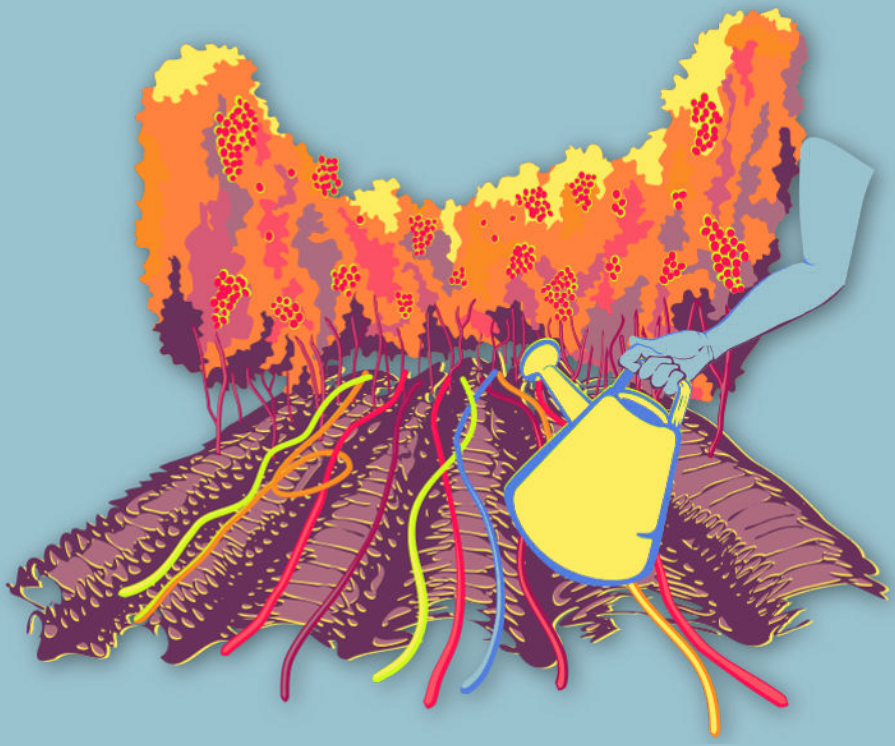
النساء فى فضاء الإنترنت



التخطيط المسبق

التخطيط المسبق

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

باب ١

الخطط والبروتوكولات الأمنية الخاصة بالمنظمة

- **الأهداف:** في هذه الجلسة، ستقمن بتسيير عملية ستنفذها المشاركات لوضع خطة أمنية والبروتوكولات المرتبطة بها التي يمكنهن إستخدامها لتطبيق إجراءات الأمن الرقمي في منظماتهن.
- **الطول:** 90 دقيقة
- **الشكل:** جلسة
- **مستوي المهارة:** متوسط
- **المعرفة المطلوبة:**
  - بمن نثقن؟ (تمارين بناء الثقة)
  - الممارسة التطبيقية بواسطة أدوات وممارسات الأمن الرقمي من التدريب السابق
  - نموذج المخاطر القائمة على النوع الاجتماعي (تحديد الحلّ الأفضل)
- **جلسات/تمارين ذات صلة:**
  - بمن نثقن؟[1]

[1] https://vrr.im/bd0d

- وجهات النظر الشخصية حيال الأمن[٢]
- كيف يعمل الإنترنت؟[٣]
- نموذج المخاطر القائمة على النوع الإجتماعي[٤]
- الخطط والبروتوكولات الأمنية الخاصة بالمنظمة[٥]

• **المواد اللازمة:**
- نموذج المخاطر من تمرين نموذج المخاطر القائمة على النوع الاجتماعي
- نماذج مطبوعة لبروتوكولات أمنية (راجعن مثال النموذج أدناه)

