصحافي.
- **الإبلاغ عن الجاني إلى المنصة**. قد يضطر الصحافيون أنفسهم إلى تقديم شكوى من خلال أدوات الإبلاغ الذاتي الخاصة بالمنصة.
- **اتخاذ إجراءات قانونية**.
- **التواصل مع الصحافيين النظراء في مؤسسات إعلامية أخرى** ممن قد يكون لديهم معلومات للمساعدة في تقييم خطورة التهديد.
- **التحدث والنشر علناً عن التهديدات** لدعم الصحافيين وتعزيز صمودهم ومعنوياتهم.
- **الإبلاغ عن المضايقات**. قد تكون هذه طريقة فعّالة لتسليط الضوء على هجوم ما، خاصةً إذا كان جزءاً من اتجاه أوسع.

٥. دعم الصحافي

قد يكون للتعرض الى موجة من المضايقات أثر نفسي عميق. يُعد الدعم التنظيمي بالغ الأهمية لتعزيز قدرة الصحافي على الصمود ومساعدته على مواصلة التغطية الصحافية دون خوف. فكّر في آليات الدعم، بما في ذلك:

- **تقديم الدعم والمشورة** من الزملاء داخل المؤسسة.
- **التوضيح بأن المؤسسة لا تلوم الصحافي أو تغطيته الصحافية**، وتدعمه في مواصلة تغطية القصة.
- **تقديم المساعدة في الإبلاغ عن المضايقات عبر منصات** التواصل الاجتماعي أو تقديم بلاغ للشرطة.
- **إجراء فحص معمق لنقاط ضعف الصحافي المتضرر** على الإنترنت للتأكد من عدم وجود أي شيء يمكن للمهاجمين استغلاله.
- **مراجعة وتحسين أمن منزل الصحافي**. اتخاذ قرار بشأن نقل الصحافي وعائلته إلى مكان أكثر أماناً.
- **الرد على الانتقادات المسيئة للمؤسسة والصحافي** عبر بيانات رسمية وسلسة من التعليقات المضادة.

٦. في الحالات القصوى والمتطرفة

قد يتفاقم التحرش الإلكتروني لدرجة تُعرّض غرفة الأخبار بأكملها للخطر. على سبيل المثال، حملة منظمة ومتعمدة من شخصية سياسية مشهورة لإثارة الغضب والكراهية قد تجعل من غير الآمن نشر أي تقارير علنية، أو العمل ضمن فعاليات معينة، أو في بعض المناطق. يجب على فرق السلامة أن تكون على دراية بهذا الاحتمال، وأن تكون مستعدة لتصعيد حالات التحرش الفردية إلى الإدارة العليا.

٧. حفظ السجلات وتوثيق الدروس والعبر

قد تختلف كل حالة جديدة من حالات التحرش الإلكتروني عن سابقاتها، وقد تجد دروساً يمكنك استخلاصها حول كيفية التعامل مع الهجمات المستقبلية. الاحتفاظ بالسجلات يُمكّن مؤسستك من تحديد الاتجاهات الناشئة، وهو أمر بالغ الأهمية لإقناع كبار المديرين والإدارة المالية بتخصيص التمويل اللازم لمكافحة هذه المشكلة.

قائمة التحقق لمديري غرف الأخبار

التدابير الوقائية الاستباقية	تحديد حجم المشكلة	التدابير الوقائية الاستباقية
	تقديم التدريب والتوعية	إدراج دورات السلامة الأساسية لجميع الصحافيين
	إنشاء قنوات الاتصال	Teams، Slack، البريد الإلكتروني
	التحقق الذاتي من المعلومات	تضمينها في عملية التوجيه وإتاحتها لغرفة الأخبار من خلال وحدة التعليم الذاتي المنشورة على الشبكة الداخلية
	إجراء أبحاث معمقة حول الثغرات الرقمية	فكّر في استخدام مزود خارجي
	استخدام خدمات حذف البيانات	اشترك في خدمة حذف البيانات للصحافيين المعرضين للخطر
	مراقبة التهديدات	يمكن لمزودي الخدمة الخارجيين البحث في الويب المظلم والعميق للوصول إليها مثل مجموعات الدردشة على «تيليجرام»
	حذف المنشورات القديمة	قم بإدراج هذه التعليمات ضمن عملية اعداد الموظفين الجدد
	إنشاء ملفات شخصية ذات تفاصيل قليلة	قم بإدراج هذه التعليمات ضمن عملية اعداد الموظفين الجدد وتدريبات السلامة
	الفصل بين الحياة الخاصة والمهنية	ناقش مسألة الفصل بين الملفات الشخصية والمهنية مع الصحافيين وفرق التحرير
	مراقبة المجموعات أو الأفراد المعرضين للخطر	عقد ورش عمل إضافية حول السلامة لفريق التحقق من المعلومات، وفريق وضع السياسات، وما إلى ذلك، والتي من الممكن أن تقدمها شركات خدمة خارجية
	التدريب على الظهور العلني	عقد تدريبات حول كيفية تعامل الصحافيين مع الظهور العام والعلني والتحدث أمام الجمهور
	المشاركة في إدارة التعليقات	يمكن لمزود خدمة خارجي أن يقوم بذلك
	إنشاء فريق استجابة متعدد الأقسام	يشمل إدارة التحرير، السلامة، محرر وسائل التواصل الاجتماعي، الدعم القانوني، الدعم من الأقران والزملاء
	توفير إرشادات السلامة التحريرية	نشرها وتعميمها من خلال الشبكة الداخلية الخاصة بالمؤسسة
	الحد من المخاطر	إزالة الصور الشخصية من ملفات الصحافيين على الإنترنت ومنصات التواصل الاجتماعي

