FE-MALE
LOUD- PROUD- FEMINISTS

الدليل النسوي

للتدريب على الأمان الرقمي

الدليل النسوي

للتدريب على الأمان الرقمي

إعداد: نادين معّوض
ترجمة: فرح قبيسي

FE-MALE
LOUD- PROUD- FEMINISTS

حول جمعية:

هي مجموعة نسوية، مدنيّة وغير حكومية، رؤيتها الوصول إلى عالم عادل وخال من الممارسات والثقافة الأبوية. تعمل الجمعية مع النساء والفتيات من أجل القضاء على التمييز واللاعدالة الجندرية من خلال بناء حركة نسوية شابة، وتمكين صانعات وصنّاع التغيير وإطلاق ودعم الحملات الهادفة إلى إلغاء القوانين والسياسات والأفكار التمييزية.

بيروت، سامي الصلح
شارع الجامعة اللبنانية – كلية الفنون،
مقابل حديقة فرن الشباك العامة،
بناية الحايك، الطابق الأرضي

009611380873

info@fe-male.org

www.fe-male.org

FeMaleComms

الدليل النسوي للتدريب حول الأمان الرقمي من إنتاج جمعية **Fe-Male**

بالشراكة مع

المركز الدولي لقوانين منظمات المجتمع المدني **(ICNL).**

تم دعم الدليل ماليًا بالكامل من قبل حكومة الدنمارك. إن الأفكار الواردة في الدليل لا تعكس بالضرورة رأي الحكومة الدنماركية، بل هي مسؤولية الناشر حصرًا.

MINISTRY OF
FOREIGN AFFAIRS
OF DENMARK
Danida

كيفيّة استخدام هذا الدليل

لقد طوّرنا **هذا الدليل** لمساعدة النسويّات في منطقتنا على تخطيط وإدارة ورش عمل حول الأمان الرقمي في مجتمعاتهن ومنظماتهن. بالطبع، قام الكثير من النسويّات الرائعات بتطوير العديد من الكتيّبات حول الأمان الرقمي على مرّ السنين، وقمنا بالإحالة إلى العديد من هذا المحتوى الذي يمكنكِ اسكتشافه ضمن الأقسام المختلفة. استند الدليل هذا، بشكل خاص، إلى نتائج استطلاع الأمان الرقمي النسوي الذي أجريناه في أبريل ٢٠٢١ مع المدافعات الإقليميات عن حقوق الإنسان، بالإضافة إلى ثلاث ورش عمل تدريبية أجريناها في بيروت، وعبر الإنترنت لحضور إقليمي.

تتعدّد الآراء حول كيفيّة بناء الصمود الرقمي لمجتمعاتنا الناشطة. يبتعد المزيد من المدربين/ات عن صيغة «ورشة العمل». فقد كان النموذج المعتمد سابقًا هو إرسال فردٍ من منظمة ما، لحضور تدريب حول الأمان الرقمي لبضعة أيام، بعدها يقوم بتطبيق ما تعلّمه في منظمته. تَبِع ذلك نموذج «تدريب المدرّبين» الذي كان يُؤمَل منه توسيع نطاق المعرفة وإتاحة المزيد من الأيدي للمساعدة في تعزيز الممارسات الآمنة. في عام ٢٠١٥، نشرت **Tactical Tech** بحثًا مفيدًا لتقييم ١٠ سنوات من التدريب على الأمان الرقمي، يمكن الاطلاع عليه هنا:

https://secresearch.tacticaltech.org

انتقل المزيد من المدربين/ات، منذ عام ٢٠١٥، إلى نموذج «المرافقة» حيث ترافق خبير/ة في الأمان الرقمي المنظمة لمدة عام أو أكثر لبناء القدرات والمساعدة أيضًا في تنفيذ السياسات. يوصي العديد من الأشخاص أيضًا، بوضع ميزانية وتوظيف تقنيين/ات بدوام عمل كاملٍ في المنظمات الكبيرة، للقيام بهذا العمل. لهذه المحاولات هدف مشترك وهو: حماية المدافعين/ات عن حقوق الإنسان والمنظمات في مواجهة المخاطر الرقمية والمراقبة والقرصنة والرقابة.

