النساء فى فضاء الإنترنت

إعادة النظر بعلاقتنا بالتكنولوجيا

وجهات النظر الشخصية حيال الأمن

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

باب ١

وجهات النظر الشخصية حيال الأمن

- **الأهداف:** ستقدمن في هذه الجلسة مفهوم الأمن الشامل للمشاركات، حيث أن كل واحدة منهن تأتي إلى قاعة التدريب بحوافزها وأسباب رفضها وعوائقها وأفكارها المسبقة الشخصية المرتبطة بالأمن الرقمي والجندر والتكنولوجيا. ستشجّع هذه الجلسة المشاركات على تحديد معنى مفهوم "الأمن" بالنسبة لهن كأفراد.
- **الطول:** 90 دقيقة
- **الشكل:** جلسة
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات صلة:**
  - بمن تثقن؟[١]
  - حقوقكن والتكنولوجيا الخاصة بكن[٢]
  - نموذج المخاطر القائمة على النوع الإجتماعي[٣]
- **المواد اللازمة:**

---

١ https://vrr.im/bd0d
٢ https://vrr.im/1151
٣ https://vrr.im/c0c3

- أوراق مسطّرة أو غير مسطّرة بقياس (٤أ) A4 (إعطين أكثر من ورقة واحدة لكل مشاركة)
- شرائح (فيها النقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
- أوراق اللوح ورقيّ

إدارة التمرين

الجزء الأوّل – ما هي السلامة بالنسبة لكن؟ ما هو الأمن بالنسبة لكن؟

١. أطلبن من المشاركات توزيع أنفسهن على مجموعات من 3 إلى 4 مشاركات كحد أقصى، وإعطينهن 15 دقيقة لمناقشة الأسئلة التالية مع بعضهن البعض:

ما هي السلامة بالنسبة لكن؟

ما هو الأمن بالنسبة لكن؟

ما الذي يجعلكن تشعرن بالأمن والأمان؟

في أي مجالات تعتقدن أنه يمكن تطبيق هذين المفهومين؟

في ما يتعلّق بالأسئلة الواردة أعلاه، لا تنسين أنه في بعض اللغات أو اللهجات قد لا توجد كلمات تعادل كلمتي "سلامة" و"أمن" أو أن الناطقين بلغةٍ ما قد يستخدمون كلمة واحدة للدلالة على المفهومين.

٢. بعد ذلك، عرفن المشاركات بواسطة شرائح معروضة أو أوراق اللوح الورقيّ بالمقاربة الشاملة للتدريب. إحرصن على شرح أهمية الأمن الرقمي والرعاية الذاتية والأمن الجسدي بالنسبة للعملية الشاملة (يمكنكن الإستعانة أو نسخ الرسم البياني التالي كطريقة بسيطة لشرح ذلك):

٣. في الكثير من الحالات، يحتمل أن تعملن مع مشاركات يحضرن التدريب من أجل

عناصر الأمان الشامل الثلاث

الأمان الرقمي

الرعاية الذاتية الأمان الشخص

عناصر الأمن الشامل الثلاث

أن يتمكّن من تطبيق إجراءات ضمن منظماتهن؛ بالتالي، من الضرورة بمكان أن تشرحن للمجموعة أن هذا التدريب سيغطي مسألة الأمن على الصعيدين الفردي والجماعي. تتألف المنظمات والجماعات من أفراد – ولمعالجة مسألة الأمن بشكلٍ شامل، علينا أولاً النظر إلى أنفسنا، ومن بعدها، علينا أن ننظر إلى الشبكات والأدوار التي نتولاها ضمن منظمة أوجماعة ما، وفي النهاية علينا أن ننظر إلى المنظمة أو الجماعة بحد ذاتها.

الجزء الثاني – ما هو الأمن الرقمي بالنسبة لكن؟

٤. أطلبن من كل مشاركة التفكير في ما تعني لها مسألة الأمن الرقمي. وأطلبن منهن أن يعملن كل واحدة وحدها على تدوين بعض الجمل يشرحن فيها مفهومهن الشخصي لها. وقبل أن يبدأن بذلك، إشرحن لهن – بحسب الظروف كالتجربة الشخصية أو الأولويات أو القضية/النشاط أو بلد الأصل – أن معنى المفاهيم الخاصة بهن قد تختلف من شخص لآخر (وقد تشمل عناصر أخرى كبعض القيود القانونية، ...إلخ). ولمساعدة كل متدربة على تطوير مفهومها الخاص، يمكنكن البدء بإطلاعهن على مفهومكن الخاص على سبيل المثال.

