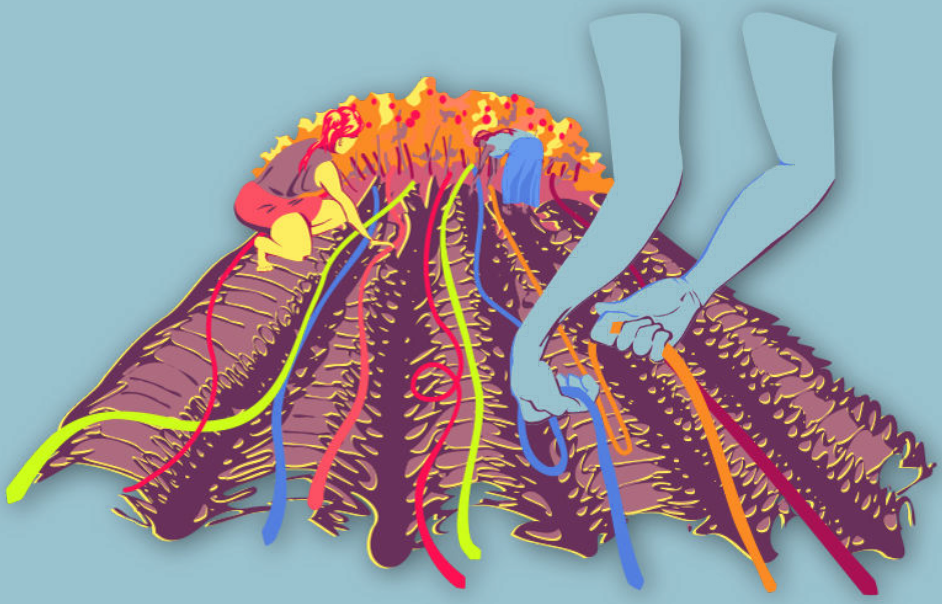

تحديد الحل الأفضل

تحديد الحل الأفضل

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

باب ١

نموذج المخاطر القائمة على النوع الإجتماعي

- **الأهداف:** في هذه الجلسة، ستوجهن المشاركات في عملية من مراحل عدّة، أوّلها تحديد المخاطر المحدقة بهن، كنساء وكمدافعات عن حقوق الإنسان، وثانيها وضع إستراتيجية أمنية فرديّة للتعامل مع هذه المخاطر.
- **الطول:** من 40 إلى 5 دقيقة
- **الشكل:** تمرين
- **مستوي المهارة:** أساسي
- **المعرفة المطلوبة:**
  - متفاوتة (راجعن التوصيات أدناه)
- **جلسات/تمارين ذات صلة:**
  - لنبدأ بتوثيق الحالات![1]
  - الخطط والبروتوكولات الأمنية الخاصة بالمنظمة[2]

[1] https://vrr.im/899f
[2] https://vrr.im/f75c

- **المواد اللازمة:**
  - أقلام خطاطة ملوّنة
  - أقلام وأقلام رصاص
  - ألواح ورقية أو لوح أبيض/أسود
- **التوصيات:** من الممكن تقديم هذه الجلسة بطرق مختلفة: قدمن الجلسة كاملة في بداية التدريب، ومن الجزء الثالث حتى النهاية بعد أن تقدّمن أدوات وممارسات محددة أكثر في جلسات سابقة؛ (a) وجّهن المشاركات في الجزئين الأوّل والثاني من هذه الجلسة عند بداية التدريب، ومن ثمّ قدّمن من الجزء الثالث حتى النهاية بعد أن تقدّمن أدوات وممارسات محددة أكثر في جلسات سابقة؛ (b) قسمن الجلسة إلى ثلاث جلسات صغيرة فردية إبتداءً من الجزء الأوّل عند بداية التدريب، والجزء الثاني في منتصفه بعد أن تتسنى للمشاركات فرصة مناقشة الأمن الرقمي في بيئاتهن الشخصية، والجزء الثالث عند النهاية بعد أن تقدّمن 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 يقدّم التدريب لأعضاء جماعة أو منظمة مدافعات عن حقوق الإنسان.

