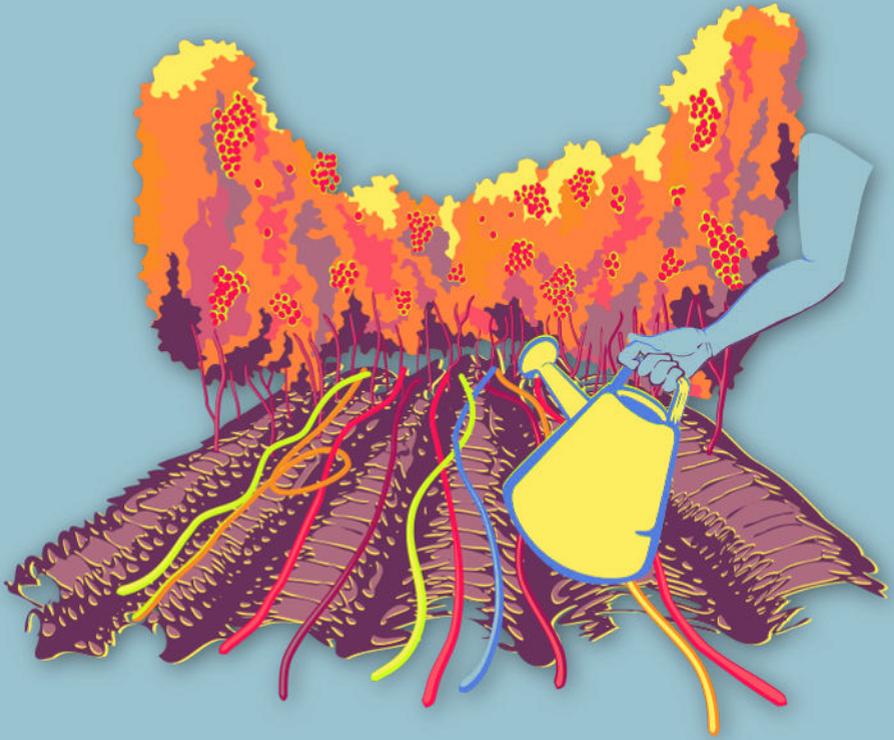




النساء فى فضاء الإنترنت



التخطيط المسبق

الخطة والبروتوكولات الأمنية الخاصة بالمنظمة

**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	الخطط والبروتوكولات الأمنية الخاصة بالمنظمة
٧	إدارة الجلسة
٧	الجزء الأول - عودة إلى نموذج المخاطر
٧	الجزء الثاني - الخطط في مواجهة البروتوكولات
٨	الجزء الثالث - وضع خطة وبروتوكولات على مستوى المنظمة
١٠	الجزء الرابع - ما هي الخطوات التالية؟

باب ١

الخطط والبروتوكولات الأمنية الخاصة بالمنظمة

- الأهداف: في هذه الجلسة، ستقمن بتسيير عملية سنتفذهها المشاركات لوضع خطة أمنية والبروتوكولات المرتبطة بها التي يمكنهن إستخدامها لتطبيق إجراءات الأمن الرقمي في منظماتهن.
- الطول: 90 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)
- جلسات/تمارين ذات صلة:
- بمن تثقن؟^١

<https://vrr.im/bd0d1>

- وجهات النظر الشخصية حيال الأمن^٢
- كيف يعمل الإنترنت^٣؟
- نموذج المخاطر القائمة على النوع الاجتماعي^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 القادמות من المنظمة أو الجماعة ذاتها، بما أن النشاطات الواردة أدناه تركز على وضع خطة أمنية على مستوى المنظمة - وعملية تصميم كل هذا سيساعدنا في تعزيز ممارستها وتنفيذها بشكل مستمر من قبل النساء المشاركات. لا بد 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 معينة أو طريقة تنفيذها 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 عاجلها، ولن يرتحن لمشاركة بعض الصعوبات الفعلية عند نشوئها.

<https://vrr.im/9339٢>

<https://vrr.im/7ba9٣>

<https://vrr.im/c0c3٤>

<https://vrr.im/f75c٥>

إدارة الجلسة

الجزء الأول - عودة إلى نموذج المخاطر

٠١. إبدأن الجلسة بالتشديد على أهمية بناء نموذج مخاطر قبل وضع مسودة خطة وبروتوكولات. ذكرن 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 ستضمن:

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

الجزء الثاني - انخطط في مواجهة البروتوكولات

٠٢. إشرحن للمشاركات الفرق بين خطة أمن رقمي وبروتوكول أمن رقمي. الفكرة الرئيسية التي 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 واحدة منها مرتبطة بنشاط أو عملية معينة ضمن المنظمة أو الجماعة. البروتوكولات فعلياً عبارة عن ممارسات دائماً تبقى فاعلة عندما يكتمل تطبيق خطة أمن رقمي معينة، وتتطور مع الوقت إستجابةً للتغيرات في بيئات المخاطر والتحديات.

قد من أمثلة عن الخطط والبروتوكولات للمشاركات - على سبيل المثال، الأنشطة كالمسرح 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 الفيروسات مثبت 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 للجزء من المشاركات، يمكن عندها للواتي لا ينتمين لأي منظمة أو مجموعة العمل على وضع خطتهن وبروتوكولاتهن الشخصية.

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

من هي العناصر المطلوبة	الموارد المطلوبة	إجراءات التخفيف	نقاط القوة والقدرات	نقاط الضعف المحددة	التهديدات والمخاطر
ما هي القطاعات أو من هم الأشخاص داخل منظمتنا الواجب إشرافهم في عملية التنفيذ؟ هل ستحتاج لأي توقع أو أي أذونات أخرى؟	ما هي الموارد (الإقتصادية، البشرية، إلخ) المطلوبة لتنفيذ هذه الإجراءات؟	ما هي الإجراءات المطلوبة للتخفيف من المخاطر التي حددناها؟ ولتكون جاهزات بشكل أفضل عند مواجهة التهديدات التي حددناها؟	ما هي نقاط القوة التي تتمتع بها منظمة فتحطينا القدرة على التعامل مع التهديدات والمخاطر التي حددناها؟	ما هي الممارسات أو الظروف التي قد تعرضنا كأفراد وكنظمات للأذى؟	ما هي التهديدات والمخاطر المحددة بنا حالياً؟ وما هي تلك التي قد تواجهها في المستقبل؟

٥. ذكرن المشاركات أنه على الرغم من التركيز في هذا التدريب على الأمن الرقمي، علينا التذكر دائماً أن نأخذ الإجراءات الشاملة بعين الاعتبار. أطلبين 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، أطلبين من المشاركات وضع لائحة بأ أنشطة أو إجراءات منظماتهن 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. يعد ذلك فرصة قيمة للمشاركات ليتعلمن من مقاربات الأخريات؛ ولكن، لا تنسين أن بعضهن قد لا تشعرن بالإرتياح لمشاركة نقاط ضعف منظماتهن 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؟

٠٨ ناقش خطوات المتابعة مع المشاركات - سيحتج تنظيم إجتماع خاص ضمن منظمتهن لتشارك المعلومات الأساسية والخلصات 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 أيضاً تذكر أن عضوات أخريات في منظمتهن سيحتجن لتدريب على ممارسات و/أو أدوات معينة في مجال الأمن الرقمي من أجل أن يصبح التنفيذ الكامل ممكناً.