٥. ما إن ينتهي الوقت المخصص لذلك، إسألن المشاركات ما إذا كنّ راغبات في مشاركة ما كتبنه مع بقية المجموعة – ليس من الضروري أن تشاركن جميعهن ما كتبن, فبعضهن قد لا تشعرن بالضرورة بالراحة إذا قمن بذلك.

٦. من بعد قيام بعض المتطوعات بمشاركة مفاهيمهن، سلطن الضوء على بعض العناصر الأساسية التي قدمنها، كعاداتنا وأجهزتنا والشبكات والمجموعات التي ننتمي لها والبيئة التي نعيش فيها والمعلومات التي نمتلكها ومكان تخزيننا لها. وإشرحن للمشاركات أن الأمن الرقمي مرتبط بنا كأفراد وكبشر قبل أي إعتبار آخر (لا سيما الأدوات والتكنولوجيا).

الجزء الثالث – تحديد الحوافز وأسباب الرفض والحواجز

٧. بعد تقسيم المجموعة إلى مجموعات صغيرة من 3 إلى 4 مشاركات كحد أقصى، أطلبن من المشاركات مناقشة حوافزهن ومخاوفهن والحواجز الموجودة بالنسبة لهن المرتبطة بمسألة الأمن الرقمي عبر الإجابة عن الأسئلة التالية:

ما السبب الذي يدفعهن للتعرّف أكثر على مسألة الأمن الرقمي؟

ما هي الأسباب الشخصية التي دفعتهن لحضور ورشة العمل؟

ما الذي يتوقعن الحصول عليه من هذا التدريب؟

هل لديهن أسباب شخصية تدفعهن إلى رفض الأمن الرقمي؟

ما هي التحديات التي واجهنها في التعلّم عن الأمن الرقمي؟ أوما الذي يشعرن أنه منعهن من تعلّم ذلك من قبل؟

٨. ما أن ينتهي الوقت المخصص لذلك، أطلبن من كل مجموعة مشاركة أفكارها ومناقشاتها مع الأخريات – كمدربات، هذه لحظة مهمة لأنه من أجل مواءمة جلسات تدريبكن بطريقة مرتبطة فعلاً ببيئة مشاركاتكن، لابد لكن أن تتنبهن جيدًا للحوافز وأسباب الرفض والحواجز المحددة التي تتشاركها المشاركات.

الجزء الرابع – المعتقدات الخاطئة المتداولة بشأن الأمن الرقمي والجندر والتكنولوجيا

٩. في ما يتعلّق بهذا الجزء من النقاش، حضرن مسبقًا ما يجب مشاركته من معلومات إضافية حول الأمثلة الواردة أدناه، عن المعتقدات الخاطئة الشائعة المتداولة بشأن الأمن الرقمي والجندر والتكنولوجيا. إلى جانب التفسيرات المستندة إلى خبراتكن الخاصة، إحرصن أيضًا على إيجاد طرق لربط النقاش دائمًا ببعض الحوافز وأسباب الرفض والحواجز التي حددتها المشاركات في القسم السابق:

١. "الأمن الرقمي صعب."

الأمن الرقمي عبارة عن مسيرة. ومع البدء بتعلّم المزيد عنه، ستكتشفن على الأرجح ممارسات غير آمنة كثيرة تعتمدنها: لا تجهدن أنفسكن! لا يتوجب عليكن الإعتقاد أنه سيترتب عليكن تغيير جميع عاداتكن في يوم واحد (أو حتى في تدريب واحد). فمجرد البدء بهذه المسيرة الشخصية الآن، هو خطوة إيجابية وصحيّة!

وكلما تقدمتن أكثر في هذا المجال، ستدركن أكثر فأكثر أن إيجاد إجابة واحدة لمعظم الأسئلة المطروحة في مجال الأمن الرقمي نادر جدًا. ما يجب الإعتراف به هو أنكن تعرفن أنفسكن بشكلٍ أفضل من أي شخص (أو شيء) آخر، وبالتالي، أنتن اللواتي يعرفن فعليًا التغييرات والعادات الجديدة التي يمكنكن إدخالها إلى روتينكن اليومي. يفضل البدء بممارسة تعتبرنها قابلة للتطبيق بشكل منطقي، عوضًا عن رفع سقف التوقعات الذي كثيرًا ما يؤدي إلى اليأس.

