النساء فى فضاء الإنترنت

الملحق

الملحق

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

[١] https://codingrights.org

[٢] https://cuidatuinfo.org
[٣] https://derechosdigitales.org
[٤] https://feministinternet.org
[٥] https://gendersec.tacticaltech.org
[٦] https://karisma.org.co
[٧] https://myshadow.org
[٨] https://prism-break.org
[٩] https://r3d.mx
[١٠] https://securityinabox.org
[١١] https://ssd.eff.org
[١٢] https://takebackthetech.net
[١٣] https://temboinalinha.org
[١٤] http://consorciooaxaca.org.mx/proteccion-a-defensoras-de-derechos-humanos
[١٥] http://donestech.net
[١٦] http://sinmiedo.com.co
[١٧] https://vimeo.com/207361788
[١٨] https://cyber-women.com/ar/downloads/quick-tips-gender-sensitive-learning-spaces-digital-security.pdf

[١٩] https://level-up.cc/

باب ١

أداة الأمن الرقمي والقدرة الرقمية الخاصة بمعهد صحافة الحرب والسلام

- **الشكل:** الملحق
- **المواد اللازمة:**
  - نسخ من هذا الاستبيان

مستند داخلي مع علامات

في ما يلي سلسلة من الأسئلة التي ستتيح لمدربكم فهم مستوى ممارسات الأمن الرقمي ضمن منظمتكم ومراقبة أي تقدّم حصل في هذا المجال على حدٍ سواء بفضل التدريب الذي ستتلقونه أو سبق أن تلقيتموه. الغرض من النتائج يقتصر على المراقبة والتقييم وستشارك من دون الكشف عن هوية المشاركين ضمن معهد صحافة الحرب والسلام ومع الممولين الداعمين لهذا المشروع.

البلد .....

1. النظام التشغيلي والبرمجيات التي أستخدمها في عملي والتي تم تحديثها: (الرجاء وضع دائرة

حول الجواب المناسب)

لم تحدث مطلقًا (صفر نقاط)

في الأشهر الستة الماضية (نقطة واحدة)

خلال الأيام الثلاثين الماضية (خمس نقاط)

منذ أكثر من ستة أشهر (صفر نقاط)

لدينا النظام الأحدث مثبتًا على هذا الحاسوب (خمس نقاط)

هي قيد التحديث حاليًا (ثلاث نقاط)

لا أعرف هذه المعلومة (صفر نقاط)

2. هل تقمن بإنشاء نسخ إحتياطية لبياناتكم بواسطة قرص صلب خارجي أو خدمة سحابة إلكترونية: (الرجاء وضع دائرة حول الجواب المناسب)

لم تحدث مطلقًا (صفر نقاط)

منذ أكثر من سنة (نقطة واحدة)

خلال الأشهر الستة الماضية (نقطان)

خلال الأيام الستين الماضية (ثلاث نقاط)

خلال الأيام الثلاثين الماضية (أربع نقاط)

تم إنشاء نسخ إحتياطية للبيانات خلال الأيام الأربعة عشر الماضية (خمس نقاط)

لا أعرف (صفر نقاط)

3. هل قرصكم الصلب أو خدمة السحابة الإلكترونية مشفّرة؟

نعم، كلاهما مشفّر (خمس نقاط)

لا (صفر نقاط)

إحداهما فقط مشفّر (ثلاث نقاط)

لا أعرف (صفر نقاط)

في حال أجبتم بالإيجاب، ما هي أداة التشفير التي تستخدمنها؟ .....

4. الحاسوب الذي استخدمه في عملي مزوّد ببرمجيات أصليّة مرخّصة (على سبيل المثال مايكروسوفت ويندوز، مايكروسوفت أوفيس، أدوبي فوتوشوب، أدوبي إلستراتير، كوريل درو، مكافح فيروسات) أو برامج برمجيات مفتوحة المصدر (أوبن أوفيس، سكريبوس)

كل البرامج مقرصنة (صفر نقاط)

بعض البرامج مقرصنة (نقطة واحدة)

معظم البرامج برامج أصلية مرخّصة (نقطان)

كل البرامج مرخّصة وأصليّة (خمس نقاط)

معظم البرامج برامج مفتوحة المصدر (نقطان)

كل البرامج برامج مفتوحة المصدر (خمس نقاط)

لست متأكدًا/متأكدةً (صفر نقاط)

5. برامج مكافحة الفيروسات محمّلة على الحاسوب والهاتف المحمول المستخدمين من قبلي في عملي وهي محدّثة وتُشغّل في كل مرة يتم تشغيل الجهاز.

