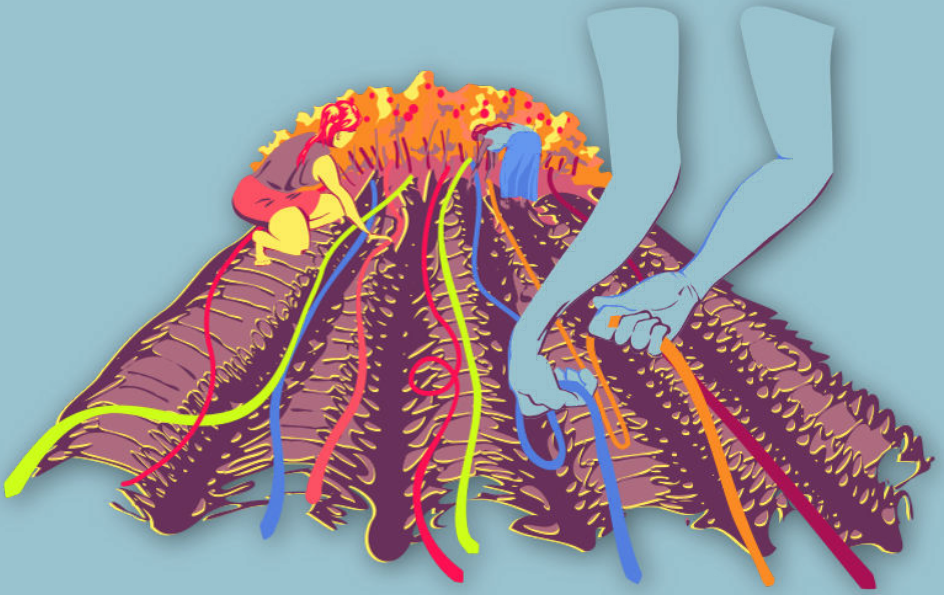




النساء فى فضاء الإنترنت



تحديد الحل الأفضل

نموذج المخاطر القائمة على النوع الاجتماعي

**INSTITUTE FOR
WAR & PEACE REPORTING**



© 2019– Institute For War And Peace Reporting

<https://iwpr.net/>



نَسَبُ الْمُصَنَّفِ - الترخيص بالمثل 4.0 دولي

<https://creativecommons.org/licenses/by-sa/4.0/deed.ar>

المحتويات

٥	١ نموذج المخاطر القائمة على النوع الاجتماعي
٧	إدارة الجلسة
٧	الجزء الأول - تحديد المخاطر والإحتمالات
٩	الجزء الثاني - تحديد مدى التأثير
١٠	الجزء الثالث - وضع إستراتيجيات للحلول
١١	الجزء الثالث - وضع إستراتيجيات للحلول
١١	المراجع

باب ١

نموذج المخاطر القائمة على النوع الإجتماعي

- الأهداف: في هذه الجلسة، ستوجهن المشاركات في عملية من مراحل عدّة، أولها تحديد المخاطر المحدقة بهن، كنساء وكمدافعات عن حقوق الإنسان، وثانيها وضع إستراتيجية أمنية فردية للتعامل مع هذه المخاطر.
- الطول: من 40 إلى 5 دقيقة
- الشكل: تمرين
- مستوى المهارة: أساسي
- المعرفة المطلوبة:
- متفاوتة (راجعن التوصيات أدناه)
- جلسات/تمارين ذات صلة:
- لنبدأ بتوثيق الحالات!^١
- الخطط والبروتوكولات الأمنية الخاصة بالمنظمة^٢

^١<https://vrr.im/899f>

^٢<https://vrr.im/f75c>

• المواد اللازمة:

- أقلام خطاطة ملونة

- أقلام وأقلام رصاص

- ألواح ورقية أو لوح أبيض/أسود

• التوصيات: من الممكن تقديم هذه الجلسة بطرق مختلفة: قدم الجلسة كاملة في بداية التدريب، ومن الجزء الثالث حتى النهاية بعد أن تقدّم أدوات وممارسات محددة أكثر في جلسات سابقة؛ (a) وجّه المشاركات في الجزئين الأول والثاني من هذه الجلسة عند بداية التدريب، ومن ثمّ قدّم من الجزء الثالث حتى النهاية بعد أن تقدّم أدوات وممارسات محددة أكثر في جلسات سابقة؛ (b) قسّم الجلسة إلى ثلاث جلسات صغيرة فردية ابتداءً من الجزء الأول عند بداية التدريب، والجزء الثاني في منتصفه بعد أن تتسنى للمشاركات فرصة مناقشة الأمن الرقمي في بيئاتهن الشخصية، والجزء الثالث عند النهاية بعد أن تقدّم أدوات وممارسات محددة أكثر في جلسات سابقة؛ (c) يمكن تنفيذ محتوى هذه الجلسة في البيئة الفردية الشخصية وضمن منظمة على حدٍ سواء، وهذا مفيد حين يقدم التدريب لأعضاء جماعة أو منظمة مدافعات عن حقوق الإنسان.