٢. "أساس الأمن الرقمي هو تعلّم كيفية استخدام مجموعة من الأدوات الجديدة التي لا أحد من أصدقائكن أو زملائكن يستخدمها".

في الواقع، معظم ممارسات الأمن الرقمي الأساسية والجوهرية لا تعتمد كثيرًا على أدوات الأمن الرقمي. فتغيير كلمات السرّ الخاصة بحساباتكن بشكلٍ دوريّ، والتحقق من إعدادات الخصوصية الخاصة بالحسابات التي تستخدمنها أصلاً, وحماية أجهزتكن بكلمات سرّ والقيام بنسخ احتياطية بشكلٍ دوري لبياناتكم، ممارسات مرتبطة بعاداتكن وسلوككن أكثر مما هي مرتبطة بالتكنولوجيا والأدوات بذاتها.

مسيرة الأمن الرقمي التي سنبدأ بخوض غمارها الآن، هدفها تزويدكن بالمعلومات التي تحتجن إليها لإتخاذ القرارات الصحيحة المناسب بشأن أمنكن الرقمي والتي تركز بشكلٍ أكبر على تعلّم المزيد عن المنصات التي نستخدمها أصلاً، وتداعيات

اختيار أدوات أوممارسات معيّنة على أنفسنا وعلى عملنا، وعلى تحسين الطرق التي نستخدم فيها التكنولوجيا في حياتنا اليومية.

معًا، سنعمل على تحسين هذه الممارسات وفي الوقت عينه سنتعلم المزيد عن المخاطر المحدقة بنا الناتجة عن إتخاذنا لهذه القرارات وإجراءنا لهذه التغييرات. سنتعلم ونتشارك المعلومات مع بعضنا البعض، والتي من شأنها مساعدتنا على إتخاذ قرارات أفضل بشأن الممارسات التي يتوجب علينا تغييرها، وعلى معرفة تلك الممارسات المناسبة التي نستخدمها أصلاً. ولكن الأهم في كل هذا، أن القرار النهائي هو قراركن أنتن!

٣. "أدوات الأمن الرقمي باهظة الثمن." في الواقع، يمكن استخدام معظم أدوات الأمن الرقمي مجانًا. وتجدر الإشارة إلى أن عدد وتنوّع الأدوات المتوفرة هذه يتزايد يومًا بعد يوم، ومشاريع البرمجيات الحرة والمفتوحة المصدر (Free/Libre and Open Source Software "FLOSS") تنتج أدوات مجانية بشكلٍ متزايد يمكن تشغيلها على عددٍ متزايد من أنظمة التشغيل الخاصة بالحواسيب والهواتف المحمولة؛ كذلك هنالك عدد لا بأس به من المنصات الأكثر شعبية تتضمن الآن خصائص أمنية سهلة الاستخدام.

٤. "لا أعرف شيئًا عن الأمن الرقمي!"

قد يفاجئكن ذلك، ولكن معظمنا سبق له أن فكّر في ممارساتنا من دون إدراك ذلك – على سبيل المثال، عدد لا بأس به منكن يستخدم كلمات السرّ لحماية هواتفكن أوحواسيبكن المحمولة أصلاً؛ وقد يستخدم بعضكن تطبيقات أوأدوات مختلفة للتواصل مع الآخرين بشأن مسائل معيّنة؛ وعدد قليلٌ منكن قد تستخدمن أسماء مستعارة أوهوية منفصلة للعمل عن تلك التي تستخدمنها في حياتهن الشخصية.

إختياري: بالنسبة لهذا المعتقد بالذات، من المفيد أن تخصصن بضع دقائق

تطلبن فيها من المشاركات تقديم أمثلة عن ممارسات سبق لهن أن طبقنها ومتعلقة بالأمن الرقمي. أكتبن هذه الممارسات على ورقة من أوراق اللوح الورقيّ لتكون معروضة أمام المجموعة وإعرضنها في مكان واضح للعودة إليها طيلة فترة التدريب.

٥. "لا أستخدم (أو بالكاد أستخدم) الإنترنت، لذا لا أهمية للأمن الرقمي بالنسبة لي."