• **التوصيات:** هذه الجلسة مناسبة للمشاركات القادمات من المنظمة أو الجماعة ذاتها، بما أن النشاطات الواردة أدناه تركّز على وضع خطة أمنية على مستوى المنظمة – وعملية تصميم كل هذا سيساعدنا في تعزيز ممارستها وتنفيذها بشكلٍ مستمر من قبل النساء المشاركات. لابد من متابعة عملية تنفيذ الخطة التي وضعتها المشاركات – وإن أمكن ذلك، تواصلن معهن كل أسبوعين أو ثلاث للتحقق من التقدم المحقق (إلى جانب الإجابة على الأسئلة التي قد يطرحنها أثناء هذه العملية). إحرصن على عدم ممارسة الضغط على المشاركات بشأن استخدام أدوات معيّنة أو طريقة تنفيذهن لها أثناء القيام بالمتابعة – إكتفين بكل بساطة بتقديم الدعم لهن والتواجد معهن والإجابة على الأسئلة أو المخاوف التي تساورهن وتقديم التوصيات عند الحاجة لذلك. في حال شعرت المشاركات بضغطٍ يمارس عليهن، قد لا يتشجعن للحصول على مشورتكن بشأن مشكلة ما عالجنها، ولن يرتحن لمشاركة بعض الصعوبات الفعلية عند نشوئها.

---

[٢] https://vrr.im/9339
[٣] https://vrr.im/7ba9
[٤] https://vrr.im/c0c3
[٥] https://vrr.im/f75c

إدارة الجلسة

الجزء الأوّل – عودة إلى نموذج المخاطر

١. إبدأن الجلسة بالتشديد على أهمية بناء نموذج مخاطر قبل وضع مسودة خطة وبروتوكولات. ذكّرن المشاركات أن الأمن الرقمي هو عملية شخصية قبل أي شيء آخر – وفي حال كان هدفهن وضع مسودة خطة أمن رقمي وتنفيذها على مستوى المنظمة، إشرحن لهن أن هذه العملية ستتضمن:

- وضع خارطة بالتهديدات بشكل جماعيٍ – يمكن القيام بذلك خلال جلستين تدريبيتين بوجود الفريق بأكمله، ولكن ذكّرن المجموعة أن التنبّه ومتابعة المستجدات بشأن التهديدات المحدقة بهن عملية مستمرة.
- تعليم الفرق بين العادات المتينة والغير الآمنة في مجال الأمن الرقمي، ومتابعة المستجدات دائمًا بشأن الأدوات الجديدة أو التحديثات المدخلة على الأدوات الموجودة.
- إتخاذ قرارات التنفيذ كفريق، ولكن أيضًا تحديد المجالات التي يمكن فيها للأفراد إنشاء عملياتهن الخاصة وممارستها وفقًا لتقديرهن.
- مراقبة تنفيذ خطة الأمن الرقمي الخاصة بمنظمتهن بشكلٍ دائم، وضمان فهم البروتوكولات المرتبطة بها جيّدًا قبل ممارستها وحلّ المشاكل وأي صعوبات تنشأ بشكل مستمر.

الجزء الثاني – الخطط في مواجهة البروتوكولات

٢. إشرحن للمشاركات الفرق بين خطة أمن رقمي وبروتوكول أمن رقمي. الفكرة الرئيسية الي يجب إيصالها هي أن:

- الخطة إطار عام للتغييرات الرئيسية التي يجب أن تحددها المنظمة أو الجماعة

كعناصر أساسية لرفع مستوى الأمن الرقمي الخاص بها. الخطط هي عملية واضحة المعالم، لها بداية ولها نهاية.

- البروتوكول عبارة عن مجموعة إجراءات أو تدابير مرتبطة بالأمن الرقمي وكل واحدةٍ منها مرتبطة بنشاط أو عملية معيّنة ضمن المنظمة أو الجماعة. البروتوكولات فعليًا عبارة عن ممارسات دائمًا تبقى فاعلة عندما يكتمل تطبيق خطة أمن رقمي معيّنة، وتتطوّر مع الوقت إستجابةً للتغييرات في بيئات المخاطر والتهديدات.

قدمن أمثلة عن الخطط والبروتوكولات للمشاركات – على سبيل المثال، الأنشطة كالسفر أو المشاركة في مظاهرات عامة يخصص لكل نشاط منها بروتوكول أمن رقمي خاص؛ البنود الواردة في خطة أمن رقمي قد تتضمن خضوع الموقع الإلكتروني الخاص بالمنظمة للتدقيق، والتحقق من توفر برنامج مكافحة للفيروسات مثبّت على كل حاسوب، وإدخال إستعمال خاصية جي بي جي GPG لتشفير رسائل البريد الإلكتروني.