نعم، الحاسوب والهاتف المحمول (خمس نقاط)

فقط على حاسوبي (ثلاث نقاط)

فقط على هاتفي المحمول (ثلاث نقاط)

ليس لدي برامج مكافحة للفيروسات (صفر نقاط)

لا أعرف إن كان لديّ برنامج مكافح للفيروسات على جميع أجهزتي (صفر نقاط)

في حال الإيجاب، ما هو برنامج مكافحة الفيروسات الموجود على حاسوبكم؟
.....

في حال الإيجاب، ما هو برنامج مكافحة الفيروسات الموجود على هاتفكم؟
.....

6. وضعت قفلاً على شاشة حاسوب عملي/هاتفي المحمول بواسطة كلمة سرّ لإقفال الشاشة.

نعم (خمس نقاط)

لا (صفر نقاط)

جهاز واحد فقط من هذين الجهازين مزوّد بكلمة سرّ

7. شبكة الإنترنت اللاسلكي الموجودة حيث أعمل مزوّدة بكلمة سرّ مختلفة عن تلك التي زودني بها مقدّم خدمة الإنترنت، وتتماشى كلمة السرّ هذه مع معايير كلمات السرّ القوية (المعايير: 1. تتضمن 25 حرفًا على الأقل، و 2. تتضمن أحرف وأرقام، و 3. تتضمن رموز خاصة، و 4. تتضمن أحرف صغيرة وأحرف كبيرة).

نعم – تغيّرت كلمة السرّ وتتماشى مع معيارين على الأقل من معايير كلمات السرّ (خمس نقاط)

لا – لم تتغير كلمة السرّ التي حددها مقدم خدمة الإنترنت (صفر نقاط)

جزئيًا – لم يطبق إلا معيار واحد من المعايير الخاصة بكلمات السرّ المذكورة أعلاه (ثلاث نقاط)

جزئيًا – تغيّرت كلمة السرّ ولكن لم يطبّق أي معيار من معايير كلمات السرّ القوية (نقطة واحدة)

8. عن إستخدام شبكات الإنترنت اللاسلكي العامة في الفنادق أو المطارات أو المقاهي

لم أستخدم يومًا شبكات الإنترنت اللاسلكي في الفنادق أو المطارات أو المقاهي إلا إذا كنت متصلاً بخدمة شبكة افتراضية خاصة. (خمس نقاط)

استخدم أحيانًا شبكات الإنترنت اللاسلكي في الفنادق أو المطارات أو المقاهي ولكن

من دون الاتصال بها عبر خدمة شبكة افتراضية خاصة. (نقطان)

استخدم دائمًا شبكات الإنترنت اللاسلكي في الفنادق أو المطارات أو المقاهي من دون استخدام خدمة شبكة افتراضية خاصة. (صفر نقاط)

9. في ما يخص إنشاء نسخ إحتياطية لمستندات عملي، استخدم أدوات تشفير لحفظ المستندات على حاسوبي المحمول

نعم (خمس نقاط)

لا (صفر نقاط)

لبعض المستندات فقط (ثلاث نقاط)

في حال أجبتم بالإيجاب، ما هي أداة التشفير التي تستخدمونها؟ .....

10. في ما يتعلّق بالنصوص المتبادلة عبر البريد الإلكتروني أو الرسائل النصية القصيرة بين أعضاء منتظمتكم.

استخدم دائمًا التشفير للبريد الإلكتروني أو الرسائل النصية القصيرة أو المحادثات لنقل بيانات حساسة (خمس نقاط)

غالبًا ما استخدم التشفير للبريد الإلكتروني أو الرسائل النصية القصيرة أو المحادثات لنقل بيانات حساسة (ثلاث نقاط)

نادرًا ما استخدم التشفير للبريد الإلكتروني أو الرسائل النصية القصيرة أو المحادثات لنقل بيانات حساسة (نقطان)

لا استخدم أبدًا التشفير للبريد الإلكتروني أو الرسائل النصية القصيرة أو المحادثات لنقل بيانات حساسة (صفر نقاط)

11. أشارك كلمات سرّي مع (الرجاء وضع دائرة على كل الإجابات المناسبة):

شريكي/شريكتي في الحياة (صفر نقاط)

أخوتي وأخواتي و/أو أهلي (صفر نقاط)

صديقي/صديقتي المفضل/ة (صفر نقاط)

زملائي في العمل (صفر نقاط)

لا أحد (خمس نقاط)

12. كلمات السرّ الآمنة تتكوّن من 25 رمزًا على الأقلّ (أحرف، أرقام، رموز خاصة، أحرف كبيرة وصغيرة). لا تستخدموا كلمات من القاموس أو تواريخ ولادة أو أي معلومات شخصية. كل كلمات السرّ الخاصة بي تتماشى مع هذه المعايير المذكورة أعلاه لضمان قوّة كلمات السرّ.