قائمة التحقق لمديري غرف الأخبار

آليات الابلاغ	إنشاء قناة خاصة للتواصل مع الصحافيين بشأن التحرش الإلكتروني	Teams، Slack، البريد الإلكتروني
	إبلاغ المنصات بالإساءة	تشمل الخيارات بوابات الشراكة، والاتصالات المباشرة عبر المنصات، والتقارير الفردية من قبل الصحافيين
آليات الرصد	رصد التهديدات العلنية	يمكن لمزود خدمة خارجي أن يقوم بذلك
	رصد ومراقبة الرسائل المباشرة	يمكن لنفس مزود الخدمة الخارجي أن يقوم بذلك، بشرط الحصول على موافقة الصحافي المستهدف
	استخدام برامج تحمي الصحافيين من رسائل كراهية	قد يحمي هذا من بعض الأذى النفسي ولكنه قد يمنع ايضاً اكتشاف التهديدات الخطيرة
	رصد وإدارة التعليقات المتتابعة	يمكن لمزود خدمة خارجي أن يقوم بذلك
آليات الاستجابة	تطوير طريق لكشف هوية المهاجمين عبر الإنترنت	يمكن استخدام Social Catfish البحث العكسي عن عناوين البريد الإلكتروني. PeekYou يمكنك البحث من خلال أسماء المستخدمين
	تحليل التهديدات	يتم ذلك من خلال فريق السلامة، وربما بدعم من مزود خدمة خارجي
	حظر المهاجمين	اطلب من المحررين والزملاء مراقبة الرسائل إذا لزم الأمر وحظر المهاجمين المحتملين
	التعامل مع التهديدات الخطيرة والقصوى	مراجعة أمن الصحافي المستهدف، إبلاغ إدارة المبنى، التواصل مع جهات إنفاذ القانون، مساعدة الصحافيين في الإبلاغ عن التهديدات، التواصل مع المنصات، اتخاذ القرارات بشأن الخيارات القانونية، التواصل مع الزملاء الصحافيين المستهدفين وأي زملاء تأثروا بالهجوم
	توفير الدعم	قد يكون المدير المباشر أو الزملاء هم الأقدر على دعم الصحافي المتضرر
	حفظ السجلات وتوثيق الدروس والعبر	يمكن لقسم أمن المعلومات تولي زمام المبادرة في هذا الأمر

الملحق ١. تعريف التحرش الإلكتروني

يتخذ التحرش والإساءة عبر الإنترنت أشكالاً متعددة، ويهدف إلى مضايقة الصحافيين أو ترهيبهم أو إسكاتهم. ويمكن أن يتجاوز ذلك مسببا إيذاء عاطفيا لضحاياه، مما قد يؤدي إلى عواقب وخيمة.

مع تطور التكنولوجيا والذكاء الاصطناعي، سنواجه إشكالات جديدة من التحرش عبر الإنترنت من خلال قنوات بالكاد نعرفها اليوم. ومن غير المرجح ألّا تكون المنصات التي تحوي حاليا أخطر أنواع التنمر والإساءة هي نفسها المنصات التي نخشى منها بشدة في السنوات القادمة.

لا شك أن اتخاذ موقف دفاعي أكثر حصانة، واستخدام استراتيجيات استباقية تعزز المواجهة، سيكون أفضل من التركيز على منصات محددة أو الاعتماد عليها للتعامل مع بلاغات الإساءة. قد يقع التحرش عبر الإنترنت ايضاً في دائرة نقاشات حرية التعبير، مما يُعقّد قدرة جهات إنفاذ القانون على التدخل، ويجعل شركات التواصل الاجتماعي مترددة في تحمل مسؤولية إدارة المحتوى.

يمكن لمن يريد الغوص في تعريفات أخرى للتحرش عبر الإنترنت الاطلاع على هذه المواقع:

Pen America; Harvard T.H. Chan School of Public Health; Dart Center for Journalism & Trauma

لماذا علينا ان نهتم؟

تحتاج غرف الأخبار إلى حماية صحافييها من التحرش الإلكتروني:

- لضمان قدرتهم على نقل الأخبار بحرية وجرأة وموضوعية.
- لحمايتهم وحماية مكان عملهم من التهديدات الجسدية.
- لدعم صحتهم النفسية وسلامتهم العاطفية على المدى الطويل.

لعل أحد الأهداف الرئيسية للتحرش الإلكتروني إسكات الصحافيين وتخويفهم من تغطية القضايا بشكل عام والحسّاسة بشكل خاص، أو دفعهم إلى ترك المهنة نهائياً. وغالباً ما يكون هذا التحرش فعالا. فقد أفاد استطلاع أجرته منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو) للصحافيات عام ٢٠٢٠ أن ٣٠٪ منهن مارسن الرقابة الذاتية على وسائل التواصل الاجتماعي بعد تعرضهن لهجمات إلكترونية. ووجد استطلاع آخر أجرته المؤسسة الدولية لإعلام المرأة (IWMF) أن ٤٠٪ من الصحافيات توقفن عن الكتابة في القضايا التي كنّ يعلمن أنها ستؤدي إلى هجمات، وأن ثلثهن فكّرن في ترك المهنة.

من شأن هذا أن يجعل من التحرش الإلكتروني تهديداً خطيراً لحرية التعبير، وتهديداً وجوديا للصحافيين وغرف الأخبار التي تحاسب وتسائل أصحاب النفوذ من خلال صحافة عالية الجودة وتحقيقات جريئة. في جميع الأحوال، قد تُلحق الإساءة الإلكترونية ضرراً نفسياً وعاطفياً بضحاياها، مخلفة آثارا نفسية عميقة.

في بعض الحالات، قد تتطور الهجمات الإلكترونية إلى عنف جسدي وتهديدات مباشرة. وقد وجدت دراسة اليونسكو أن ٢٠٪ من المستطلَعات عالمياً أفدن بتعرضهن لاعتداءات فعلية على أرض الواقع، نتيجة تعرضهن للعنف الإلكتروني. وفي الشرق الأوسط، كانت هذه النسبة أعلى من ذلك، حيث أفادت أكثر من نصف الصحافيات في المنطقة، اللواتي أبلغن دراسة اليونسكو بأنهن تعرضن للإساءة الإلكترونية، بأنهن ايضاً تعرضن لاعتداءات جسدية.

التحرش عبر الإنترنت كسلاح

تستخدم العديد من الدول التحرش الإلكتروني كسلاح للرقابة والقمع. وقد استخدمته الحكومات الاستبدادية، والجماعات المتطرفة، والجهات السياسية الفاعلة، أو الأفراد اصحاب النفوذ وعديمي الضمير، لتعبئة وتحريض حشود إلكترونية ضد معارضيهم و منتقديهم. ولعل تأثير ألف رسالة تهديد أو إهانة، أعظم بكثير من تأثير مجموعة بسيطة منها.

