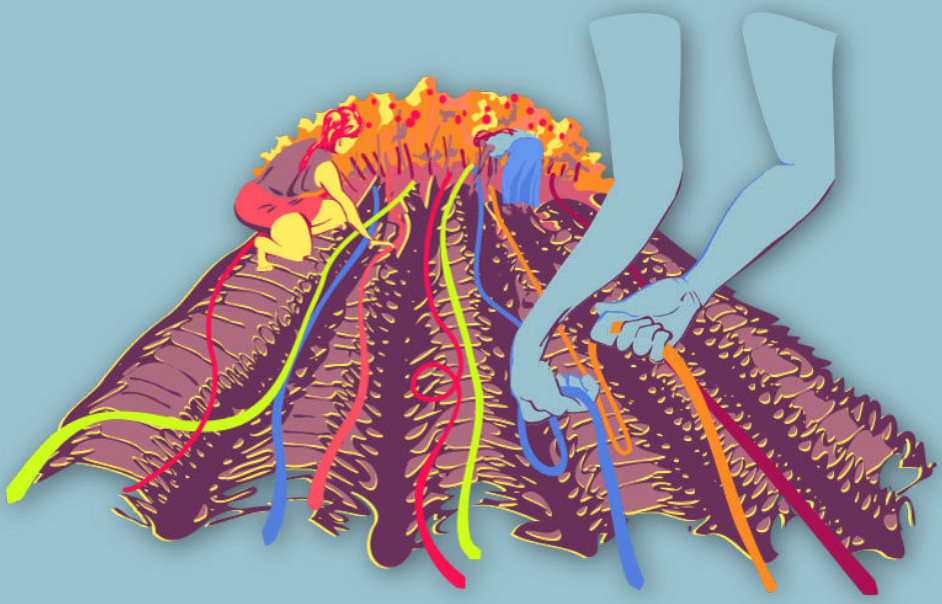

# تحديد الحل الأفضل

# القرارات المرتبطة بالأمن الرقمي

INSTITUTE FOR
WAR & PEACE REPORTING



https://iwpr.net/

# المحتويات

# باب ١

# 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.