نعم (خمس نقاط)

لا (صفر نقاط)

واحد منها فقط (ثلاث نقاط)

13. لدي كلمات سرّ مختلفة لكل جهاز وحساب من أجهزتي وحساباتي (الحاسوب، الهاتف، البريد الإلكتروني، مواقع التواصل الإجتماعي، الحساب المصرفي، ألخ)

نعم (خمس نقاط)

لا (صفر نقاط)

استخدم بعض كلمات السرّ المختلفة ولكن تتكرّر أحيانًا (نقطة واحدة)

بعض كلمات سرّي محددة بشكلٍ تلقائي من قبل منظمتي/مكتبي/ مقدم الخدمة لي (ثلاث نقاط)

14. اتخذت قرارات إستراتيجية بشأن كيفية إدارة هوياتي على مواقع التواصل الإجتماعي لحسابتي الشخصية والحسابات الخاصة بعملي/نشاطي استنادًا إلى مستوى الخطر المحدق بي. (على سبيل المثال، استخدام هويات وحسابات مختلفة/مزيّفة للنشاط/العمل، أو إستخدام اسمي وصورتي وهويتي الحقيقية في حال لا أشعر أنني مهدد...)؟

نعم – فكرت بالموضوع وأشعر أنني بأمان وفقًا لإدارتي الحالية لهوياتي على الإنترنت (خمس نقاط)

لا – لم أفكر بالموضوع (صفر نقاط)

جزئيًا – أعتبر أنه من المنطقي إنشاء هويات مختلفة أو غير مكشوفة على الإنترنت ولكنني لم أجري أي تغيير بعد (نقطان)

جزئيًا – فكرت في هوياتي على الإنترنت وأجريت التغييرات، ولكنني لست متأكدًا بعد من أن الترتيب هذا آمن (أربع نقاط)

نظرًا لوضعي، من المنطقي بالنسبة لي إستخدام اسمي الفعلي وهويتي الحقيقية في كل حساباتي على مواقع التواصل الاجتماعي (خمس نقاط)

15. أخزّن كلمات سرّي على سلسلة مفاتيح رقمية آمنة محمية بكلمة سرّي

نعم (خمس نقاط) لا (صفر نقاط) بعض الحسابات فقط (ثلاث نقاط) لا أعرف ماهية هذه الأداة (صفر نقاط)

أي تخزن سلسلة المفاتيح وبأي شكل؟ .....

16. أثناء تصفحكم، هل تستخدمون المواقع المزوّدة ببروتوكول نقل النص التشعبي الآمن (HTTPS)؟

نعم (خمس نقاط) لا (صفر نقاط) ما هذا؟ (صفر نقاط)

أتحقق من ذلك دائمًا ولكن ليس من الممكن تصفّح الإنترنت بواسطة بروتوكول نقل النص التشعبي الآمن (ثلاث نقاط)

17. في ما يخص حساباتكم الشخصية على مواقع التواصل الإجتماعي.

كل منشوراتي ظاهرة للعموم على مواقع التواصل الإجتماعي (صفر نقاط) لا أعرف من قادر على الاطلاع على منشوراتي على مواقع التواصل الاجتماعي (صفر نقاط)

اختار إعدادات خاصة لكل منشور (أربع نقاط)

أعدّل الإعدادات للتحكّم بإمكانية إطلاع كل شخص على كل معلومة متاحة على حساباتي على مواقع التواصل الإجتماعي (خمس نقاط)

لا أعرف كيف أضبط إعدادات الإدارة على أي من حساباتي على مواقع التواصل الإجتماعي (صفر نقاط)

18. أنقر على الروابط أو أفتح الملفات المرفقة في رسائل البريد الإلكتروني عندما: (الرجاء وضع دائرة على الإجابات المناسبة)

يبدو أنها تحتوي على معلومات هامة أو طارئة (صفر نقاط)

أعرف المرسل، ولكن حين تكون الرسالة غير متوقعة (مثال: الشركاء العاطفيين، الأصدقاء القدامى) (نقطة واحدة)

ترد من الشبكة التي أثق بها (نقطان)

أتوقع وصولها (ثلاث نقاط)

أعرف المرسل ويكون المرسل متحققًا منه (خمس نقاط)

19. استخدم مواقع التحادث الآمنة وأدوات التواصل الصوتي الآمنة (VOIP) لإجراء اتصالاتي.