النساء وصحافيو الأقليات

تتعرض الصحافيات بشكل خاص و المنتميات إلى الأقليات لانتهاكات عبر الإنترنت أكثر من زملائهن الرجال البيض، وغالباً ما تكون ذات طابع كراهية للنساء أو عنصرية. عندما ترغب مؤسسة إخبارية في معرفة مدى تعرض أعضاء غرفة أخبارها للانتهاكات عبر الإنترنت، ينبغي عليها التأكد من استهداف صحافييها من النساء، الأقليات ومثليي الجنس ومزدوجي التوجه الجنسي والمتحولين جنسيا (مجتمع الميم)، إذ يُرجّح أن يكونوا المستهدفين الرئيسيين.

المواضيع التي تثير الكراهية عبر الإنترنت

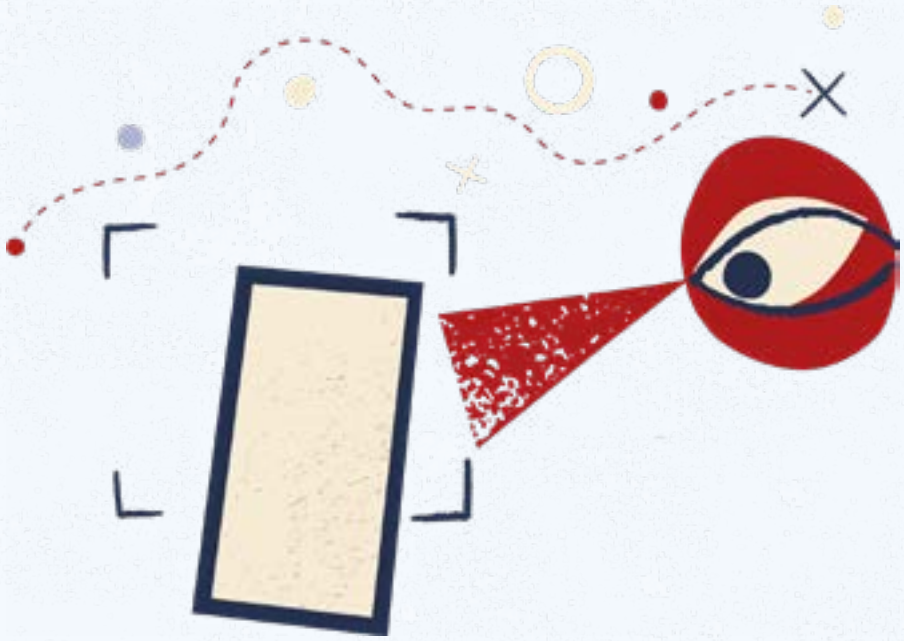
تُعدّ الأخبار السياسية في الدول التي تشهد استقطاباً سياسياً كبيراً، مثل الولايات المتحدة، مصدراً رئيسياً للهجمات الإلكترونية. وفي الدول التي تحكمها أنظمة استبدادية أو غير شرعية، قد تقمع المعارضة في كثير من الأحيان، بحيث تسعى الحكومات إلى استخدام التحرش الإلكتروني كسلاح لإسكات الأصوات.

في المناطق التي أدت فيها الخصومات العرقية أو القبلية أو الطائفية إلى صراعات، قد تُثير التقارير التي تُعتبر انتقادية لأحد الأطراف، أو التي تستخدم لغة تُعتبر منحازة، ردود فعل غاضبة. وهذه مشكلة شائعة عندما تُترجم القصص والتقارير من قِبل محررين خارج السياق المحلي، دون مراعاة الفروق اللغوية الدقيقة.

تكتسب الألعاب الإلكترونية، والاستثمارات من خلال الإنترنت شعبية في منصات التواصل الاجتماعي، بينما تُعدّ الرياضة والموسيقى الشعبية مواضيع مثيرة قد تؤدي الى الكثير من الإساءة الالكترونية والتنمر.

من بين القضايا الواقعية الأخرى التي غالباً ما تؤدي إلى فضاءات إلكترونية سامة:

- اليمين المتطرف واليسار المتطرف
- كراهية النساء
- الاتهام بمعاداة السامية
- الحروب الثقافية
- التضليل
- العنصرية
- النقاشات حول حرية التعبير مقابل الرقابة
- التوترات الجيوسياسية



أنواع الهجمات الإلكترونية

هجمات/ملاحقة جماعية إلكترونية

تشجيع الآخرين على استهداف شخص ما في حملة منسقة. قد يشمل ذلك قيام العديد من المتحرشين بالإبلاغ عن حساب صحافي لانتهاكه شروط خدمة منصة ما لحذفه. قد تستخدم الحكومات أو الجيوش أو الأحزاب السياسية مجموعات من المتصيدين شبه رسمية لإثارة هجوم جماعي.

التهديد بالإيذاء

التهديد بالإعدام، أو المقاضاة، أو الاغتصاب، أو القتل، أو مطاردة أو استهداف أفراد الأسرة، بمن فيهم الأطفال. بعضها تهديدات مباشرة قد تستدعي رداً من جهات إنفاذ القانون، لكن معظمها لا يصل الى حد الإجرام أو يندرج تحت حماية حرية التعبير.

الإفصاح

نشر معلومات شخصية حساسة، مثل عنوان المنزل أو اسم مدرسة الطفل. قد ينشر المعتدون هذه المعلومات الشخصية لتشجيع الآخرين على مضايقة الصحافي المستهدف أو مراقبته أو الاعتداء عليه جسدياً أو انتحال هويته. يمكن أن يحدث التشهير أثناء تواجد الصحافي في مهمة عالية الخطورة في مكان يحتمل أن يكون خطيرا.

الملاحقة الإلكترونية

مضايقة الضحية وترهيبها لفترة طويلة. قد يستخدم المتحرشون المراقبة والملاحقة وسرقة الهوية وغيرها من أعمال التنمر الإلكتروني. غالباً ما تُعد الملاحقة الإلكترونية جريمة جنائية، وينبغي على الصحافيين المستهدفين الحصول على استشارة قانونية، لأن المعتدين قد لا يكونوا مستقرين عقليا أو عاطفيا.

التبليغ الكاذب

تقديم بلاغ كاذب عن جريمة كالقتل أو احتجاز الرهائن لدفع الشرطة إلى مداهمة منزل المستهدف. في كثير من الدول تكون فرق التدخل السريع التابعة للشرطة مدججة بالسلاح وتتوقع التعرض لإطلاق نار، لذا قد تكون المداهمات بالغة الخطورة وغالباً ما تؤدي إلى وفيات.