وقد أضافت النسويّات تقليديًا إلى حركة الأمان الرقمي هذه، عنصرين هامّين: الأول، هو التصدّي للانحياز الذكوري في مجال التكنولوجيا. ثانيًا، رفض التعامل مع التقنيّة كمجرد أداة، دون الانخراط في البيئة السياسية التي تحكم مساحات وسياسات التكنولوجيا.

انطلاقًا من هذه الروحيّة

نوصي باستخدام هذا الدليل لغرضين:

1

للمساعدة في تطوير عدسة نسويّة في سياسات واقتصاد الإنترنت، بالإضافة إلى الأمان الرقمي.

غالبًا ما يضعنا الأمان الرقمي في موقف دفاعي. لذا، نحن بحاجة إلى اتّباع نهجٍ أكثر استباقية لحماية أنفسنا وتقديم تحليلنا لتصميم ولسياسة الإنترنت.

2

لفهم المبادئ الشاملة للأمان الرقمي، ذلك أنّ الأدوات والتطبيقات الموصى بها دائمة التغيّر.

مع ذلك، تبقى الرياضيات كما هي. لقد صمّمنا هذا الدليل للمساعدة على اكتساب الثقة وتعلّم الاستراتيجية، بحيث يمكن في المستقبل، تحديد الأداة المناسبة لغرضكِ وظرفكِ.

هذا الدليل هو بمثابة كتيّب تمهيدي لموضوع دائم التغيّر وشديد الاتساع. نحن في عام ٢٠٢١، ونواجه مشاكل عالميّة ومحليّة معقّدة. يمكن لأي قضيّة أن تستحق أقصى الاهتمام. وبالفعل، حوكمة التكنولوجيا هي إحدى هذه القضايا الملحّة. نشجعكِ على الغوص في مجالات اهتمامكِ الخاصة ونأمل أن تَلقي في هذه الصفحات ما يثير ويعزز ثقتكِ بنفسكِ حول إمكانيات الاشتباك النسوي مع التكنولوجيا.

تحضير أجندة التدريب

ستحتاجين إلى تنظيم الأجندة وفق الوقت المخصّص. من الممكن تعديل الأجندة لتحقيق مُخرج تعليمي واحد في الساعة، على الأقل. ومن الممكن تخصيص ساعات عدة أخرى للمُخرج التعليمي نفسه. إذ تتيح مساحة الوقت الإضافية، مجال تعلّم أعمق بالطبع. ولكن في كثير من الأحيان، يكون هذا خارج عن سيطرتنا، ويعتمد على الوقت الذي تتيحه المنظمة المضيفة وميزانيتها.

بشكل عام، نوصي بما يلي:

- **قومي دائمًا** بتضمين عنصر المناقشة السياسية في العرض أو التدريب، بصرف النظر عن محدوديّة الوقت. لا تفصلي أبدًا الأمان الرقمي عن السياق الاقتصادي-الاجتماعي للسياسة الرقمية.
- **قومي دائمًا** بمنح الأولويّة لمبادئ الأمان الرقمي بدلاً من أدوات الأمان، ذلك أنّ الأدوات متغيّرة.
- **استخدمي دائمًا** التمارين التي تبدأ من علاقة شخصيّة بالتكنولوجيا. يساعد ذلك في دحض الأسطورة حول احتكار المهندسين/ات لفهم التقنيّة.

نصائح في المنهجيّة

عند التدريب من منظور نسوي، من المفيد مراعاة ما يلي:

احرصي على عدم التحدّث من منطلق الخبيرة التي تمتلك كل المعرفة. ليس الهدف إظهار الخبرة، بل تعزيز الثقة على البحث والتحقّق من صحّة المعلومات المتاحة بسهولة على الإنترنت المفتوح.