من الممكن تقديم هذه الجلسة بطرق مختلفة: قدمن الجلسة كاملة في بداية التدريب، ومن الجزء الثالث حتى النهاية بعد أن تقدّمن أدوات وممارسات محددة أكثر في جلسات سابقة؛ (a) وجّهن المشاركات في الجزئين الأوّل والثاني من هذه الجلسة عند بداية التدريب، ومن ثمّ قدّمن من الجزء الثالث حتى النهاية بعد أن تقدّمن أدوات وممارسات محددة أكثر في جلسات سابقة؛ (b) قسمن الجلسة إلى ثلاث جلسات صغيرة فردية إبتداءً من الجزء الأوّل عند بداية التدريب، والجزء الثاني في منتصفه بعد أن تتسنى للمشاركات فرصة مناقشة الأمن الرقمي في بيئاتهن الشخصية، والجزء الثالث عند النهاية بعد أن تقدّمن 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 يقدّم 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 جدًا لكن كمدربات أن تقمن بإدارة مستوى الإجهاد في الغرفة. 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 إخافتهن، حيث تتوفر نشاطات كثيرة يمكنهن إعتمادها لمكافحة العنف على الإنترنت.

هذه الجلسة مُعدّة إستنادًا إلى جلسة وضعتها جينيفر شولتي Jennifer Schulte في معكسر 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 الأوّل – تحديد المخاطر والإحتمالات

١. إبدأن الجلسة بنقاش جماعي حول المخاطر المحددة التي تواجهها أو قد تواجهها المدافعات عن حقوق الإنسان – ذكّرن 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 تتبدّل وفقًا لعدد من العوامل الخارجية التي تزيد أو تخفض 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 ينخفض في حال أرسلت مشفّرة عبر تطبيق كتطبيق سيجنال؛

وعلى نحو مماثل، في حال كان شخص ما ناشطًا مستهدفًا في دولته، خطر إعتراض رسالة

يرتفع بشكلٍ ملحوظ في حال أُرسلت بواسطة تطبيق الرسائل النصية القصيرة على هاتف متصل بشبكة إتصالات دولته، ولكن منسوب هذا الخطر ينخفض بشكلٍ ملحوظ، في حال أُرسلت بواسطة تطبيق كتطبيق سيجنال من على شبكة إتصالات في دولة أجنبية؛

ما يرد أعلاه مجرّد مثال بسيط عن كيفية تأثير العوامل التقنية الخارجية على إحتمالية 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. إرسمن جدولاً شبيهًا بالجدول الوارد أدناه على ورقة كبيرة من أوراق الألواح الورقية، وضعن عدداً من المخاطر الرقمية تحت خانة "الخطر الرقمي"، إستخدمن المخاطر المختلفة المناقشة والمشاركة في المرحلة الأولى كأمثلة (إحرصن على ترك الجانب الأيسر خاليًا 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 إحتمالية 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 إفتراضي كمثال في هذه الجلسة.

٥. يمكنكن تحديد مقياس لقياس إحتماليات حدوث هذه المخاطر. على سبيل المثال، يمكنكن إستخدام مقياس بسيط من 1 إلى 5، حيث الدرجة الخامسة تدل إلى أن إحتمالية تحوّل الخطر إلى حقيقة "عالية جدًا" وحيث الدرجة الأولى تدل إلى أن

إحتمالية تحوّل الخطر إلى حقيقة "منخفضة جدًا". ما الدرجة التي يمكن إعطاؤها لكل خطر؟ يمكنكن البدء بملء الجدول للمجموعة أثناء مناقشة كل خطر على حدة، ليبدوكما يلي:

الخطر الرقمي	إحتمالية الحدوث 1= منخفضة جدًا 5= مرتفعة جدًا
النقر على رابط في بريد إلكتروني فيه برمجية خبيثة عن طريق الخطأ!	4
تتعرض مكاتبنا للمداهمة من قبل الشرطة لمصادرة أقراصنا الصلبة أو أجهزة أخرى!	2

الجزء الثاني – تحديد مدى التأثير

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

٧. إشرحن أن آثار المخاطر، تمامًا كالمخاطر نفسها، متقلبة هي الأخرى. تعتمد طبيعة التأثير وحدّته أيضًا على عدد من العوامل الخارجية. هل ستطال تداعيات أثار 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 كمّي مشابه للذي أستخدم لقياس إحتمالية الحدوث، أو قد يستخدم كأداة قياس نوعي يصف طبيعة وتفاصيل التأثير بدقّة. 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 مجرّد مفاهيم نظرية

(لأغراض هذه الجلسة، سنستعين بمقياس كمّي).