انتحال الهوية عبر الإنترنت

إنشاء حسابات وهمية على مواقع التواصل الاجتماعي لنشر رسائل مهينة أو تحريضية تهدف إلى تشويه سمعة المستهدف أو تشجيع المزيد من المضايقات. قد تشمل الأهداف الأخرى الاحتيال المالي أو التأثير على الرأي العام.

الملحق ٢. دليل تعامل الصحافيين مع العنف الرقمي

لعل الهدف الأساسي للتهديدات والمضايقات الإلكترونية هو إسكات الصحافيين ودفعهم إلى ممارسة الرقابة الذاتية. قد يكون تلقي سيل من التهديدات أمراً مخيفاً وله تأثير نفسي. كما قد تؤدي الهجمات الإلكترونية إلى عنف جسدي.

في حال تعرضك لأي تهديد أو مضايقة الكترونية عليك ابلاغ مشرفك أو رئيس التحرير إذا تعرضت لهجوم خطير.

من المهم ايضاً تعزيز قدرتك على مواجهة المضايقات الإلكترونية من خلال تقليل كمية المعلومات الشخصية المتاحة على الإنترنت. التهديد العام سيء بما فيه الكفاية، ولكنه أسوأ إذا كان المهاجم يعرف مكان مدرسة طفلك أو عنوان منزلك.

للحد من مخاطر الهجمات أو التهديدات يُنصح بإجراء فحص ذاتي للبيانات الشخصية المنشورة، وضبط إعدادات الخصوصية في حساباتك على مواقع التواصل الاجتماعي.

كما يُنصح إنشاء حسابات عامة وخاصة منفصلة على الإنترنت، وتقليل كمية المعلومات الشخصية التي تشاركها مع العالم من خلال حساباتك المهنية، واقتصار الحسابات الشخصية على العائلة والأصدقاء.

أمن المعلومات

تحديث البرامج والتطبيقات الخاصة بك

في الغالب، يتمكن المعتدون من اكتشاف الثغرات الأمنية في البرامج التي تشغّل أجهزة الحاسوب والهواتف، حيث يسارع المخترقون والمجرمون إلى استغلالها. وينطبق هذا ايضاً على هواتفنا وأجهزة الحاسوب المحمولة والمكتبية. لذلك، احرص ايضاً على حماية أجهزة الحاسوب والهواتف الخاصة بك، وتأكد من تحديث جميع برامجك.

لا تنقر أبداً على الروابط المشبوهة

أكثر من ٧٥٪ من الهجمات الإلكترونية تحدث عبر رسائل بريد إلكتروني «تصيّدية» (Phishing) تحتوي على رابط أو مرفق (attachment) يُعرّض جهاز الكمبيوتر الخاص بك للخطر. إذا وصلتك رسالة بالبريد إلكتروني تُخبرك بأمر مُلحّ للغاية، أو تطلب منك إدخال تفاصيل حسابك، أو تحتوي على كلمات بتهجئة غريبة، فاطلب الدعم من قسم تكنولوجيا المعلومات لديك، أو استخدم برنامجاً مثل Dangerzone لفتح المرفق بأمان أو في بيئة آمنة.

ادارة كلمات المرور

تستطيع برامج اختراق كلمات المرور الجاهزة تخمين مئات الملايين من كلمات المرور في الثانية، وتزويدها بمعلومات عن شخص معين من حساباته على مواقع التواصل الاجتماعي. فكّر في استخدام برنامج لإدارة كلمات المرور 1Password أو Dashlane أو KeePassXC لإنشاء كلمات مرور عشوائية لكل حساب وتخزينها بأمان. تأكد من أن كلمة مرورك الرئيسية يصعب اختراقها.

تحقق مما إذا كان قد تم اختراق حساباتك

يمكن لبرنامج have i been pwned? أن يُظهر أي من حساباتك تم اختراقها. قم بتغيير كلمة مرور في حال اكتشفت انه تم الاختراق.

استخدام المصادقة الثنائية

يُنصح بتفعيل المصادقة الثنائية two-factor authentication حيث يتم ارسال رمز وصول إضافي عبر رسائل نصية أو تطبيق مثل Google Authenticator أو Symantec VIP Access. يُفضّل استخدام هذه التطبيقات، إذ يُمكن اعتراض الرسائل النصية في حال استنساخ بطاقة الهاتف الذكية (SIM).

تقييم التهديدات الأمنية للمعلومات بشكل منتظم

قد لا تعتقد أن تقريرك او قصتك تتضمن أي حساسية، ولكن لا يمكنك دائماً التنبؤ بما إذا كانت ستؤدي إلى أمر حساس يتطلب الحماية. فكّر في أمن المعلومات منذ بداية أي مهمة، واتخذ خطوات أمن المعلومات الأساسية الموضحة في هذه الوثيقة قبل أن تتحول قصة روتينية الى شديدة الحساسية وبالتالي تحتاج إلى إجراءات أمنية إضافية.

استخدام هاتف مؤقت غير متصل بشبكة الانترنيت

فكّر فيما إذا كان عليك أخذ هاتفك المعتاد إلى اجتماعاتك مع المصادر إذا كنت تعدّ تقريراً حول قضية حساسة. قد يستخدم المتتبّعون الماهرون هاتفك لمعرفة موقعك أنت والمصدر، مما يُعرّض أمنك وأمن مصدرك للخطر. استشر مشرفك أو المحرر أو قسم تكنولوجيا المعلومات بشأن استخدام هاتف مؤقت.

استخدام الشبكات الافتراضية الخاصة VPN

استخدم شبكة افتراضية خاصة VPN التي تعمل على تشفير اتصالك بالإنترنت - عند توصيل أجهزة الكمبيوتر المحمولة الخاصة بالعمل والشخصية وهاتفك بشبكات الإنترنت اللاسلكي Wi-Fi العامة ضعيفة الحماية في الفنادق والمطارات. يمكن استخدام Proton VPN كخيار مجاني جيد.

استخدام تطبيق مشفر للاتصالات الحساسة

«واتساب»، «سيجنال»، وWire خيارات جيدة، مع أن شركة «ميتا»، مالكة «واتساب»، تحتفظ بما يُسمى «البيانات الوصفية» تحدد من تواصلت معه ومتى دون أن تشمل محتوى محادثاتك. لا يُشفّر «تيليجرام» تلقائيا إلا إذا اخترت خيار المحادثة السرية.