لا تتردّدي في الإجابة بـ «لا أعرف، سوف أبحث عن الجواب»، إن لم تكوني متأكدة من الإجابة.

تجنّبي وصف الجوانب التقنيّة بأنها «شديدة التعقيد» أو تفوق القدرات الشخصيّة.

إن كنتِ تعملين مع مجموعات نسويّة، استفيدي من خبراتها ومعارفها في تحليل بيئة سياسة الإنترنت.

مُخرجات التعلّم وقياس الأثر

مُخرجات التعلّم مهمّة لأي معلّم/ة أو مدرّب/ة. ماذا تهدفين من كلّ جلسة؟ ماذا ستكسب المشاركات بنهايتها من معرفة ومهارات ومواقف وسلوكيات؟

إن ذهبت إلى الجلسة واضعةً في الاعتبار هدفًا واضحاً، يمكنكِ التركيز على تحقيقه. كما يسمح وضوح الهدف للمشاركات بالمشاركة الفاعلة في مسار تعلمهّن.

من المفيد تصميم المُخرج التعلّمي وصياغته على شكل فعل أو تصرّف يدلّ على اكتساب المعرفة أم المهارات المُرادة. فكّري في صياغة مُخرجات التعلّم وفق البنية التالية:

بنهاية هذه الجلسة، ستتمكّن المشاركات من

شرح / تعداد / تحديد

بنهاية هذه الجلسة، ستتمكّن المشاركات من

رسم / تقييم / تركيب

بنهاية هذه الجلسة، ستقوم المشاركات

بتحميل وتشغيل

يمكن قياس أثر التدريب باستخدام نموذج التقييم أو باستخدام نموذجَي الاختبار القبلي والبعدي للتدريب. يمكن لهذا الاختبار قياس مدى ازدياد المعرفة أو التغيّر في الموقف أو اكتساب المهارات.

وهنا بعض الأمثلة:

اختبار المعرفة

إن كنتِ تيسّرين جلسة حول حوكمة الإنترنت،

يمكن اختبار الزيادة في المعرفة، طبقًا لهذا المثال:

من الذي يضع سياسات الإنترنت؟

- الحكومات
- المجتمعات التقنيّة
- الشركات
- المجتمع المدني
- كلّ ما سبق (إجابة صحيحة)

إن كنت تدرّبين على مبادئ الأمان،

حدّد/ي مبدأين شاملين للأمان الرقمي:

اختبار المواقف والآراء

يقيس اختبار المواقف الآراء الشخصيّة، وهو طريقة جيدة لقياس مدى ازدياد الثقة بالتكنولوجيا. يمكن التحقّق من كيفيّة إجابة المشاركات قبل ورشة العمل وبعدها. وهنا بعض الأمثلة:

أفهم كيفيّة عمل المخاطر الرقميّة

(من ١ إلى ٥)

- أشعر أنّه من الممكن أن أكون آمنة تمامًا على الإنترنت (من ١ إلى ٥)
- أشعر أنّه يمكنني اتخاذ قرارات متينة بشأن الأدوات الآمنة التي يمكن استخدامها (من ١ إلى ٥)

نموذج الأجندة

عند التخطيط للأجندة، تذكري أنّ التحضير والمزيد من التحضير أمر أساسي – بخاصة عندما تكونين مبتدئة في هذا المجال. كلّما قمتِ بتضمين المزيد من التفاصيل في الأجندة، كلّما استعددتِ بشكل أفضل للجلسة.

تذكري أيضاً بأن تضافر الجهود من شأنه أن يؤمّن بيئة ملائمة للتعلّم للميسرة/ات والمشارِكات على حد سواء، لذا أطلبي الدعم من فريقك أو من المنظمة المضيفة، وتأكّدي من مشاركة الأجندة المفصّلة معهن والاتفاق على توزيع الأدوار.