٩. إشرحن للمجموعة أن إستباق رد فعلكن الممكن مع آثار المخاطر جزء مهمٌ من فهم المخاطر وقياسها – إسألن المشاركات عن تفاعلهن المحتمل على الصعيد الشخصي تجاه خطر معيّن؟ ومن ثمّ ناقشن كيف – تمامًا كالإحتمالية والتأثير – ستضعن مقياسًا لقياس رد الفعل الذي قد يكون هوالآخر كمّيًا أو نوعيًا (ولكن لأغراض هذه الجلسة سنستعين بمقياس كمّي).

إستنادًا إلى ما بدأتن بشرحه في المرحلة الخامسة، سيشبه جدولكن الآن الجدول المبيّن أدناه كمثال:

الخطر الرقمي	إحتمالية الحدوث 1= منخفضة جدًا 5= مرتفعة جدًا	الأثر 1= خطورة منخفضة 5= خطورة مرتفعة	رد الفعل 1 = هادئ، تحت السيطرة 5 = حالة ذعر وتوتر شديد
النقر على رابط في بريد إلكتروني فيه برمجية خبيثة عن طريق الخطأ!	4	3	3
تعرض مكالمتنا للمداهمة من قبل الشرطة لمصادرة أقراصنا الصلبة أوأجهزة أخرى!	2	5	5

الجزء الثالث – وضع إستراتيجيات للحلول

١٠. كما سبق وذكرنا في التوصيات، تتضمن هذه الجلسة نقاشًا مفصّلاً عن المخاطر الشخصية من منظور بيئة المدافعات عن حقوق الإنسان – قد تبدأ معالم القلق أوالإجهاد 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 هوعدم إخافتهن، 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

المعطاة من قبل المجموعة ستختلف وتتبدّل وفقًا للمرحلة التي ستقدمن فيها هذه الجلسة خلال عملية التدريب – في حال قدمتن هذه الجلسة في بداية التدريب، قد لا تتوفر لديهن إجابات مفصّلة جدًا، ولكن إن قدمتن هذه الجلسة عند نهاية التدريب عندها ستصبح إجاباتهن أكثر إرتباطًا بشأن بعض الأدوات والممارسات.

١٢. إستكمالاً للجدول الذي بدأتن 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	إحتمالية الحدوث 1= منخفضة جدًا 5= مرتفعة جدًا	الأثر 1= خطورة منخفضة 5= خطورة مرتفعة	رد الفعل 1 – هادئ، تحت السيطرة 5 – حالة ذعر وتوتر شديد	ماذا يمكنني أن أفعل؟
النقر على رابط في بريد إلكتروني فيه برمجية خبيثة عن طريق الخطأ!	3	4	3	تنزيل برمجية مكافحة فيروسات وتثبيتها؛ تنبيه الآخرين في شبكتي إصطفني في حال ظهر لديهم الرابط ذاته
تعرض مكاتبنا للمداهمة من قبل الشرطة لمصادرة أقراصنا الصلبة أو أجهزة أخرى!	4	5	5	القيام بنسخ احتياطية عن بياناتنا بشكلٍ دوري، وتخزينها 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

باب ٢

القرارات المرتبطة بالأمن الرقمي

- **الأهداف:** الهدف من هذه الجلسة هوتعريف النساء بعملية التفكير الإستراتيجي النقدي المستخدمة في صنع القرارات الواعية بشأن تنفيذ وتطبيق ممارسات وأدوات الأمن الرقمي، وتحديد الموارد التي ستساعدهن في متابعة المستجدات بعد هذا التدريب.
- **الطول:** 90 دقيقة
- **الشكل:** جلسة
- **مستوي المهارة:** متوسط
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
- **جلسات/تمارين ذات صلة:**
  - وجهات النظر الشخصية حيال الأمن[١]
  - كيف يعمل الإنترنت؟[٢]
  - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟[٣]

---

١ https://vrr.im/9339
٢ https://vrr.im/7ba9
٣ https://vrr.im/47ba

- **المواد اللازمة:**
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
  - شرائح بالنقاط المفتاحية الواردة أدناه
  - نسخ عن الرسوم البيانية الخاصة بحالات المدافعات عن حقوق الإنسان (راجعن الملاحق)
- **التوصيات:** بما أن هذه الجلسة تستوجب حد أدنى من المعرفة الأساسية بمفاهيم الأمن الرقمي، يفضل تقديمها في تدريب على عدّة أيّام أو كجزء من ورشة عمل قصيرة المدّة، تركّز أكثر على تصميم البروتوكولات الأمنية الفردية.