تشفير القرص الصلب (hard drive) الخاص بك

من المفترض ان يكون القرص الصلب لجهاز الكمبيوتر المحمول مُشفّراً، والّا فيمكن الوصول إلى المعلومات الموجودة على جهاز الكمبيوتر بسهولة. فإذا كان مُشفّراً وجهاز الكمبيوتر مُطفأً، فستكون المعلومات آمنة. ينطبق الأمر نفسه على الهواتف.

التصفح الآمن في الإنترنت

احرص دائماً أن المواقع التي تزورها آمنة. استخدم HTTPS Everywhere لضمان تصفحك النسخة الآمنة من المواقع. تجنب المواقع التي تبدأ عناوينها بـ http:// وليس https://

تشفير الملفات والمستندات الحساسة

من الممكن استخدام برامج التشفير المفتوحة المجانية مثل لتشفير VeraCrypt و Zip-٧ المجلدات والملفات.

تجنب محطات شحن USB

يُنصح شحن الهاتف دائماً باستخدام مقبس كهربائي بدلاً من محطة شحن USB عامة. في البرازيل، خلال كأس العالم ٢٠١٤، قامت عصابة إجرامية بتركيب بعض نقاط شحن USB في مطار «ريو»، وأدى ذلك إلى سرقة المعلومات من هواتف المسافرين. ويُنصح باستخدام مانع بيانات لضمان وصول الطاقة فقط عند توصيل كابل USB بالهاتف من محطة شحن عامة.

أمان الأجهزة

يُنصح إبقاء الهواتف وأجهزة الكمبيوتر المحمولة قريبة منك عند العمل على تقارير حساسة. إذا تركت جهاز الكمبيوتر المحمول في غرفة فندق، فلا توجد طريقة لمعرفة ما إذا كان أحدهم قد استخدمه أثناء غيابك.

استخدم تطبيقات تكتشف ما إذا كان هاتفك مُستهدفا ببرامج ضارة، بما في ذلك تطبيق iVerify الذي يُتيح للمستخدمين إجراء فحص شامل مجاني مرة واحدة شهرياً، وتطبيق F-Secure Mobile Security (المعروف سابقا باسم Lookout Lite). غالباً ما يُمكن إزالة البرامج الضارة المُثبتة في الذاكرة قصيرة المدى بإعادة تشغيل جهازك.

توخي الحذر الشديد عند عبور الحدود

احفظ معلوماتك الحساسة في «التخزين السحابي» (Cloud) قبل عبور الحدود. سجّل خروجك من الحسابات أو التطبيقات في حال طلب مسؤول الحدود الوصول إلى هاتفك أو حاسوبك المحمول ويُفضل ان تقوم بذلك قبل الوصول الى نقطة الحدود. أوقف تشغيل أجهزتك ليتعذر الوصول إلى المعلومات.

نشر المعلومات الخاصة

المعلومات المنشورة على الإنترنت قد تجعلنا عرضة لهجمات من قبل من لا تعجبهم قصصنا وتقاريرنا. قد يبحث المعتدون عن منشورات سابقة على مواقع التواصل الاجتماعي تُضعف مصداقيتنا كصحافيين، أو تكشف عن تفاصيل شخصية مثل عنوان المنزل. يأمل المعتدون أن تُحفّز المعلومات التي ينشرونها الآخرين على مهاجمتنا جسديا.

انظر إلى هذه الأمثلة:

- قد يهاجمونك بالاتصال بالشرطة والإبلاغ عن حالة احتجاز رهينة وهمية.
- ناقدة ثقافية نسوية تحدّت هيمنة الرجال على صناعة الألعاب، وواجهت تهديدات بالاغتصاب والتفجير والقتل.
- يمكن أن يتحول المتصيّد إلى مُلاحق حقيقي.

قد تحتاج إلى الكشف عن معلوماتك الشخصية (ما يُعرف بالكشف الذاتي) لمعرفة ما هو متاح عنك على الإنترنت والذي قد يستخدمه المتصيدون. فكّر في اتخاذ الخطوات التالية:

البحث في جوجل

قم بعمليات البحث على جوجل، بينج (Bing)، ياندكس (Yandex) أو DuckDuckGo وBaidu. قد تختلف النتائج من محرك بحث لآخر، خاصةً إذا كنتَ قد عشت في الخارج.

«الاسم الأول اسم العائلة» أو «اسم المستخدم» "Firstname Lastname" OR "username"	استخدم علامات الاقتباس للبحث عن كلمة أو مجموعة كلمات محددة. ابحث عن مجموعات مختلفة من اسمك، وأسماء المستخدمين المتكررة، وعناوين البريد الإلكتروني.
١. «الاسم الأول اسم العائلة» - «اسم وسيلة الإعلام» "Firstname Lastname" - "Medianame" ٢. «الاسم الأول اسم العائلة» «اسم وسيلة الإعلام» - site:Medianame.com Firstname Lastname "Medianame" -site:Medianame.com	١. سيؤدي هذا إلى استبعاد النتائج التي تتضمن مؤسستك الإعلامية، مما سيظهر النتائج التي قد تكون مخفية في الصفحات اللاحقة. كما أن علامة الطرح طريقة جيدة لإزالة النتائج المتعلقة بأشخاص آخرين يشاركونك نفس الاسم. ٢. ابحث عن الصفحات التي تذكر اسمك واسم مؤسستك الاعلامية، مع تصفية الصفحات من موقعها الإلكتروني Medianame.com
«الاسم الأول * الاسم الأخير» "Firstname * Lastname"	تعمل علامة النجمة كعلامة نائبة لأي مصطلحات عامة، على سبيل المثال اسمك الأوسط أو الحرف الأول من اسمك.
"(650) 656-5656" OR "6506565656"	ابحث عن رقم هاتفك. أضف صيغاً بديلة.
"username@gmail.com" filetype:pdf	سيعرض هذا أي ملفات PDF تحتوي على بريدك الإلكتروني الشخصي، على سبيل المثال منشورات الخريجين أو العروض التقديمية السابقة.
«الاسم الأول * اسم العائلة» ١٠١ شارع ماين، لوس أنجلوس، كاليفورنيا "Firstname * Lastname" ١٠١ Main St Los Angeles CA	ابحث عن الارتباطات بالعناوين السابقة والمدن والبلدات والمؤسسات والوظائف والمنشورات.
الاسم الأول اسم العائلة الموقع: reddit.com Firstname Lastname site:reddit.com	ابحث في مواقع محددة للعثور على نتائج غير مفهرسة بواسطة محركات البحث.