يمكنك استخدام النموذج التالي للأجندة وتعديله كما ترينه مناسباً، وعامةً ما نشارك النسخة المبسّطة من الأجندة (أي العواميد الثلاث الأولى) والمخرجات التعلّمية للتدريب مع المشارِكات للاطلاع عليها والتعليق.

مدّة الجلسة	عنوان الجلسة	مُخرج/ات التعلّم	تفاصيل الجلسة والملاحظات	الميسّرة/ات	المواد المطلوبة

إليكِ مثال على أجندة تدريب لمدة ٤ ساعات حول التصفّح الآمن:

مدّة الجلسة	عنوان الجلسة	مُخرج/ات التعلّم	تفاصيل الجلسة والملاحظات	الميسّرة/ات	المواد المطلوبة
٣٠ دقيقة	إعداد المساحة المشتركة	بنهاية الجلسة، ستتعرّف المشاركات على بعضهن البعض ويتعرّفن على التوقعات المشتركة لحيّز ورشة العمل هذه وسيضعن أيضًا سويًا قواعد الجلسة.	ترحب الميسّرة بجميع المشاركات في التدريب وتطلب من الجميع تقديم أنفسهن ومشاركة توقعاتهن من ورشة العمل (١٥ دقيقة) تضع المشاركات، بشكل جماعي، قواعد «المساحة الآمنة» (١٥ دقيقة)	مهى (الميسرة الرئيسية) سامية (الدعم)	-ورق لاصق كبير من ٥ ألوان -لوح ورقي -أقلام
٦٠ دقيقة	كيف تعمل المتصفّحات	بنهاية الجلسة، ستتمكّن المشاركات من شرح كيفيّة عمل المتصفّحات تقنيًا وتحديد مجالات المخاطر المرتبطة بالتصفّح.	تقدم الخبيرة عرضًا حول الجوانب التقنيّة للمتصفحات وتشرح أين تكمن المخاطر (٤٥ دقيقة) تطرح المشاركات أسئلة استيضاحيّة (١٥ دقيقة)	سارة (خبيرة) مهى (دعم)	-بروجكتور - كابل HDMI لابتوب - Slide deck
٣٠ دقيقة	استراحة قهوة				
٩٠ دقيقة	تمرين عملي: متصفّح آمن	بنهاية الجلسة، ستتحوّل المشاركات إلى التصفّح الآمن ويقمن بتثبيت الوظائف الإضافية وتنظيف معلومات التصفّح القديمة من أجهزة الكمبيوتر والهواتف المحمولة. تقدم الخبيرة عرضًا حول الأدوات الموصى بها للتصفّح الآمن (٣٠ دقيقة).	تقوم الميسّرة بإرشاد المشاركات للعمل على أجهزة الكمبيوتر والهواتف المحمولة الخاصة بهن للانتقال إلى تصفّح أكثر أمانًا، بدعم من الخبيرة (٦٠ دقيقة).	سارة (خبيرة) مهى (دعم)	- بروجكتور - كابل HDMI لابتوب - Slide deck - محركات أقراص USB مع حزم تثبيت البرامج
٣٠ دقيقة	الختام والتقييم	بنهاية الجلسة، تقوم المشاركات بتقييم معلوماتهن وترسيخها.	تلخص الميسّرة الدروس المستفادة في اليوم وتطلب من المشاركات مشاركة تقييمهن لما تعلّمنه وما نوع الدعم الذي يرغبن به في المستقبل.	مهى (الميسرة الرئيسية)	نماذج التقييم المطبوعة