إدارة الجلسة

الجزء الأوّل – المقدمة

١. إبدأن بسؤال المشاركات عن عدد المرات التي طرحن فيها على مدربة أو خبيرة أخرى سؤالاً عن الأمن الرقمي، فتلقين إجابات مختلفة في كل مرة بحسب الشخص الذي طرح عليه السؤال – هذا أمرٌ محيّر، أليس كذلك؟ أحيانًا حين نطلب نصائح عن الأمن الرقمي، قد لا يشرح الأشخاص الذين يقدمون لنا المساعدة سير العملية، بل يكتفون "بحلّ المشكلة" على أجهزتنا من دون أن يشرحوا ما قاموا به - ألا تفضلن معرفة ماهية الحلّ المناسب لكي تتمكّن من تطبيقه مرة أخرى في حال واجهتن المشكلة مرّة أخرى؟

٢. إشرحن لهن أن الهدف من هذه الجلسة هو تعريف المجموعة بعملية التفكير النقدي الإستراتيجي المستخدمة في صنع القرارات الواعية بشأن تطبيق وتنفيذ ممارسات وأدوات الأمن الرقمي، وتحديد الموارد التي من شأنها مساعدتهن على متابعة المستجدات بعد التدريب. ناقشن فكرة أن الأمن الرقمي ليس محصورًا فقط بتنزيل تطبيقات جديدة، بل تشمل أيضًا معرفة ممارساتكن جيّدًا وإتخاذ قرارات واعية لبناء بيئة أكثر أمانًا لكنّ.

الجزء الثاني – كيف تم بناء البرمجيات التي تستخدمنها؟

٣. إعرضن أو إشرحن مرّة أخرى للمشاركات بعض الأدوات أوالمنصات التي سبق لكن أن قمتن بتقديمها للمشاركات (مثلاً: سيجنال، برمجية إيتش تي تي بي إس إفريوير، أبسكوراكام، سكايب، تليغرام، إلخ) – أطلبن منهن تحديد نوع كل برمجية منها إستناداً إلى المعلومات المتاحة لهن، من قبيل الموقع الإلكتروني الخاصة بالأداة.

٤. إشرحن ما هي البرمجيات التجارية (المغلقة المصدر): ما هي خصائص هذا النوع من البرمجيات (قدمن أمثلة عن برامج). ما هي تداعيات استخدام هذا النوع من البرمجيات على الأمن الرقمي؟

٥. إشرحن ما هي البرمجيات المفتوحة المصدر: ما هي خصائص هذا النوع من البرمجيات (قدمن أمثلة عن برامج). ما هي تداعيات استخدام هذا النوع من البرمجيات على الأمن الرقمي؟ إحرصن أيضًا على توضيح ما هو مجتمع البرمجيات المفتوحة المصدر والتدقيق في البرمجيات لمزيد من التوضيح.

٦. إشرحن عن مشاريع البرمجيات الحرة والمفتوحة المصدر (Free/Libre and Open Source Software FLOSS): ما هي خصائص هذا النوع من البرمجيات (قدمن أمثلة عن برامج). ما هي تداعيات استخدام هذا النوع من البرمجيات على الأمن الرقمي؟

الجزء الثالث – التفكير في المستخدمين؟

٧. في حال سبق لكن أن قدمتن جلسة بمن تثقن؟ من وحدة "إعادة النظر بعلاقتنا بالتكنولوجيا"، ذكرن المجموعة بالأمثلة عن الخصوم التي قدمنها، وفي حال قدمتن تمرين نموذج المخاطر القائمة على النوع الاجتماعي، ذكرن المجموعة بنموذج المخاطر الذي أنشأنه معًا.