نعم (خمس نقاط)

لا (صفر نقاط)

أحيانًا (نقطان)

لا أعرف ما هذا (صفر نقاط)

ما هي الأدوات الآمنة التي تستخدمونها؟ .....

20. استخدم أجهزة منظّمة للطاقة لحماية أجهزتي الإلكترونية المهمة من ارتفاع منسوب الطاقة:

نعم (خمس نقاط)

لا (صفر نقاط)

فقط في مكتبي (نقطان)

فقط في منزلي (نقطان)

فقط لبعض الأجهزة (نقطان)

اجمعوا النقاط وسجلوها على لائحة العلامات الخاصة بالمنظمة.....نقاط100/ نقطة

باب ٢

نماذج لجداول أعمال التدريبات

- **الشكل:** الملحق

على الرغم من أننا ندرك أن المحتوى النهائي لأي جلسة تدريب سيستند إلى التشخيص الذي تجريه كل مدربة مع كل مجموعة، إلا أننا سنقدم لكن بعض النماذج عن جداول أعمال التدريبات إدناه.

نماذج جداول الأعمال المعروضة أدناه منظمة وفقًا لمدة التدريب (عدد الأيام)، ومن ثمّ وفقًا لمستوى مهارات المشاركات. هناك بعض معايير التخطيط الأخرى ستؤثر حتمًا على التصميم النهائي لتدريبكن، ولكن الوقت المتاح هوالعنصر الأهم عادةً:

- سيحدد الوقت المتاح لكنّ في النهاية كمّ المحتوى الذي ستتمكنّ من تغطيته في ورشة عمل واحدة؛ وهذا سيحدده أيضًا مستوى المهارات الجماعي للمشاركات.
- أغلب الظن، ستعرفن عدد الساعات أوالأيام المتاحة للعمل مع مجموعة قبل معرفة العوامل الأخرى كمكان التدريب أوعدد المشاركات أومستوى المهارات الجماعي.

نماذج لجداول أعمال لورشات عمل تتراوح مدتها بين يوم واحد ويوم واحد ونصف اليوم

ورشة عمل من يوم واحد ونصف اليوم حول تقييم المخاطر

المدة الزمنية التقريبية اللازمة: 10 ساعات

جدول أعمال هذا التدريب مخطط له وفقًا لسيناريويشتمل على ورشة عمل تعرّف بالأمن الرقمي، تمتد ليوم واحد ونصف اليوم مع مجموعة من المدافعات عن حقوق الإنسان أوجماعة نسائية، وتركز بشكلٍ أساسي على تقييم المخاطر بشكلٍ عام. ويفضّل أن تكون النساء المشاركات في ورشة العمل هذه قد أصبحن بنهايتها قادرات على تحديد المخاطر المحدقة بهن، وقادرات على التعبير بشكلٍ أوضح عن حاجات الأمن الرقمي الخاصة بهن.

جدول الأعمال هذا يشتمل على جلسات حول أسس الأمن الرقمي وممارسات الرعاية الذاتية وتقنيات توثيق حالات الإستغلال أوالتهديدات والتعامل معها. في هذا السيناريو، يجب وضع إستراتيجية متابعة من قبل المدربة من أجل التعامل مع نتائج عمليات تقييم المخاطر التي أجرتها المشاركات.

١. التمرين: قواعد اللعبة (تمارين بناء الثقة)
٢. التمرين: بينغو المدافعات (تمارين بناء الثقة)
٣. الجلسة: وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)
٤. التمرين: بمن نثقن؟ (تمارين بناء الثقة)
٥. الجلسة: حقوقكن والتكنولوجيا الخاصة بكنّ (إعادة النظر بعلاقتنا بالتكنولوجيا)
٦. التمرين: نموذج المخاطر القائمة على الجندر (تحديد الحلّ الأفضل)
٧. التمرين: بناء الرعاية الذاتية النسوية (الرعاية الذاتية)
٨. الجلسة: بناء كلمات سرّ قوية (أسس الأمن الرقمي،الجولة الأولى)
٩. الجلسة: كيفية حماية حاسوبكن (أسس الأمن الرقمي،الجولة الأولى)
١٠. الجلسة: التصفح الآمن (أسس الأمن الرقمي،الجولة الأولى)