* ملاحظة: إن الأمثلة المعطاة هنا ترتكز على تقنيات التدريب وجهاً لوجه وما يتيحه من مساحة ماديّة مشتركة. وفي حال اخترت أو اضطرك الأمر إلى تنفيذ التدريب عبر الإنترنت، قومي بتعديل التمارين وتطويعها بحيث تلائم ظروف المساحات الافتراضية وتستخدم أدوات التدريب المتاحة عبر الإنترنت، مثل ألواح الكتابة الالكترونية (**whiteboard**) أو شرائح العرض المتاحة لمساهمة المشاركات. ومن الممكن الاطلاع على دليل التدريب عبر الإنترنت الذي طورته منظمة ٣٥٠ هنا:

https://trainings.350.org/resource/online-monster-manual/

*نصيحة: قومي بعمل نسخة ورقية من الأجندة لترافقك أثناء التدريب، وقومي بتدوين أيّ ملاحظات حول كيفيّة سير الأمور في الجلسات الفعليّة؛ ربما كان عليكِ إضافة المزيد من الوقت لمُخرج ما، أو أنّ تمرينًا معيّنًا لم يسرْ كما هو مخطط له. بهذه الطريقة، يمكن العودة إلى النسخة الورقية عند التحضير للتدريب التالي وتذكّر ما نجح وما يحتاج إلى تحسين.

* تذكير: خصّصي وقتًا إضافيًا كافيًا لأيّ تطبيق عمليّ مع المشاركات حول برنامج آمن. قد تظهر العديد من السّقطات (مثل نفاذ البطارية، اتصال إنترنت بطيء، تعرّف المشاركات على البرنامج، إلخ.)

تمارين كسر الجليد

مشاركة الخبرات (دقيقتان لكل مشارِكة)

عند الإنتقال بين المشاركات في الغرفة لتعريف أنفسهن، استدعي ما يربطهن بالتكنولوجيا. إذ أنّ تشجيع المشاركات على إعادة التفكير في تجاربهن السابقة مع الإنترنت يشكّل أحد الأمثلة الممتعة. إليكِ بعض النماذج:

تمرين سلّم الآراء

(١٥ – ٣٠ دقيقة)

اطلبي من المشاركات الاصطفاف وفق سلّم آراء يبدأ من «أوافق بشدة» انتهاءً بـ» لا أوافق بتاتًا»، مع إتاحة خيار الوقوف في الوسط إن كنّ مترددات بشأن الإجابة. شاركي عبارات حول الحقوق الرقميّة ولاحظي كيف تتحرّك المشاركات. استطلعي بعض الآراء من جوانب السلّم المختلفة. شجّعي المشاركات على التحرك متى سمِعن من زميلاتهن حجّة مقنعة أو بدّلن آرائهن.

- أخبرينا عن تجربتكِ الأولى مع الإنترنت
- ما هو أوّل ما قمتِ بالبحث عنه على الإنترنت؟
- أطلعينا على أوّل مدوّنة أو محتوى رقمي قمتِ بنشره

يمكنكِ أيضًا استدعاء ما يحفّز مخيّلة المشاركات حول التكنولوجيا.

إليكِ بعض الأمثلة:

- إن كان لديكِ تمويلاً غير محدود، ما هي التقنيّة الجديدة التي ستقومين بابتكارها؟
- إذا كان لديكِ روبوت مساعد، ما الوظائف التي تريدين منه القيام بها يوميًا؟
- ما هي الفكرة التي تجول في رأسك لتطبيق لطالما اعتقدتِ بأنه سيكون مفيدًا؟

إليكِ بعض الأمثلة عن العبارات الممكنة:

- لا توجد خصوصيّة على الإنترنت بتاتاً، لذا لا ينبغي لنا شَغل أنفسنا بالموضوع.
- أنصح ابنة أخي المراهقة بعدم إرسال صور عارية من هاتفها.
- توفّر شركات وسائل التواصل الاجتماعي حرية تعبير أكبر من وسائل الإعلام التقليدية.
- من الممكن أن تكوني آمنةً جدًا في التواصل الإلكتروني.
- تُشجّع المجهولية على العنف الإلكتروني.
- يجب على الحكومات حجب المواقع الإباحية لأنها ضارة.