من الممكن تقديم هذه الجلسة بطرق مختلفة: قدم الجلسة كاملة في بداية التدريب، ومن الجزء الثالث حتى النهاية بعد أن تقدّم أدوات وممارسات محددة أكثر في جلسات سابقة؛ (a) وجّه المشاركات في الجزئين الأول والثاني من هذه الجلسة عند بداية التدريب، ومن ثمّ قدّم من الجزء الثالث حتى النهاية بعد أن تقدّم أدوات وممارسات محددة أكثر في جلسات سابقة؛ (b) قسّم الجلسة إلى ثلاث جلسات صغيرة فردية ابتداءً من الجزء الأول عند بداية التدريب، والجزء الثاني في منتصفه بعد أن تتسنى للمشاركات فرصة مناقشة الأمن الرقمي في بيئاتهن الشخصية، والجزء الثالث عند النهاية بعد أن تقدّم أدوات وممارسات محددة أكثر في جلسات سابقة؛ (c) يمكن تنفيذ محتوى هذه الجلسة في البيئة الفردية الشخصية وضمن منظمة على حدٍ سواء، وهذا مفيد حين يقدم التدريب لأعضاء جماعة أو منظمة مدافعات عن حقوق الإنسان. تتضمن هذه الجلسة نقاش مفصّل عن المخاطر الشخصية من وجهة نظر بيئة مدافعات عن حقوق الإنسان - خاصة عند الوصول إلى الجزء الثالث (لا سيما إن كانت هذه الجلسة مقدمة دفعة واحدة وغير مقسّمة إلى أجزاء منفصلة)، قد تبدأ معالم القلق أو الإجهاد

بالظهور على المشاركات. لذا، يصبح من الضروري جداً لكن كمدربات أن تقمن بإدارة مستوى الإجهاد في الغرفة. إحرصن على تذكير المجموعة بشكلٍ دوريٍّ أن هذه الجلسة ستركّز في النهاية على تحديد الإستراتيجيات والأدوات والشبكات أو الحلفاء القادرين على مساعدتهن على مواجهة المخاطر، هدفكن هو عدم إخافتهن، حيث تتوفر نشاطات كثيرة يمكنهن إعتماها لمكافحة العنف على الإنترنت.

هذه الجلسة مُعدّة إستناداً إلى جلسة وضعتها جينيفر شولتي Jennifer Schulte في معسكر تدريب معهد صحافة الحرب والسلام المخصصة لموضوع الجندر في نيسان/أبريل 2016 في برلين، ألمانيا، بالتشاور مع "دليل إدارة مخاطر الكوارث للإعلاميين الاجتماعيين" (الأونسكو)

إدارة الجلسة

الجزء الأول - تحديد المخاطر والإحتمالات

١. إبدأن الجلسة بنقاش جماعي حول المخاطر المحددة التي تواجهها أو قد تواجهها المدافعات عن حقوق الإنسان - ذكرن المشاركات بالمعنى المقصود من كلمة "خطر": إحتمال حدوث أمرٍ ما قد يتسبب بضرر أو أذية. إكتبن بعض الأمثلة المحددة عن المخاطر التي قدمنها المشاركات - راجعنها بعد أن تحصلن على عددٍ مناسبٍ منها.

٢. وجهن النقاش نحو الطبيعة المتقلبة للمخاطر - إحتمالية حدوث الخطر تبدّل وفقاً لعدد من العوامل الخارجية التي تزيد أو تُخفض من إحتمالية حدوث الخطر حين تصبح هذه العوامل متوفرة أكثر أو أقل - على سبيل المثال:

يرتفع خطر إعتراض رسالة نصيّة من قبل الخصوم عند إستخدام تطبيق إرسال الرسائل النصية القصيرة الإعتيادي، ولكنه يخفض في حال أرسلت مشفرة عبر تطبيق كتطبيق سيجنال؛