الهدف من كل ذلك في النهاية تعزيز فكرة أن لكل شخص فينا حاجات خاصة به أو أن الجميع لا يواجهون المخاطر ذاتها من حيث الأمن الرقمي:

- عند البحث عن حلّ في مجال الأمن الرقمي، عليكن تعلّم أكبر كمية من المعلومات عن الحاجة التي تم تحديدها. ماذا تردن فعله أو جعله أكثر أمانًا؟ ما هو المكان الأكثر أمانًا الذي يمكنكن الإحتفاظ فيه بأمرٍ ما؟ ممن نحن بحاجة للحماية؟
- فكرن في المنصات أو الأدوات المستخدمة من قبلكن حاليًا – إلى أي مدى أو هل من الممكن أن توافقن على إستبدالها بمنصات أو أدوات جديدة أو تغيير طريقة استخدامكن لمنصاتكن أو أدواتكن الحالية؟
- إلى أي مدى تؤثر القدرة على الاتصال على أي حلّ ممكن في مجال الأمن الرقمي؟ هل تتوفر لكن عادةً إمكانية اتصال ثابتة وموثوق بها بالإنترنت، أو هل تحتجن إلى العمل من دونها لفترات طويلة؟
- في حال كنتن تفكرن في حلّ في مجال الأمن الرقمي ضمن بيئة منظمة أو جماعة، فكرن في الأجهزة أو أنظمة التشغيل المختلفة المستخدمة من قبل أعضاء تلك المجموعة – هل سينجح الحلّ لدى الجميع؟ هل سينجح الحلّ لدى أغلبية الأعضاء؟

الجزء الرابع – التفكير في الأدوات

٨. الأسئلة التالية هي أسئلة لابد من طرحها عند التفكير في إستخدام منصة أو أداة جديدة – إشرحن ذلك للمشاركات. لا حاجة لشرحها والإجابة عنها كلها (فهي أسئلة محددة جدًا)، ولكن إحرصن على قراءتها بصوتٍ عالٍ وإشرحن بإيجاز سبب أهمية كل واحد منها:

هل البرمجية مجانية ومفتوحة المصدر؟

هل تعرفن من برمج الأداة، أو من موّل المشروع؟

هل هي متوفرة بلغتكن؟

إبحثن عن منشورات مدونات أو أي موقع يأتي على ذكر الأداة على الإنترنت، ماذا وجدتن؟ متى أُدخل التحديث الأخير على الأداة؟ هل النسخة المتوفرة نسخة ثابتة من

الأداة؟ هل توفر جهة ما الدعم التقني للأداة أم هي مدعومة من متطوعين/ات؟ ما مدى سهولة إعدادها؟ هل خضعت الأداة للإختبار أو التدقيق؟ هل الأداة متوفرة لنظام التشغيل الذي تستخدمنه على أجهزتكن؟ تحققن من شروط الخدمة الخاصة بالأداة – هل توافقن عليها أم تبدو لكن مريبة؟ في حال كانت الأداة أو المنصة تستعين بخوادم عن بعد، هل تعرفن أين تتواجد هذه الخوادم؟ هل قام مطورها في يوم من الأيام بتسليم بيانات أي مستخدم إستجابة لطلب حكومةٍ ما؟ كيف تُخزن المعلومات على خوادمها؟ هل هي مشفّرة، وإن كان الأمر كذلك هل يمتلك المشروع طريقة لفك التشفير والوصول إليها؟ في حال ساورتكن أي شكوك، إبحثن عن طريقة للتواصل مباشرة مع المطورين والتحدث معهم.

٩. ذكرن المجموعة مرّة أخرى أن لا وجود لحلول أو توصيات في مجال الأمن الرقمي قابلة للتطبيق في كل مكان ولجميع الناس- فليست كل الأدوات مناسبة لكل المستخدمين. التعامل بطريقة إستراتيجية مع الأدوات والممارسات الخاصة بالأمن الرقمي مرتبط إلى حدٍ كبير بمعرفتنا لأنفسنا كمستخدمين، وإختيار الأدوات المناسبة لكل واحدة منّا إستنادًا إلى معرفتنا لظروفنا الخاصة.