١١. الجلسة: الخصوصية (الخصوصية)
١٢. الجلسة: الهواتف المحمولة،الجزء الأوّل (هواتف محمولة أكثر أمانًا)
١٣. الجلسة: لنبدأ بتوثيق الحالات! (العنف ضد المرأة على الإنترنت)
١٤. التمرين: أزهار النسويات (تمارين الختام والمراجعة)

تدريب توعوي ليوم واحد للمدافعات عن حقوق الإنسان اللواتي يتعاملن مع التحرش على الإنترنت

المدة الزمنية التقريبية اللازمة: 5 ساعات

جدول أعمال هذا التدريب مخطط له وفقًا لسيناريويشتمل على ورشة عمل تعرّف بالأمن الرقمي تمتد ليوم واحد مع مدافعات عن حقوق الإنسان بدأن لتوهن بالتعامل مع حوادث تحرّش على الإنترنت. ويفضّل أن تكون النساء المشاركات في ورشة العمل هذه قد أصبحن بنهايتها قادرات على التعبير بشكلٍ أوضح عن حاجات الأمن الرقمي الخاصة بهن، وقادرات بسرعة أكبر على تحديد إشارات أوأنماط الخطر الدالة على حالات العنف القائم على النوعي الاجتماعي (الجندر) على الإنترنت .

يتضمن جدول الأعمال هذا جلسات خاصة للتعريف بالأمن والسلامة على المستوى الشخصي، وبممارسات الأمن الرقمي الأساسية وبالتعرّف على أنماط الإستغلال والتحرّش

١. التمرين: قواعد اللعبة (تمارين بناء الثقة)
٢. التمرين: الحلوى المخادعة (تمارين بناء الثقة)
٣. الجلسة: وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)
٤. الجلسة: بناء كلمات سرّ قوية (أسس الأمن الرقمي،الجولة الأولى)
٥. التمرين: العنف الرمزيّ (العنف ضد المرأة على الإنترنت)
٦. التمرين: حان وقت المراقبة! (التحادث الجنسي)
٧. الجلسة: التحادث الجنسي (التحادث الجنسي)
٨. التمرين: التفكير في الرعاية الذاتية (استنتاجاتنا) (الرعاية الذاتية)

تدريب على تقييم المخاطر ليوم واحد للمدافعات عن حقوق الإنسان اللواتي يتعاملن مع التحرّش على الإنترنت

المدة الزمنية التقريبية اللازمة: 7 ساعات

جدول أعمال هذا التدريب مخطط له وفقًا لسيناريويشتمل على ورشة عمل تعرّف بالأمن الرقمي تمتد ليوم واحد، مع مدافعات عن حقوق الإنسان يتعاملن مع حوادث التحرّش على الإنترنت المستمرة، واللواتي يحتجن للدعم في وضع خطط أمنية وإستراتيجيات للتعامل معها. يفضّل أن تكون النساء المشاركات في ورشة العمل هذه قد أصبحن بنهايتها قادرات على التعبير بشكلٍ أوضح عن حاجات الأمن الرقمي الخاصة بهن، وعلى التمتع بقدرة أكبر للسيطرة على بيئة المخاطر الشخصية من حولهن، وقادرات على وضع خطة أمنية خاصة ببيئتهن للتعامل مع هذه الحالات وبروتوكول أمني خاص بهن.

يتضمن جدول الأعمال هذا جلسات خاصة للتعريف بالأمن والسلامة على المستوى الشخصي وبممارسات الأمن الرقمي الأساسية وبعمليات تقييم المخاطر القائمة على النوع الاجتماعي (الجندر).

١. التمرين: قواعد اللعبة (تمارين بناء الثقة)
٢. الجلسة: وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)
٣. التمرين: بمن نثقن؟ (تمارين بناء الثقة)
٤. التمرين: نموذج المخاطر القائمة على الجندر (تحديد الحلّ الأفضل)
٥. الجلسة: الخصوصية (الخصوصية)
٦. التمرين: الاستقصاء عن المعلومات الشخصية الخاصة بالمتصيد (العنف ضد المرأة على الإنترنت)
٧. التمرين: بناء الرعاية الذاتية النسوية (الرعاية الذاتية)

أمثلة عن جدوال أعمال لورش عمل ممتدة على ثلاثة أيام

تدريب تمهيدي ممتد على ثلاثة أيام

المدة الزمنية التقريبية اللازمة: 15 ساعة

صمم جدول أعمال هذا التدريب ليتناسب مع ورشة عمل تمتد على ثلاثة أيام مخصصة لمدافعات مبتدئات عن حقوق الإنسان، لم يتعرفن بعد (أويعرفن القليل) على الممارسات الأمنية الرقمية. بما أنه يشمل تعريفًا بأسس الأمن الرقمي وممارسات تقييم المخاطر، مع التركيز بشكلٍ واضح أيضًا على إستراتيجيات الرعاية الذاتية في الوقت عينه، يعتبر جدول أعمال هذا التدريب مناسبًا إما لورشة عمل خاصة بمنظمة أولورشة عمل لمجموعة مختلطة من المدافعات عن حقوق الإنسان من مجموعات أودول مختلفة يعملن في المنطقة ذاتها.