الجزء الثالث – وضع خطة وبروتوكولات على مستوى المنظمة

٣. هذه الجلسة مناسبة لمجموعات المشاركات الآتيات من المنظمة أو الجماعة ذاتها، إذ قد يستطعن إغتنام الفرصة للتعاون على وضع خطتهن وبروتوكولاتهن الخاصة بشكلٍ جماعي. ولكن، إن لم يكن الوضع كذلك إلا لجزء من المشاركات، يمكن عندها للواتي لا ينتمين لأي منظمة أو مجموعة العمل على وضع خططهن وبروتوكولاتهن الشخصية.

٤. أطلبن من المشاركات مراجعة نموذج المخاطر من تمرين نموذج المخاطر القائمة على النوع الإجتماعي، بالإضافة إلى ملاحظاتهن من تمرين بمن نثقن؟. أطلبن منهن القيام بوضع مسودة بخطتهن الأمنية – الجدول التالي قد يكون مفيدًا. إشرحن للمشاركات كل قسم من الأقسام (يجب إضافة سطر جديد لكل خطر أو تهديد نحدده):

التهديدات والمخاطر	نقاط الضعف المحددة	نقاط القوة والقدرات	إجراءات التخفيف	الموارد المطلوبة	من هي العناصر المطلوبة
ما هي التهديدات والمخاطر المحدقة بنا حاليًا؟ وما هي تلك التي قد نواجهها في المستقبل؟	ما هي الممارسات أو الظروف التي قد تعرضنا كأفراد وكمنظمات للأذى؟	ما هي نقاط القوة التي نتمتع بها كمنظمة فتعطينا القدرة على التعامل مع التهديدات والمخاطر التي حددناها؟	ما هي الإجراءات المطلوبة للتخفيف من المخاطر التي حددناها؟ ولتكون جاهزاتٍ بشكلٍ أفضل عند مواجهة التهديدات التي حددناها؟	ما هي الموارد (الإقتصادية، البشرية، إلخ.) المطلوبة لتنفيذ هذه الإجراءات؟	ما هي القطاعات أو من هم الأشخاص داخل منظمتنا الواجب إشراكهم في عملية التنفيذ؟ هل سنحتاج لأي تواقيع أو أي أذونات أخرى؟

٥. ذكرن المشاركات أنه على الرغم من التركيز في هذا التدريب على الأمن الرقمي، علينا التذكر دائمًا أن نأخذ الإجراءات الشاملة بعين الإعتبار. أطلبن من المشاركات التفكير في الإجراءات التي يجب إتخاذها من أجل أمنهن الجسدي ورعايتهن الذاتية عند وضع مسودة خططهن وبروتوكولاتهن الأمنية.

٦. بعد ذلك، بعد أن ينتهين من وضع مسودتهن الأولى لجدول الخطة، أطلبن من المشاركات وضع لائحة بأنشطة أو إجراءات منظمتهن التي ستحتاج برأيهن لبروتوكولات خاصة بها.

٧. بعد إن تنتهي المشاركات من وضع مسودة جدول الخطة ولائحة أنشطتهن التي تحتاج لبروتوكولات أمنية، يفضل تخصيص بعض الوقت لكي يتمكن الجميع من مشاركة خططهن. يعدّ ذلك فرصة قيّمة للمشاركات ليتعلمن من مقاربات الأخريات؛ ولكن، لا تنسين أن بعضهن قد لا تشعرن بالإرتياح لمشاركة نقاط ضعف منظمتهن أو شخصهن لعدم وثوقهن بهن. لمعالجة هذه المشكلة بشكلٍ فعّال، قد يتوجب عليكن الطلب من المجموعة مشاركة العناصر الرئيسية فقط من خطتهن (العمود الرابع من الجدول "إجراءات التخفيف") والإحتفاظ بالمعلومات الأخرى أي "التهديدات والمخاطر" و"نقاط الضعف المحددة" لأنفسهن.