تذكير: لا يهدف هذا التمرين إلى التعلّم، بقدر ما يهدف إلى فتح النقاش. من المستحسن أن تختاري العبارات التي تشكّل موضوعات ستعودين إليها لاحقاً خلال التدريب، لكي تتيحي للمشاركات فرصة تعلّم المزيد حول هذه القضايا.

القسم الأول:
التكنولوجيا من منظور نسوي

على الرغم من أنّ البرمجة بدأت أساساً كـ «وظيفة نسائية»، نعلم جيدًا مدى تفشّي التمييز الجندري في مختلف مجالات التكنولوجيا؛ ففي العادة، لا يتم تشجيع الفتيات على دراسة العلوم أو الرياضيات؛ وليس هذا بالأمر الجديد! فنحن نعلم أنّ مجالات التكنولوجيا تهيمن عليها الثقافة الذكورية فضلاً عن التمييز ضد النساء؛ وواقع الأمر، أنّه لا بدّ من إزالة الحواجز التي تُثني الفتيات عن الالتحاق بالعلوم والتقنيّة، لتعكس هذه الأخيرة، وبشكل أفضل، الخبرات والمصالح المشتركة للنساء في هذه المجالات. لكن لا يجب أن نتوقف عند هذه النقطة وحسب. فنحن بحاجة إلى مقاربة نسويّة لتصميم وحوكمة التكنولوجيا– بخاصةٍ الآن في العام ٢٠٢١، حيث تنقلنا التطورات التقنيّة، بشكل كبير، نحو شكل جديد من النظام الرأسمالي العالمي المبني على المعلومات والمراقبة.

دحض الأسطورة

من السهل على التقنيين جعل النساء يشعرن بأنّ التكنولوجيا ليست من اختصاصهن. وقد تشعرين بأنك لستِ مؤهلة للتدريب على الأمان الرقمي لأنكِ لم تدرسي علوم الكمبيوتر أو الهندسة.

لكن تذكّري!

X لستِ بحاجة إلى أن تكوني مهندسة ميكانيكية لتعرفي أنّ النقل العام يربط المجتمعات ويعزّز المشاركة الاقتصادية.

X لستِ بحاجة إلى أن تكوني مهندسة كهرباء لتعرفي أنّ الكهرباء ضرورة وحقّ للجميع.

X لستِ بحاجة إلى أن تكوني كيميائية أو صيدلانية لتعرفي أنّ الكل يحتاج إلى سهولة الوصول إلى الأدوية المنقذة للحياة.

التكنولوجيا هي مظهر من مظاهر الإبداع البشري لحل المشكلات ويمكننا جميعًا المشاركة في تصميمها وحوكمتها – وعلينا إتاحة المساحات التي تسمح لنا بالقيام بذلك.

إنّ المكان الأفضل للبدء في استكشاف مجال التكنولوجيا من منظور نسويّ هو المبادئ النسويّة للإنترنت التي عملت على تطويرها جمعية الاتصالات التقدمية **(APC)** وشبكة كبيرة من مجموعات التكنولوجيا النسويّة من جميع أنحاء العالم. قومي بزيارة

www.feministinternet.net

لتصفّح المبادئ السبعة عشر– حيث يناقش كلٌ منها وجهة نظر نسويّة حول قضايا التكنولوجيا. وقد قمنا باستعراضها في الأقسام الآتية.

اعتمادًا على الوقت المتاح واهتمامات المجموعة، يمكن فتح نقاش حول واحد أو أكثر من القضايا المعنيّة بالتكنولوجيا. يحتوي موقع الإنترنت النسوي على الكثير من التمارين التمهيدية لحثّ المشاركات على التفكير– بأنفسهن – حول ما يقوم به أو يبدو عليه أو يسهّله الإنترنت النسوي. لقد قمنا بتكييف أحد هذه التمارين كاقتراح هنا:

تمرين:
تخيّلي الإنترنت النسوي

(٢٠ – ٣٠ دقيقة)

المواد المطلوبة:
أوراق لاصقة وأقلام ولوحات ورقية

1

اطلبي من المشاركات التفكير، في مجموعات أو بشكل فردي، في ما يعنيه الإنترنت النسوي بالنسبة إليهن. استخدمي عبارات توجيهية مثل: «في الإنترنت النسوي...» أو «الإنترنت النسوي هو...» ليكملنها بكلمة أو عبارة أو فقرة. قد يكتبن الأفكار على أوراق لاصقة ملوّنة أو على لوحات ورقية أو في ملف مشترك على الإنترنت. إنّه وقتهن للإستكشاف والحلم.