وعلى نحو مماثل، في حال كان شخص ما ناشطاً مستهدفاً في دولته، خطر إعتراض رسالة

يرتفع بشكل ملحوظ في حال أُرسِلت بواسطة تطبيق الرسائل النصية القصيرة على هاتف متصل بشبكة اتصالات دولته، ولكن منسوب هذا الخطر ينخفض بشكل ملحوظ، في حال أُرسِلت بواسطة تطبيق كتطبيق سيجنال من على شبكة اتصالات في دولة أجنبية؛ ما يرد أعلاه مجرد مثال بسيط عن كيفية تأثير العوامل التقنية الخارجية على احتمالية حدوث خطر ما - ولكن ماذا عن الجندر كعنصر من عناصر الخطر؟ هل المخاطر المحدقة بالمدافعات عن حقوق الإنسان هي ذاتها تلك المحدقة بالمدافعين عن حقوق الإنسان الذين لا يعرفون عن أنفسهم كنساء؟

٣. إرسن جدولاً شبيهاً بالجدول الوارد أدناه على ورقة كبيرة من أوراق الألواح الورقية، وضعن عدداً من المخاطر الرقمية تحت خانة "الخطر الرقمي"، استخدمن المخاطر المختلفة المناقشة والمشاركة في المرحلة الأولى كأمثلة (إحرصن على ترك الجانب الأيسر خالياً لإضافة أعمدة إضافية لأجزاء أخرى من هذه الجلسة):

الخطر الرقمي	إحتمالية الحدوث

٤. بعد الإنتهاء من اللائحة الواردة أعلاه، ستعملن الآن مع المشاركات على تحديد احتمالية حدوث كل خطر من المخاطر في الواقع - يسهل إجراء هذا التمرين في حال كانت كل المشاركات من الخلفية والبيئة ذاتها (الدولة، نوع النشاط... إلخ)؛ في حال تواجد مشاركات من خلفيات متعددة ومختلفة، قد ترغبن بتقديم شخص إقتراضي كمثال في هذه الجلسة.

٥. يمكنكن تحديد مقياس لقياس احتمالات حدوث هذه المخاطر. على سبيل المثال، يمكنكن استخدام مقياس بسيط من 1 إلى 5، حيث الدرجة الخامسة تدل إلى أن احتمالية تحول الخطر إلى حقيقة "عالية جداً" وحيث الدرجة الأولى تدل إلى أن

إحتمالية تحوّل الخطر إلى حقيقة “منخفضة جداً”. ما الدرجة التي يمكن إعطاؤها لكل خطر؟ يمكن البدء بممل الجدول للمجموعة أثناء مناقشة كل خطر على حدة، وليدو كما يلي:

إحتمالية الحدوث 1=منخفضة جداً 5=مرتفعة جداً	الخطر الرقمي
4	الفرق على رابط في بريد إلكتروني فيه برمجية خبيثة عن طريق الخطأ!
2	تعرض مكاتبنا للمداومة من قبل الشرطة لمصادرة أقرصنا الصلبة أو أجهزة أخرى!

الجزء الثاني - تحديد مدى التأثير

٦. والآن وقد عملت مع المشاركات على تحديد أمثلة عن المخاطر ووضع نظام بسيط لتحديد إحتمالية حدوث كل خطر من المخاطر، إشرح لهن أنكن ستنقلن الآن إلى المرحلة التالية، ألا وهي تحديد مدى التأثير الحقيقي لهذه المخاطر، أو ما هي نتائجها على الفرد والمنظمة والشبكة... إلخ، في حال صار خطر ما واقعاً.

٧. إشرح أن آثار المخاطر، تماماً كالمخاطر نفسها، متقلبة هي الأخرى. تعتمد طبيعة التأثير وحدته أيضاً على عدد من العوامل الخارجية. هل ستطال تداعيات آثار المخاطر الفرد أم المنظمة؟ قد تطال الفرد والمنظمة على حدٍ سواء، وفي هذه الحال، ما مدى تشابه أو اختلاف هذين التأثيرين؟

٨. في الجزء التالي من هذه الجلسة، ستقمن بتحديد مقياس لقياس التأثير - قد يستخدم هذا المقياس كأداة قياس كمي مشابه للذي أستخدم لقياس إحتمالية الحدوث، أو قد يستخدم كأداة قياس نوعي يصف طبيعة وتفاصيل التأثير بدقة. الخيار يعود لكن أنتن والمشاركات - المهم في كل ذلك هو أن تشدد هذه الجلسة على مخاطر وتداعيات محددة بحيث يصبح من السهل على المشاركات فهمها على أنها ليست مجرد مفاهيم نظرية

(لأغراض هذه الجلسة، سنستعين بمقياس كمي).

٩. إشرح للمجموعة أن إستباق رد فعلك الممکن مع آثار المخاطر جزء مهم من فهم المخاطر وقياسها - إسألن المشاركات عن تفاعلهن المحتمل على الصعيد الشخصي تجاه خطر معين؟ ومن ثم ناقشن كيف - تماماً كالأحتمالية والتأثير - ستضعن مقياساً لقياس رد الفعل الذي قد يكون هو الآخر كميّاً أو نوعياً (ولكن لأغراض هذه الجلسة سنستعين بمقياس كمي).