بالإضافة إلى ذلك، سيحضّر جدول الأعمال هذا المجموعة للخضوع لتدريب متابعة متوسط المستوى (راجع تدريب متوسط المستوى ممتد على ثلاثة أيام الوارد أدناه)؛ إلا أنه من الممكن استخدامه أيضًا لورشة عمل مستقلة.

١. التمرين: قواعد اللعبة (تمارين بناء الثقة)
٢. التمرين: بينغو المدافعات (تمارين بناء الثقة)
٣. الجلسة: وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)
٤. التمرين: بمن نثقن؟ (تمارين بناء الثقة)
٥. الجلسة: حقوقكن والتكنولوجيا الخاصة بكنّ (إعادة النظر بعلاقتنا بالتكنولوجيا)
٦. الجلسة: كيف يعمل الإنترنت؟ (أسس الأمن الرقمي،الجولة الأولى)
٧. التمرين: أزهار النسويات (تمارين الختام والمراجعة)
٨. التمرين: نموذج المخاطر القائمة على الجندر (تحديد الحلّ الأفضل)
٩. التمرين: فعل الرفض (الرعاية الذاتية)
١٠. الجلسة: بناء كلمات سرّ قوية (أسس الأمن الرقمي،الجولة الأولى)
١١. الجلسة: التصفح الآمن (أسس الأمن الرقمي،الجولة الأولى)

١٢. الجلسة: البرمجيات الخبيثة والفيروسات (أسس الأمن الرقمي،الجولة الأولى)
١٣. التمرين: بناء الرعاية الذاتية النسوية (الرعاية الذاتية)
١٤. الجلسة: كيفية حماية حاسوبكن (أسس الأمن الرقمي،الجولة الأولى)
١٥. الجلسة: ماذا يمكن لبياناتكن الوصفية أن تفصح عنكن؟ (المناصرة الآمنة على الإنترنت)
١٦. التمرين: ماركو بولو (هواتف محمولة أكثر أمانًا)
١٧. الجلسة: الهواتف المحمولة،الجزء الأوّل (هواتف محمولة أكثر أمانًا)
١٨. الجلسة: الجمهور الشبكي (الخصوصية)
١٩. الجلسة: الخصوصية (الخصوصية)
٢٠. الجلسة: لنبدأ بتوثيق الحالات! (العنف ضد المرأة على الإنترنت)

تدريب متوسط المستوى ممتد على ثلاثة أيام

المدة الزمنية التقريبية اللازمة: 15 ساعة

صمم جدول أعمال هذا التدريب ليتناسب مع ورشة عمل تمتد على ثلاثة أيام مخصصة للمدافعات اللواتي سبق لهن أن خضعن لتدريب تمهيدي (راجعي تدريب متوسط المستوى ممتد على ثلاثة أيام الوارد أعلاه) ويفترض أن يقدّم كتدريب متابعة. فمستواه التقني أعلى بشكلٍ ملحوظ من جدول أعمال التدريب التمهيدي، ويركّز على التطبيقات العملية لمفاهيم الأمن الرقمي، بالإضافة إلى مهارات التفكير النقدي من أجل إتخاذ قرارات مستندة إلى معرفة بشأن استخدام الأدوات. كما يعالج مواضيع معينة بشكلٍ معمقٍ أكثر كعلاقة النساء بالتكنولوجيا والخصوصية والتشفير والمحافظة على سريّة الهوية.

في حال كنتن تعملن مع مشاركات من المنظمة ذاتها، سيقدّم هذا التدريب لهن أيضًا مقاربات إستراتيجية للبدء بمشاركة معرفتهن مع الأخريات في منظمتهن، بما في ذلك تصميم الخطط والبروتوكولات الأمنية الخاصة بالمنظمة.