١٠. وضحن للمجموعة أن عددًا كبيرًا من برمجيات الأمن الرقمي تتضمن تشفيرًا بدرجات متفاوتة – فسّرن للمشاركات أنه في حال كان التشفير خاصية مهمة بالنسبة لهن، يوصى إذًا بإستخدام البرمجيات المفتوحة المصدر. فالبرمجيات المفتوحة المصدر قابلة للتدقيق من قبل المجتمع من أجل ضمان عدم وجود أي أبواب خلفية؛ في حال لا تشمل أداة برمجية ما خاصية التشفير، ولم يكن التشفير عاملاً مهمًا في عملية صنع القرار، قد يكون إستخدام البرمجيات المفتوحة المصدر أقل أهمية (مع أنه أبخس ثمنًا حتمًا).

١١. أكملن هذا الجزء من الجلسة عبر تقسيم المشاركات إلى مجموعات من 3 إلى 4 أشخاص كحدٍ أقصى – وضمن مجموعاتهن الصغيرة، أطلبن منهن وضع لائحة ببعض أدوات الأمن الرقمي التي يعرفنها، والإجابة عن الأسئلة الورادة أعلاه عن كل أداة. أثناء قيامهن بذلك، يتوجب على كل مجموعة مناقشة الإيجابيات والسلبيات التي يجدنها في كل أداة

من الأدوات على لائحتهن – إمنحن المشاركات من 10 إلى 15 دقائق من الوقت لإتمام هذه المرحلة، وعلى كل مجموعة تقديم نتائج عملها عند إنتهاء الوقت.

الجزء الخامس – التدرب على التفكير في الحلول

١٢. قدمن للمشاركات مجموعة من الرسوم البيانية عن حالات مدافعات عن حقوق الإنسان (راجعن الملاحق) وأطلبن منهن البقاء ضمن مجموعاتهن من المرحلة السابقة – إحرصن على توفر حالات كافية لتزويد كل مجموعة بواحدة منها. لا تقدمن مكوّن الحل للمجموعات – خلال هذه المرحلة، يتوجب على المشاركات العمل معًا للتوصل إلى حلولهن الخاصة إستنادًا إلى المعلومات المقدمة لهن خلال هذه الجلسة وما قد يعرفنه مسبقًا عن أدوات الأمن الرقمي.

الجزء السادس – الموارد اللازمة للتمكن من متابعة المستجدات

١٣. لابد للمشاركات في تدريبكن أن تتوفر لديهن إمكانية الوصول إلى المزيد من الموارد بعد إنتهاء التدريب، التي يمكنهن العودة إليها للمحافظة على تدريبهن والتمكن من متابعة المستجدات بشأن الأدوات أو الممارسات الجديدة التي تنتج عن مجتمع الأمن الرقمي.

إليكن بعض الموارد المقترحة التي يمكن تقديمها للمشاركات:

- الهدوء وفن جعل التنكولوجيا تعمل لصالحك // Tactical Technology Collective (تاكتيكل تكنولوجي)[٤]
- موقع "سيكيوريتي إن آي بوكس Security in a Box (فرونتلاين ديفندرز Frontline Defenders وجماعة تاكتيكل تكنولوجي)[٥]
- مشروع "سورفايلنس سلف ديفينس" Surveillance Self-Defense (مؤسسة إلكترونيك فرونتير)[٦]

اختياري: يمكنكن ايضًا وضع لائحة بمنظمات مختلفة تستطيع المشاركات متابعتها (على

[٤] https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual
[٥] https://securityinabox.org
[٦] https://ssd.eff.org/en/module/choosing-your-tools

الإنترنت عموماً وعلى تويتر،.إلخ) للوصول إلى المزيد من المعلومات عن الأمن الرقمي في بلدانهن.

باب ٣

أنا صاحبة القرار

- **الأهداف:** الهدف من هذه الجلسة هو توجيه المشاركات في عملية التفكير النقدي الإستراتيجية لإتخاذ القرارات بشأن أدوات أو ممارسات محددة في مجال الأمن الرقمي سيقمن بتطبيقها لأنفسهن.
- **الطول:** 15 دقيقة
- **الشكل:** تمرين
- **مستوي المهارة:** أساسي
- **المعرفة المطلوبة:**
  - ممارسة التطبيقية بواسطة أدوات وممارسات الأمن الرقمي من التدريب السابق
  - القرارات المرتبطة بالأمن الرقمي (تحديد الحلّ الأفضل)
- **جلسات/تمارين ذات صلة:**
  - وجهات النظر الشخصية حيال الأمن[١]
  - كيف يعمل الإنترنت؟[٢]