الجزء الرابع – ما هي الخطوات التالية؟

٨. ناقشن خطوات المتابعة مع المشاركات – سيحتجن لتنظيم إجتماع خاص ضمن منظمتهن لتشارك المعلومات الأساسية والخلاصات الرئيسية من هذه الجلسة، بالإضافة إلى تمرين نموذج المخاطر القائمة على النوع الإجتماعي وتمرين بمن نثقن؟ - والأهم في هذه الجلسة هي اللائحة بالأنشطة والإجراءات التي تحتاج لبروتوكولات أمنية خاصة بها. يجب مناقشة هذه الخطة والتوافق عليها كفريق، وتحديد فترات زمنية معقولة لتنفيذها – وخلال التفكير ذلك، سيتوجب على المشاركات أيضًا تذكر أن عضوات أخريات في منظمتهن سيحتجن لتدريب على ممارسات و/أو أدوات معيّنة في مجال الأمن الرقمي من أجل أن يصبح التنفيذ الكامل ممكنًا.

باب ٢

خطط وبروتوكولات الأمن الرقمي: إعادة تنفيذها بعد التدريب

- **الأهداف:** في هذه الجلسة، ستستند المشاركات إلى جلسة الخطط والبروتوكولات الأمنية الخاصة بالمنظمة. ستقمن هنا بعرض مجموعة توصيات تساعد المشاركات في تسهيل عملية إعادة تنفيذ الخطط والبروتوكولات بعد التدريب ضمن منظماتهن.
- **الطول:** 40 دقيقة
- **الشكل:** جلسة
- **مستوى المهارة:** متوسط
- **المعرفة المطلوبة:**
  - بمن تثقن؟ (تمارين بناء الثقة)
  - الممارسة التطبيقية بواسطة أدوات وممارسات الأمن الرقمي من التدريب السابق
  - نموذج المخاطر القائمة على النوع الاجتماعي (تحديد الحلّ الأفضل)
  - الخطط والبروتوكولات الأمنية الخاصة بالمنظمة (التخطيط المسبق)
- **جلسات/تمارين ذات صلة:**

- بمن نثقن؟[1]
- وجهات النظر الشخصية حيال الأمن[2]
- كيف يعمل الإنترنت؟[3]
- نموذج المخاطر القائمة على النوع الإجتماعي[4]
- الخطط والبروتوكولات الأمنية الخاصة بالمنظمة[5]

• **المواد اللازمة:**
- شرائح (فيها النقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض

إدارة الجلسة

الجزء الأوّل – وضع خارطة بالهيكليات والعوائق التنظيمية

١. ضمن مجموعات من شخصين، أطلبن من المشاركات وصف منظماتهن:
   • كم عدد الأشخاص المشاركين/ات فيها؟
   • كم مرة يلتقون في الأسبوع/السنة؟

٢. ضمن الثنائيات من الخطوة السابقة، أطلبن من المشاركات الآن تشارك مع بعضهن البعض، بعض العوائق أوالتحديات التي يتوقعن مواجهتها ضمن منظماتهن عند تقديم خططهن الأمنية والتعبير عن الحاجة للبدء بعملية التنفيذ.

---

[1] https://vrr.im/bd0d
[2] https://vrr.im/9339
[3] https://vrr.im/7ba9
[4] https://vrr.im/c0c3
[5] https://vrr.im/f75c

الجزء الثاني – تسيير تنفيذ المنظمة

٣. بعد أن تنتهي المجموعات من مناقشة النقاط المذكورة أعلاه، شاركن بعض الأفكار التي قد تساعد المشاركات في تسيير عملية تنفيذ خططهن وبروتوكولاتهن الأمنية ضمن منظماتهن بعد التدريب:

- أوصينهن بأن يعرضن ذلك كبداية لعملية تفكير – سيتطلب تنفيذ الخطة ووضع البروتوكولات وإختبارها الكثير من الوقت، وستمر المنظمة في مرحلة تكيّف إلى أن يعتاد أفرادها على هذه التغييرات. ومع ذلك، يجب أن يحرصن على التشديد أن التفكير بشكلٍ نقديّ أكثر بشأن الأمن التنظيمي خطوة في الطريق الصحيح.
- حذرن المشاركات أنهن سيتلقين بعض الرفض بسبب مصطلح "بروتوكول" بما أن معناه أصبح تقنيًا ومشحونًا أكثر من اللازم، يجب أن يذكّرن الأخريات في منظمتهن أن البروتوكولات ليست إلا إتفاق بشأن المخاطر والتهديدات المحدقة بهن، والإلتزام بحلّها معًا عبر تحديد إجراءات إستراتيجية لمصلحة المنظمة ومهمتها.
- شددن على أهمية التعاون والإشراك في عملية التنفيذ. يجب أن تعمل المشاركات مع فرق مختلفة ضمن منظماتهن على تقييم مستويات المخاطر في فريقهن، ومن ثمّ مشاركة نتائج هذا التقييم والخطوات اللاحقة مع بقية زميلاتهن. شددن أيضًا على أن يحرصن المشاركات على إفساح المجال للأخريات في منظمتهن من أجل تقديم الملاحظات بشأن الخطط والبروتوكولات الأمنية – بما أن مهام أشخاص مختلفين ستتأثر بطرق مختلفة بهذه التدابير الجديدة، لابد لهن من تفادي إضافة أعباء جديدة على مهام أي شخصٍ كان.
- أطلبن من المشاركات التفكير في طرق أخرى لإشراك فرق مختلفة من المنظمة بشكلٍ جماعي – إحدى تلك المقاربات الممكنة هي أن يقترحن "هيئة أمن رقمي" تشمل ممثلات (لديهن ما يلزم من معرفة لإتخاذ قرارات) عن كل فريق أومجال عمل، مهمتها الإشراف على تنفيذ الخطة الأمنية. ومن ثمّ يمكنهن تنفيذ

هذه العملية بشكلٍ تدريجي، فيركزن أولاً على الموظفات ذوات المستوى الأعلى أوالبدء مع فرق معيّنة ومن ثمّ توسيع رقعة المشاركة. المقاربة الفضلى ستختلف كثيرًا من منظمة لأخرى.

- في الختام – أطلبن من المشاركات مشاركة بعض الأفكار التي لديهن والتي قد تساعد في تسيير عملية التنفيذ في منظماتهن.

الجزء الثالث – طرح المسألة

٤. أطلعن المشاركات على هيكلية أساسية لطرح هذه المسألة المهمة لمناقشتها ضمن منظماتهن – قد يكون ذلك عبارة عن مجموعة أسئلة، أو خطة تدريب ممكنة خاصة بهن تتضمن جلسات وتمارين معينة مرتبطة ببيئة المخاطر التنظيمية.

٥. ذكرن المجموعة أن تتنبه للمتطلبات اللوجستية اللازمة، ولا سيما عامل الوقت – قد لا يتوفر للأخريات في منظمتهن الوقت الكافي لتخصيص فترة ما بعد الظهر كاملةً، أو يوم كامل أو فترة أطول من ذلك حتى للتدريب. وتتطلب عملية تغيير عادات قديمة وقتًا طويلاً والكثير من الصبر، لذا يفضل أن تبحث المشاركات عن طرق لطرح هذه المسائل (أو التدريبات) خلال الإجتماعات الدوريّة الموجودة أو خلال تجمعات أخرى. إليكن هيكلية بسيطة قد تتبعها المشاركات لزيادة مستوى الوعي بشأن مواضيع معيّنة – تبدأ هذه بنقاش حول أهمية الأمن الرقمي بالنسبة للمنظمة، ومن ثمّ يأتي دور الجلسات (من هذا المنهاج) التي تعرض تفاصيل أكثر عن مواضيع الأمن الرقمي – وتعود مسألة إختيار كيفية إجراء هذه النقاشات للمشاركات:

- **نقاش**: ما أهمية الأمن الرقمي بالنسبة لمنظمتنا
- **الجلسة**: [كيف يعمل الإنترنت؟ (أسس الأمن الرقمي،الجولة الأولى)]
- **الجلسة**: [لنبدأ بتوثيق الحالات! (العنف ضد المرأة على الإنترنت)]
- **الجلسة**: [الهواتف المحمولة،الجزء الأوّل (هواتف محمولة أكثر أمانًا)]
- **الجلسة**: [الإتصالات المشفّرة (التشفير)]

• **الجلسة**: [نموذج المخاطر القائمة على النوع الإجتماعي (تحديد الحلّ الأفضل)]

٦. ذكرن المشاركات أن هذه ليست سوى مقاربة مقترحة – لهن الحريّة في تعديل الجلسات والمواضيع وفقًا لما يرينه مناسباً. لابد أن تكنّ متواجدات أثناء قيام المشاركات بعملية التنفيذ في منظماتهن (قدر المستطاع) لتوفير الدعم والإجابة على الأسئلة التي قد تساورهن.