١. التمرين: الحلوى المخادعة (تمارين بناء الثقة)
٢. التمرين: أنا صاحبة القرار (تحديد الحلّ الأفضل)

٠٣. الجلسة: قصتها مع التكنولوجيا (إعادة النظر بعلاقتنا بالتكنولوجيا)
٠٤. التمرين: إطرحي عليّ ما تريدينه من أسئلة! (الخصوصية)
٠٥. الجلسة: التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟ (الخصوصية)
٠٦. الجلسة: الحملات الآمنة على الإنترنت (المناصرة الآمنة على الإنترنت)
٠٧. الجلسة: الهواتف المحمولة،الجزء الثاني (أسس الأمن الرقمي،الجولة الأولى)
٠٨. الجلسة: تعريف بمسألة التشفير (التشفير)
٠٩. الجلسة: التواصل المشفّر (التشفير)
١٠. التمرين: القدْر المغلي (المرجل) (تمارين الختام والمراجعة)
١١. الجلسة: التخزين والتشفير (أسس الأمن الرقمي،الجولة الثانية)
١٢. التمرين: الصديقة السريّة (المحافظة على سريّة الهوية)
١٣. الجلسة: المحافظة على سريّة الهوية (المحافظة على سريّة الهوية)
١٤. الجلسة: القرارات الخاصة بالأمن الرقمي (تحديد الحلّ الأفضل)
١٥. الجلسة: الخطط والبروتوكولات الأمنية الخاصة بالمنظمة (التخطيط المسبق)
١٦. التمرين: رسالة حب إلى نفسي (الرعاية الذاتية)

تدريب متقدم ممتد على ثلاثة أيام

المدة الزمنية التقريبية اللازمة: 12 ساعة

صمم جدول أعمال هذا التدريب ليتناسب مع ورشة عمل تمتد على ثلاثة أيام، مخصصة للمدافعات اللواتي سبق لهن أن خضعن للتدريب التمهيدي والتدريب المتوسط المستوى (راجعي الأمثلة السابقة) وبتن جاهزات لتجربة متقدمة أكثر.

تركز ورشة العمل هذه، التي تعتبر تكتيكية أكثر بطبيعتها مقارنة بالتدريبات السابقة، بدرجة أقّل على رفع مستوى المعرفة النظرية إلى مستوى وضع ممارسات خاصة بأدوات معيّنة. وتركز أكثر على تطبيق مهارات التفكير النقدي وصنع القرارات وفقًا لسيناريوهات تستند إلى الواقع (سيمكنكن ذلك كمدربات من إجراء عمليات تقييم أشمل لمدى التقّدم الإجمالي للمجموعة).

١. التمرين: الفوازير! (تمارين الختام والمراجعة)
٢. الجلسة: المواقع الإلكترونية الأكثر أمانًا (المناصرة الآمنة على الإنترنت)
٣. التمرين: المزيد من الهويات الإلكترونية! (المحافظة على سريّة الهوية)
٤. الجلسة: لنعد إلى خانة الصفر! (أسس الأمن الرقمي،الجولة الثانية)
٥. التمرين: الاستقصاء عن المعلومات الشخصية الخاصة بالمتصيد (العنف ضد المرأة على الإنترنت)
٦. الجلسة: الخطط والبروتوكلات الخاصة بالأمن الرقمي: عملية إعادة التطبيق بعد التدريب (التخطيط المسبق)
٧. التمرين: لمسة محبة (الرعاية الذاتية)
٨. التمرين: خلاصة الأمن الرقمي (تمارين الختام والمراجعة)

باب ٣

موارد إضافية

منظمة "حقوق البرمجة"[١]

تقود نساء برازيليات منظمة تجري بحوثًا وتنفّذ مشاريع تهدف إلى تعزيز تطبيق حقوق الإنسان في العالم الرقمي عبر إدخال استخدامات ومفاهيم التكنولوجيا ضمن عمليات صنع السياسات.

منظمة "انتبهوا لمعلوماتكم"[٢]

أمن المعلومات والاتصالات

[١] https://codingrights.org
[٢] https://cuidatuinfo.org

منظمة الحقوق الرقمية[٣]

منظمة مستقلة لا تبغى الربح من أميركا الجنوبية تأسست سنة 2005 وأهدافها الأساسية هي التنمية والدفاع عن حقوق الإنسان والترويج لها في البيئة الرقمية في المنطقة.

منظمة الإنترنت النسوي[٤]

تعمل من أجل تمكين المرأة وأعضاء مجتمع الميم بشكلٍ أكبر – في وجه كل المصاعب – من أجل أن يتمكنوا من التمتع بحقوقهم/ن والتمكن من التمتع واللعب ولتفكيك النظام الأبوي.