البحث العكسي عن الصور

- استخدم بحث الصور في ياندكس Yandex للبحث عن صورك. حمّل صورة لنفسك باستخدام خاصية البحث العكسي للصور في ياندكس.
- حمّل صورك الشخصية على X وFacebook وLinkedIn وInstagram إلى TinEye لمعرفة أماكن استخدامها الأخرى.

إغلاق إعدادات الخصوصية على وسائل التواصل الاجتماعي

تجمع منصات التواصل الاجتماعي معلومات عنك لبيع الإعلانات. تحكّم في كيفية استخدامها لهذه المعلومات وحجمها من خلال تعديل إعدادات الخصوصية لديك. تذكّر أن إعدادات الخصوصية قابلة للتغيير وقد تحتاج إلى تحديث.

«فيسبوك»

ابدأ باستخدام أداة المساعدة الذاتية للخصوصية من «فيسبوك»:

للمستخدمين بالعربية	للمستخدمين بالإنجليزية
• اكتب «التحقق من الخصوصية» في حقل البحث بالصفحة الرئيسية وانقر على «زيارة». • راجع من يمكنه رؤية تفاصيل ملفك الشخصي. تأكد من عدم وجود أي منها «عامة». • حدد من يمكنه رؤية منشوراتك بـ «الأصدقاء» أو «أصدقاء محددون» أو «أنا فقط». • تذكر أن صورة غلافك ستكون دائماً عامة. استبدلها بصورة لا تُظهر وجهك. اتبع هذه الخطوات الإضافية في «سجل النشاطات»: • انقر على « سجل النشاطات» لمراجعة يومياتك. اخفِ أو احذف أي شيء تريد إخفائه. تأكد من عدم وجود صور في «مراجعة الصور». ستظهر الصور هنا إذا فعّلت ميزة التعرّف على الوجه، والتي يمكنك تعطيلها. • انقر على «نشاط تمت الإشارة إليك فيه» لمعرفة من قام بالإشارة إليك. قد يكون هذا المنشور مرئياً للعامة، وذلك حسب إعدادات خصوصية الشخص الذي نشر المنشور.	• اكتب Privacy Checkup في حقل البحث بالصفحة الرئيسية وانقر على Visit • راجع من يمكنه رؤية تفاصيل ملفك الشخصي. تأكد من عدم وجود أي منها Public. • حدد من يمكنه رؤية منشوراتك بـ Friends أو Specific Friends أو Only Me. • تذكر أن صورة غلافك ستكون دائماً عامة. استبدلها بصورة لا تُظهر وجهك. اتبع هذه الخطوات الإضافية في Activity Log: • انقر على Use Activity Log لمراجعة يومياتك. أخفِ أو احذف أي شيء تريد إخفاؤه. تأكد من عدم وجود صور في Photo Review ستظهر الصور هنا إذا فعّلت ميزة التعرّف على الوجه، والتي يمكنك تعطيلها. • انقر على Activity You›re Tagged In لمعرفة من قام بالإشارة إليك. قد يكون هذا المنشور مرئياً للعامة، وذلك حسب إعدادات خصوصية الشخص الذي نشر المنشور.

بعد ذلك

للمستخدمين بالعربية	للمستخدمين بالإنجليزية
• ارجع إلى صفحة «الخصوصية» وانقر على «تقييد من يمكنه رؤية المنشورات السابقة». • راجع من يمكنه رؤية التطبيقات التي تستخدمها وكيف يمكن اكتشافك. • تحقق من إعدادات خصوصية الأصدقاء. قد تكون تعليقاتك أو إعجاباتك على صفحاتهم، وكذلك تعليقاتهم وإعجاباتهم على صفحتك، قابلة للاكتشاف. حتى لو لم يكن مُشارا إليك، قد يتمكن المصممون على تتبعك من البحث عن الأشخاص المرتبطين بك، مثل العائلة وزملاء العمل، أو الأشخاص الذين تفاعلوا مع الأقسام العامة في صفحتك على فيسبوك، مثل الإعجاب بصور غلافك أو صور ملفك الشخصي. • تأكد من ضبط إعدادات «تفضيلات الإعلانات». • في «الملف الشخصي والإشارات»، فعّل خيار مراجعة المنشورات التي تم الإشارة اليك فيها قبل ظهورها في يومياتك. • تحقق من كيفية ظهور ملفك الشخصي للآخرين عبر ميزة «عرض باسم».	• ارجع إلى صفحة Privacy وانقر على Limit Last Posts. • راجع من يمكنه رؤية التطبيقات التي تستخدمها وكيف يمكن اكتشافك. • تحقق من إعدادات خصوصية الأصدقاء. قد تكون تعليقاتك أو إعجاباتك على صفحاتهم، وكذلك تعليقاتهم وإعجاباتهم على صفحتك، قابلة للاكتشاف. حتى لو لم يكن مُشارا إليك، قد يتمكن المصممون على تتبعك من البحث عن الأشخاص المرتبطين بك، مثل العائلة وزملاء العمل، أو الأشخاص الذين تفاعلوا مع الأقسام العامة في صفحتك على فيسبوك، مثل الإعجاب بصور غلافك أو صور ملفك الشخصي. • تأكد من ضبط إعدادات Ads. • في Profile and Tagging فعّل خيار مراجعة المنشورات التي تم الإشارة اليك فيها قبل ظهورها في يومياتك. • تحقق من كيفية ظهور ملفك الشخصي للآخرين عبر ميزة View As.

«انستغرام»

قم بإنشاء حساب احترافي على «انستغرام» وقم بإغلاق حسابك الشخصي/الخاص تماما، او اجعله مقتصرا على الأصدقاء/العائلة.