الأمن الرقمي لا يقتصر فقط على ما تقمن به على الإنترنت – فالممارسات خارج الإنترنت، كالإطلاع بشكلٍ دوري على المعلومات (الأرقام والصور والمستندات والملفات الصوتية وملفات الفيديو... إلخ) التي خُزنت من قبلكن على حاسوبكن وهواتفكن الذكية (و"غير" الذكية) ومفاتيح اليواس بي، بالإضافة إلى الإدراك الجسدي لمكان وجود أجهزتكن أو لمن لديه إمكانية الوصول إليها مهمة بالقدر ذاته – حتى لولم تكن متصلة بالإنترنت. لابد أيضًا من معرفة التطبيقات والبرمجيات المثبتة على أجهزتكن – لأنه أحيانًا، من أجل الوصول إلى معلومات معيّنة على الأجهزة، قد نضطر لتثبيت تطبيقات جديدة أوإ نشاء حسابات جديدة من دون أن ندرك.

٦. "ليس لدي أي شيء أخفيه، وإذا كان لدي أمر أخفيه، فهذا لا يهم لأن الحكومة (أو أي طرف آخر) ستعرف في جميع الأحوال."

كما ورد في الشرح المقدم في مشروع "تاكتيكل تكنولوجي" Tactical Tech-nology "أنا وظلي" [1]:

الخصوصية ليست إختباء – بل هي إستقلالية وقوّة وقدرة على التحكّم؛ هي مرتبطة بقدرتكن على اختيار كيف تقدمن أنفسكن للعالم

قد تظنن أنه ليس لديكن ما تخفينه، ولكن فكرن لبرهة بأنواع المعلومات التي تشاركنها: مع معن تتكلمن أوتتواصلن بشأنها؟ ما هي القنوات التي تستخدمنها للقيام بذلك؟ هل هذه القنوات عامة أو متاحة بطريقة أخرى أمام الجميع للإطلاع عليها؟

بطريقة أو بأخرى، نتخذ قرارات بشأن أنواع المعلومات التي نشاركها ومع من نشاركها كل يوم. عليكن أيضًا الأخذ بعين الإعتبار أنه قد لا يوجد الآن شيء تخفينه، ولكن قد يتغيّر ذلك في المستقبل – لذا قد ترغبن في الإستعداد لهذه الإمكانية!

هل شعرتن يومًا باليأس أو الانكسار لدى سماعكن عن المراقبة الرقمية أو تكتيكات التحرّش الرقمي المستخدمة من قبل الحكومات أو المجموعات الأخرى ضد المدافعات عن حقوق الإنسان؟ طبعًا في سياق نشاطاتكن، من الطبيعي أن تواجهن مثل هذه اللحظات، وليس فقط في سياق الأمن الرقمي أو التهديدات على الإنترنت – لهذا السبب سنبدأ هذه العملية الشاملة. معًا سنبني مقاربة من مستويات متعددة تساعدنا على حماية أنفسنا وحماية معلوماتنا.

الجزء الخامس – الملاحظات الختامية

١٠. إختتمن النقاش من خلال طرح بعض (أو كل) الأفكار والتشجيعات التالية على المجموعة – ونكرر، خذن بعين الإعتبار الحوافز وأسباب الرفض والحواجز التي حددتها المشاركات وإخترن وفقًا لها:

كيف يمكننا تخطي عائق فكرة "أنا لا أتفق كثيرًا مع التكنولوجيا"؟

ليس للأدوات والتكنولوجيا سطوة سحرية خارقة علينا! نحن من يقرر ما يمكنها الوصول إليه، وفي حال طرأ أي حادث، يمكننا دومًا إعادة ضبطها أو تغيير الأدوات التي نستخدمها.

نحن وحدنا فقط نعرف ممارسات الأمن الرقمي المناسبة لنا، ونحن وحدنا الأقدر على إختيار الممارسات الأفضل التي تعتبر مناسبة للتطبيق من الناحية العملية.

إختياري: في حال كان تدريبكن سيدرج ذلك كنتيجة مرغوبٍ بها فأن الوقت الآن مناسب لتشرحن للمشاركات أنهن سيكتبن خططهن الفردية الخاصة بالممارسات

والأدوات التي سيطبقنها خلال تقدمكن معًا في المسيرة التدريبية. يجب أن تتضمن مثل هذه الخطط الأهداف الشخصية التي ستشجعهن على التقدّم بسرعتهن الخاصة.

المراجع

- https://myshadow.org/es/tracking-so-what
- https://ssd.eff.org/en/module/seven-steps-digital-security