موقع ويكي أمن النوع الإجتماعي من منظمة "تاكتيكل تيك"[٥]

هذا الدليل هو مورد وضعه أعضاء مجتمعنا الذي يزداد عدداً والذي يضم ناشطات ومدافعات عن حقوق الإنسان ومختصات بالتكنولوجيا من النساء والعابرين/ات جنسياً.

مؤسسة كاريزما[٦]

هي منظمة من منظمات المجتمع المدني متخصصة في الترويج للإستخدام السليم للتكنولوجيات في البيئات الرقمية وتقديم الدعم لهذا الإستخدام.

---

[٣] https://derechosdigitales.org
[٤] https://feministinternet.org
[٥] https://gendersec.tacticaltech.org
[٦] https://karisma.org.co

مشروع "أنا وظلي"[٧]

يساعدكم مشروع "أنا وظلي" من منظمة "تاكتيكل تيك" في التحكم في آثار بياناتكم، ومعرفة ما إذا كنتم تتعرّضون للتعقّب وتعلّم المزيد عن قطاع البيانات.

"إنسحب من برنامج بريزم"[٨]

الإنسحاب من برامج التجسس على البيانات العالمية مثل برنامج بريزم PRISM وبرنامج "إكس كي سكور" XKeyscore و"تيمبورا" Tempora.

منظمة "شبكة الدفاع عن الحقوق الرقمية"[٩]

هي منظمة مكسيكية معنية بالدفاع عن حقوق الإنسان في العالم الرقمي.

"سيكيوريتي إن آي بوكس"[١٠]

في حال تعرفتن حديثًا على عالم الأمن الرقمي، يمكنكن الإطلاع على دلائل التكاتيكات التي تتناول المبادئ الأساسية، بما في ذلك النصائح حول كيفية إستخدام منصات التواصل الإجتماعي والهواتف المحمولة بشكلٍ أكثر أمانًا.

---

٧ https://myshadow.org
٨ https://prism-break.org
٩ https://r3d.mx
١٠ https://securityinabox.org

مشروع حماية الذات من المراقبة[١١]

نصائح وأدوات وإرشادات خاصة بإجراء إتصالات أكثر أمانًا على الإنترنت.

مشروع "لنسترجع التكنولوجيا"[١٢]

هذا المشروع نداء للجميع، ولا سيما النساء والفتيات، لإسترجاع القدرة على التحكّم بالتكنولوجيا لوضع حدٍ للعنف ضد المرأة.

هل تخضعون للمراقبة على الإنترنت؟[١٣]

دليل عملي حول كيفية مكافحة الرقابة على الإنترنت.

حماية المدافعات عن حقوق الإنسان[١٤]

هو مشروع لتعزيز حماية المدافعات عن حقوق الإنسان وأمنهن ورعايتهن الذاتية.

---

١١ https://ssd.eff.org
١٢ https://takebackthetech.net
١٣ https://temboinalinha.org
١٤ http://consorciooaxaca.org.mx/proteccion-a-defensoras-de-derechos-humanos

"دونس تيك"[١٥]

عملية تحقيق ناتجة عن الرغبة في توضيح بعض المسائل من أجل تحويل البحوث إلى مصدر من المعرفة المفيدة للأشخاص المهتمين بعدم المساواة بين الأنواع الإجتماعية وأيضًا للأشخاص المهتمين بالتحولات الإجتماعية والسياسية.

"بلا خوف"[١٦]

إلى الشارع من دون خوف، أدوات ضد القمع.

العنف على الإنترنت هو عنف أيضًا (فيديو)[١٧]

العنف على الإنترنت هو عنف أيضًا.

نصائح سريعة بشأن المساحات[١٨]

نصائح سريعة بشأن تسيير مساحات التعلّم حول الأمن الرقمي تراعي الحساسيات الجندرية. دليل وضعه معهد صحافة الحرب والسلام ومنظمة "سوشل تيك" Tic، Social يتضمن مواد قدمتها إنديرا كورنيليو Indira Cornelio، دانيالا فالك Dhaniella Falk، وألما أوغارتي Alma Ugarte.

[١٥] http://donestech.net
[١٦] http://sinmiedo.com.co
[١٧] https://vimeo.com/207361788
[١٨] https://cyber-women.com/ar/downloads/quick-tips-gender-sensitive-learning-spaces-digital-security.pdf

موقع "لفل أب"[١٩]

موارد حول التدريب على السلامة الرقمية العالمية.

[١٩] https://level-up.cc/