للمستخدمين بالعربية	للمستخدمين بالإنجليزية
• قم بتغيير حسابك إلى «حساب خاص» ليتمكن فقط من توافق عليهم رؤية منشوراتك. • قم بإلغاء تحديد «إظهار حالة النشاط» في الرسائل وردود القصص حتى لا يتمكن أحد من رؤيتك عندما تكون متصلاً بالإنترنت. • في صفحة «تحرير الملف الشخصي»، قم بإلغاء تحديد خيار السماح باقتراح حسابك على ملفات شخصية أخرى. • يتم التحكم في أذونات الموقع الجغرافي من خلال إعدادات الخصوصية والأمان في تطبيق هاتفك. أوقف الوصول إلى الموقع الجغرافي، أو حدده عندما تريد المشاركة. • تحقق من خيارات الرسائل والقصص في عناصر التحكم «الإشارات» و«التعليقات».	• رقم بتغيير حسابك إلى Private Account ليتمكن فقط من توافق عليهم رؤية منشوراتك. • قم بإلغاء تحديد Show Activity Status في الرسائل وردود القصص حتى لا يتمكن أحد من رؤيتك عندما تكون متصلاً بالإنترنت. • في صفحة Edit Profile قم بإلغاء تحديد خيار السماح باقتراح حسابك على ملفات شخصية أخرى. • يتم التحكم في أذونات الموقع الجغرافي من خلال إعدادات الخصوصية والأمان في تطبيق هاتفك. أوقف الوصول إلى الموقع الجغرافي، أو حدده عندما تريد المشاركة. • تحقق من خيارات الرسائل والقصص في عناصر التحكم Tags وComment and Mentions.

«لينكدإن»

بما أن «لينكدإن» أداة احترافية للتواصل، فسيكون ملفاً شخصياً عاماً مع صورة شخصية متاحة للجميع. ومع ذلك، تُنشئ وكالات الاستخبارات بانتظام حسابات وهمية، وتتواصل معك، ثم تتحقق من شبكاتك. على سبيل المثال، أصبح «لينكدإن» ايضاً منصة شائعة للمحتالين الذين يعلنون عن وظائف وهمية.

للمستخدمين بالعربية	للمستخدمين بالإنجليزية
• من «ظهور ملفك الشخصي وشبكتك» في «الإعدادات والخصوصية»، تأكد من توافقك مع مدى مشاركة اسمك ومعلومات معارفك ومنطقتك. • راجع من يمكنه رؤية معلومات زملائك. قم بإلغاء هذه الخاصية لتحدد «أنت فقط» إذا كنت قد تواصلت مع مصادر حساسة. • اختر «نمط التصفح الخاص» حتى لا يتم التعرف على من تطّلع على ملفاتهم الشخصية. • حدد من يمكنه رؤية بريدك الإلكتروني بـ «الزملاء من الدرجة الأولى».	• ضمن Visibility of Your Profile & Network في Settings & Privacy تأكد من توافقك مع مدى مشاركة اسمك ومعلومات معارفك ومنطقتك. • راجع من يمكنه رؤية معلومات زملائك. حدد Only You إذا كنت قد تواصلت مع مصادر حساسة. • اختر Private Mode حتى لا يتم التعرف على من تطّلع على ملفاتهم الشخصية. • حدد من يمكنه رؤية بريدك الإلكتروني بـ 1st Degree Connections.

بعد ذلك

للمستخدمين بالعربية	للمستخدمين بالإنجليزية
• قم بإلغاء «عرض الملف الشخصي خارج لينكدإن» إذا كنت لا ترغب في ظهور ملفك الشخصي على منصات أخرى شريكة. • يمكنك إدارة من يمكنه اكتشاف ملفك الشخصي من بريدك الإلكتروني أو رقم هاتفك إذا لم يكن مرتبطا بك. • ضمن «ظهور نشاطك على «لينكدإن»، ثم «المتابعون»، حدد ما إذا كنت تريد أن يتابع جميع مستخدمي «لينكدإن» تحديثاتك العامة أم متابعيك فقط.	• اختر No ضمن Profile Visibility off LinkedIn إذا كنت لا ترغب في ظهور ملفك الشخصي على منصات أخرى شريكة. • يمكنك إدارة من يمكنه اكتشاف ملفك الشخصي من بريدك الإلكتروني أو رقم هاتفك إذا لم يكن مرتبطا بك. • ضمن Visibility of your LinkedIn activity ثم Followers حدد ما إذا كنت تريد أن يتابع جميع مستخدمي «لينكدإن» تحديثاتك العامة أم متابعيك فقط.

- احذر من مزامنة جهات الاتصال synced contacts إذا كانت لديك أي مصادر حساسة، وفكّر في إزالة جميع عناصر التقويم المتزامنة synced calendar.
- تأكد من عدم نشر سيرة ذاتية قديمة تحتوي على عنوان المنزل.
- احذف مدرستك الثانوية.

منصة X

يُعدّ موقع X أحد أبرز منصات التحرش الإلكتروني بالصحافيين، ومن أوائل الأماكن التي قد يبحث فيها المهاجمون عن ثغرات في حماية خصوصيتك.

اتخذ خطوات لتأمين ملفك الشخصي، بما في ذلك:

للمستخدمين بالعربية	للمستخدمين بالإنجليزية
• حدّد ما إذا كنت ترغب في استخدام صورة يمكن استخدامها في برامج التعرّف على الوجه لتتبعك، وما المعلومات التي تريد إضافتها إلى سيرتك الذاتية. • تجنّب إضافة تاريخ ميلادك إلى ملفك الشخصي، بالإضافة إلى موقعك الجغرافي، والذي يجب إلغاء تحديده ايضاً في «منشوراتك». • في قائمة «الخصوصية والأمان»، اختر «حماية منشوراتك» من قسم «الجمهور، والوسائط، والوسم» لتحديد من يمكنه رؤية منشوراتك. فعّل «الوسم بالصور». • حدّد من يمكنه إرسال رسائل إليك في قسم «الرسائل المباشرة». • حدّد ما إذا كان بإمكان الأشخاص الذين لديهم عنوان بريدك الإلكتروني أو رقم هاتفك العثور عليك في قسم «إمكانية الاكتشاف». • يجب توخي الحذر عند مزامنة جهات الاتصال على هاتفك مع X إذا كانت تتضمن مصادر حساسة. • قم بإيقاف تشغيل «الإعلانات المخصصة» في «تفضيلات الإعلانات» ضمن قسم «مشاركة البيانات والتخصيص». • قم بإلغاء خيار تخصيص تجربتك في «الهوية المستنتَجة» أو مشاركة معلوماتك مع شركاء العمل في «مشاركة البيانات مع شركاء العمل». • حدد ما إذا كنت تريد استخدام محتواك لتدريب الذكاء الاصطناعي الخاص بـ Grok، X.	• حدّد ما إذا كنت ترغب في استخدام صورة يمكن استخدامها في برامج التعرّف على الوجه لتتبعك، وما المعلومات التي تريد إضافتها إلى سيرتك الذاتية. • تجنّب إضافة تاريخ ميلادك إلى ملفك الشخصي، بالإضافة إلى موقعك الجغرافي، والذي يجب إلغاء تحديده ايضاً في Your Posts. • في قائمة Privacy and Safety اختر Protect Your Posts من قسم Audience, Media and Tagging لتحديد من يمكنه رؤية منشوراتك. قم بتعطيل Photo Tagging. • حدّد من يمكنه إرسال رسائل إليك في قسم Direct Messages. • حدّد ما إذا كان بإمكان الأشخاص الذين لديهم عنوان بريدك الإلكتروني أو رقم هاتفك العثور عليك في قسم Discoverability. • يجب توخي الحذر عند مزامنة جهات الاتصال على هاتفك مع X إذا كانت تتضمن مصادر حساسة. • قم بإيقاف تشغيل Personalized Ads في Ads Preferences ضمن قسم Data Sharing and Personalization. • قم بإلغاء خيار تخصيص تجربتك في Inferred Identity أو مشاركة معلوماتك مع شركاء العمل في Data Sharing With Business. • حدد ما إذا كنت تريد استخدام محتواك لتدريب الذكاء الاصطناعي الخاص بـ Grok، X.

المواقع الشخصية

إذا كان لديك موقع شخصي على الإنترنت، فسيتم ربط النطاق بعنوان ورقم هاتف واسمك وبريدك الإلكتروني. هذه طريقة سهلة للحصول على معلومات الاتصال بك.

- اذهب إلى DomainTools وأدخل عنوان URL لموقعك الإلكتروني وتحقق مما إذا كانت معلوماتك الشخصية متاحة للعامة.
- فكّر في اخفاء معلوماتك الشخصية باستخدام خدمة حماية الخصوصية مثل Who is Guard.
- تحقق من مسجّل نطاقك لمعرفة الخيارات المجانية أو المدفوعة التي يقدمها لإخفاء معلوماتك الشخصية.

تغيير كلمات المرور على الحسابات المخترقة

إذا تعرضت حساباتك للاختراق، فمن الممكن أن يكون اسم المستخدم وكلمة المرور الخاصين بك قد تم بيعهما ومن المرجح أن يكونا متاحين على الويب المظلم.

- have i been pwned؟ سيُعلمك هذا التطبيق ما إذا كانت كلمات مرورك وأسماء المستخدمين الخاصة بك قد تعرضت للاختراق في عمليات اختراق البيانات. غيّر كلمات المرور فوراً، وكذلك كلمات المرور الخاصة بالحسابات الأخرى التي تستخدم نفس اسم المستخدم وكلمة المرور.
- استخدم برامج إدارة كلمات المرور مثل Keeper Security لإنشاء كلمات مرور أو عبارات مرور طويلة وعشوائية.
- فعّل المصادقة الثنائية two-factor authentication، واستخدم تطبيقاً للمصادقة بدلا من الرسائل النصية القصيرة لتلقي رموز المصادقة الثنائية.
- استخدم بريداً إلكترونياً آمنا تماما محميا بمفتاح YubiKey مثل Gmail.
- فكّر في إنشاء اسم مستخدم غير قابل للاختراق بناءً على حساب بريد إلكتروني جديد تستخدمه فقط لغرض محدد، مثل بوابات التسوق.

وسطاء البيانات

هناك العشرات من وسطاء البيانات الذين يجمعون المعلومات في تقارير ثم يبيعونها. يمكنك إلغاء الاشتراك، ولكن قد يكون ذلك صعبا وقد يتطلب تكراره، مما يستغرق وقتا طويلاً.

- اشترك في خدمة إلغاء «اشتراك تلقائي» مثل DeleteMe أو Optery، وستتولى هذه الخدمة مهمة الغاء الاشتراك.
- استخدم تطبيق Permission Slip لإرسال طلبات إلغاء اشتراك تلقائية. يتميز الإصدار المدفوع بوظائف أفضل.

الملحق ٣. أدوات للصحافيين والمدراء

الاداة	الاستخدام
Tall Poppy	حزمة خدمات كاملة للحد من التحرش عبر الإنترنت، تشمل التدريب والاستجابة للحوادث وخدمة المرافقة لكبار الشخصيات
PEN America	التدريب
Troll Busters	التدريب والاستشارات
Theseus	تحليل التهديدات
DeleteMe	حذف المعلومات الشخصية
Permission Slip app	حذف المعلومات الشخصية
Mark Monitor	حماية العلامة التجارية، وإدارة النطاق، وحماية انتحال الشخصية
Proofpoint	الحماية ضد انتحال الشخصية
ZeroFox	مراقبة الويب المظلم وحماية انتحال الشخصية
Elv.ai	إدارة المحتوى ورصد التهديدات
Memetica	رصد التهديدات
Interfor	رصد وسائل التواصل الاجتماعي، ورصد التهديدات
Ontic	تحليل التهديدات والتحقيقات
Dataminr	رصد التهديدات
JustDeleteMe	حذف الحسابات القديمة
TweetDelete	حذف الحسابات القديمة على موقع X
tweeteraser	حذف الحسابات القديمة على موقع X
Google's PerspectiveAPI	إدارة التعليقات

مصادر أخرى

- مؤسسة Pen America دليل Online Harassment Field Manual
- قائمة التحقق easy to use digital safety checklist في موقع Zebra Crossing
- استشارات فردية One-to-one safety consultations تقدمها International Women's Media Foundation
- تقرير التحرش عبر الانترنيت Online Harassment of Journalists report الصادر عن منظمة صحافيون بلا حدود.

INSI

INTERNATIONAL
NEWS SAFETY
INSTITUTE

International News Safety Institute
C/O Thomson Reuters Foundation
5 Canada Square
Floor 8
Canary Wharf
London E5 14AQ

info@newssafety. org
www. newssafety. org
@INSInews