[١] https://vrr.im/9339
[٢] https://vrr.im/7ba9

- التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟[٣]
- القرارات المرتبطة بالأمن الرقمي[٤]

• **المواد اللازمة:**
- رسومات عن أدوات السلامة الرقمية (يفضل أن تتوفر نسختين أو ثلاث من كل واحدة منها، ولكن ليس ما يكفي لكل مشاركة من المشاركات)

• **التوصيات:** كمدربات، غالبًا ما نفرض منظورنا الخاص عن ممارسة الأمن الرقمي على المشاركات، إما عن قصد إنطلاقًا من نوايا حسنة، وإما عن غير قصد. ولكن، لابد لنا أن نتذكر – بصفتنا مدربات وخبيرات – أن المشاركات غير مجبرات على إستخدام الأدوات التي نعلمهن عنها، أو التكييف مع الممارسات التي نعتبرها "الأكثر أمانًا".

إدارة التمرين

١. إفتتحن الجلسة بشرح كيف أن بناء ممارسة في مجال الأمن الرقمي عبارة عن عملية متكررة وغالبًا ما تكون صعبة على أي شخصٍ كان. تستند هذه الجلسة على العمل الذي بدأتنه خلال جلسة القرارات المرتبطة بالأمن الرقمي من هذه الوحدة التي بدأت المشاركات خلالها تحديد الأدوات الممارسات الخاصة بهن.

٢. ضعن الرسومات الخاصة بأدوات السلامة الرقمية (ستبحثن أنتن عن الرسوم) على طاولة أو أي سطح مسطح آخر – يجب أن يكون ذلك في وسط غرفة التدريب، أو أي مكان مركزي وظاهر لكل المشاركات

٣. أخبرن المشاركات أنهن على الأرجح سيلاحظن أنهن تعرّفن على عدد من الأدوات المعروضة على الطاولة قبل هذه الجلسة – من قبيل مفاتيح بي جي بي PGP أو تطبيق سيجنال أو أوبسكوراكام أو إيتش تي تي بي إس إيفريوير. ذكرن المجموعة أنه كما سبق أن ذكرتن في مراحل سابقة من التدريب، هنّ من سيتوجب عليهن إختيار الأدوات

[٣] https://vrr.im/47ba
[٤] https://vrr.im/043a

المناسبة لهن ولحاجاتهن وليس أنتن كمدربات أو متخصصات تقنياً أو أي شخص آخر.

٤. أطلبن من المشاركات التقدم نحو الطاولة وإختيار من بين رسومات الأدوات الموجودة هناك، تلك التي يعتبرنها مهمة لهنّ ولحاجاتهن الفردية، وتلك التي سيستمرن في التدرّب على استخدامها والإستمرار في إستخدامها بعد إنتهاء التدريب بأكمله.

٥. بعد أن تختار كل المشاركات أدواتهن، أطلبن من كل واحدة منهن شرح سبب إختيارهن للأدوات التي إخترنها – عليهن الوقوف أو الجلوس في حلقة حول الطاولة، ومن ثمّ، يعرضن واحدة تلو الأخرى خياراتهن وأسبابها إلى أن تقمن جميعاً بذلك. لابد لهن أيضًا من ذكر إن وجدن أي أداة أردن إختيارها ولكن إخترنها الأخريات قبلهن.

٦. والآن، إسألنهن إن كنّ يعتقدن أن بعض الأدوات الأخرى غير متوفرة على الطاولة – حتى إذا كن لا يعرفن اسمها (أو حتى لا يعرفن إن كانت موجودة أم لا) أطلبن منهن التعبير عن أي مخاوف ما زالت تساورهن إذ لا تعالجها كما يجب أي أداة من الأدوات التي توفرت لديهن.

٧. إختتمن الجلسة بالتفكير جماعياً حول كيفية مشاركة المعرفة، وأنه على اللواتي إخترن أداةً أردنها مشاركات أخريات أيضًا (ولكن لم يستطعن لعدم توفر ما يكفي منها) مشاركتها وتبادلها لكي نتمكن جميعاً من "التعلّم" من بعضنا البعض.