إستناداً إلى ما بدأتن بشرحه في المرحلة الخامسة، سيثبه جدولكن الآن الجدول المبين أدناه كمثال:

رد الفعل	الأثر	إحتمالية الحدوث	الخطر الرقمي
1 - هائل، تحت السيطرة 5 - حالة ذعر وتوتر شديد	1- خطورة منخفضة 5- خطورة مرتفعة	1- منخفضة جداً 5- مرتفعة جداً	النظر على رابط في بريد إلكتروني فيه برقية خبيثة عن طريق الخطأ!
3	3	4	
5	5	2	تعرض مكاتبنا للعداوة من قبل الشرطة لمصادرة أرقامنا الصلبة لأجهزة أخرى!

الجزء الثالث - وضع إستراتيجيات للحلول

١٠. كما سبق وذكرنا في التوصيات، تتضمن هذه الجلسة نقاشاً مفصلاً عن المخاطر الشخصية من منظور بيئة المدافعات عن حقوق الإنسان - قد تبدأ معالم القلق أو الإجهاد بالظهور على المشاركات الآن. إحرصن على تذكير المجموعة بشكلٍ دوريّ أن هذه الجلسة ستركّز في النهاية على تحديد الإستراتيجيات والأدوات والشبكات أو الحلفاء القادرين على مساعدتهن على مواجهة المخاطر؛ هدفكن هو عدم إحاقتهن، حيث تتوفر نشاطات كثيرة يمكنهن إعتمادها لمكافحة العنف على الإنترنت.

١١. والآن وقد قمتن بتحديد وقياس إحتمالية وأثر ورد الفعل الخاصة بكل خطر من المخاطر، إشرحن أن هذا الجزء من الجلسة مخصص للتفكير في الحلول. لكل خطر من المخاطر، إسألن المشاركات: ماذا يمكن أن تفعلن لمعالجة خطر ما و/أو منعه حدوثه؟ الإجابات

المعطاء من قبل المجموعة ستختلف وتبدّل وفقاً للمرحلة التي ستقدم فيها هذه الجلسة خلال عملية التدريب - في حال قدمتم هذه الجلسة في بداية التدريب، قد لا تتوفر لديهن إجابات مفصّلة جداً، ولكن إن قدمتم هذه الجلسة عند نهاية التدريب عندها ستصبح إجاباتهن أكثر إرتباطاً بشأن بعض الأدوات والممارسات.

١٢. إستكمالاً للجدول الذي بدأتم بنائه خلال هذه الجلسة، قمن بإضافة عمود أخير هو عمود “ماذا يمكنني أن أفعل؟” - وفي هذا العمود، أكتبن الإجابات المقدمة من قبل المجموعة خلال المرحلة الحادية عشرة. وبعد الإنتهاء من ذلك، إعرضن الجدول في مكان ظاهر في غرفة التدريب طيلة الفترة المتبقية من ورشة العمل لكي تتمكن المشاركات من إعادة قراءة وتحليل إجاباتهن. قد يساعد ذلك المشاركات في معرفة ما يجب إضافته إلى الجدول إن اقتضى الأمر ذلك، مما يشكّل قاعدة متينة لتصميم بروتوكول أمن رقمي. يرد أدناه نموذج عن الجدول النهائي المثالي:

الخطر الرقمي	إحتماله الحدوث	الأثر	رد الفعل	ماذا يمكنني أن أفعل؟
	1- منخفضة جداً 5- مرتفعة جداً	1- خطيرة منخفضة 5- خطيرة مرتفعة	1 - هائل، تحت السيطرة 5- حالة ذعر وتوتر شديد	
الشر على رابط في بريد إلكتروني فيه بريجة خيئة عن طريق الخطأ!	3	4	3	تزيلي بريجة مكافحة فيروسات وتبيها؛ تنبيه الآخرين في شبكتي لمنظمتي في حال ظهر لديهم الرابط ذاته
تعرض مكاتبنا للضاهمة من قبل الشرطة لضائرة أفراسا الضاللة أو أجرة أخرى!	4	5	5	القيام بنسخ احتياطية عن بياناتنا بشكل دوري، ونحفظها في مكان آمن خارج مكاتبنا، وتنبيه الآخرين في شبكتنا إذا ما تعرضت معلومات خاصة بهم للكشف

الجزء الثالث - وضع إستراتيجيات للحلول

المراجع

<https://ssd.eff.org/en/module/assessing-your-risks> •