2

قومي بجمع هذه الأفكار وتحديد الكلمات المفتاحية وتقسيمها وفق ترابطها. يمكن تعميق النقاش وفق ما تحدّده المشاركات من أولويّة أو يمكن استخدام المُخرجات كمدخل للعرض.

هناك طريقة أخرى للقيام بهذا التمرين، وهي الطلب من المشاركات «التصويت» على أكثر الكلمات المفتاحية إثارة لإعجابهن عن طريق لصق نقاط صغيرة على البطاقات، لإظهار دعمهن لأفكار مطروحة. يجب أن تحصل كلّ مشاركة على عدد محدّد من «النقاط» للصقها، مع إمكانية لصقها جميعًا حول فكرة واحدة لتظهير وزنها. هذه الخطوة مفيدة بعد القيام بتجميع أو تلخيص المدخلات.

المبادئ النسويّة للإنترنت

يعمل الإنترنت النسوي على تمكين عدد أكبر من النساء والأفراد الكويريين/ات، بكلّ تعدداتنا، على التمتّع الكامل بحقوقنا والمشاركة في المتعة واللعب وتفكيك النظام الأبوي. وذلك بدمج اختلافات واقعنا وسياقاتنا وخصوصياتنا، بما في ذلك الأعمار والإعاقات والجنسانيات والهويات والتعبيرات الجنسية والمواقع الاقتصادية والاجتماعية والقناعات الدينية والسياسية والأصول الإثنية والعرقية.

إنّ تَحقُّق المبادئ الأساسية التالية حاسم في القدرة على إدراك إنترنت نسوي.

الاتصال

١. الاتصال بالإنترنت

يبدأ الإنترنت النسوي بتمكين عدد أكبر من النساء والأفراد الكويريين/ات من التمتّع بإتصال بالإنترنت شامل ومقبول وميسّر التكلفة وغير مشروط ومفتوح ومجدي ومتساوٍ.

٢. الوصول للمعلومات

نحن نحمي وندعم الوصول غير المقيّد للمعلومات العامّة للنساء والأفراد الكويريين/ات، وبخاصة المعلومات المتعلّقة بالحقوق والصحة الجنسية، والإنجابية، والمتعة، والإجهاض الآمن، والمعلومات القانونية، وقضايا مجتمع الميم. ويتضمّن ذلك استيعاب تعدّد القدرات واللغات والاهتمامات والسياقات.

٣. استخدام التقنية

يحق للنساء والأفراد الكويريين/ات، تصميم وتعديل واستخدام تقنية المعلومات والاتصالات بشكل نقدي ومستدام، لاستعادة التقنيّة كمنبر للإبداع والتعبير، ومواجهة ثقافة التحيّز الجنسي والتمييز بأشكالها المتعدّدة في كل المجالات.

الحركات والمشاركة العامة

٤. المقاومة النسوية

الإنترنت مساحة يتم فيها ممارسة الأعراف الاجتماعية وفرضها وإعادة التفاوض عليها. وعادةً ما تكون امتدادًا لمساحات تشكّلت من خلال الأبوية والغيرية الجنسية. لذا، فإن مقاومتنا على الإنترنت هي امتداد لمقاومتنا في مساحات أخرى، عامة وشخصية أو ما بينهما.

٥. بناء الحركات

الإنترنت مساحة سياسية للتغيير، تُسهّل أشكالاً جديدة من المواطنة، متيحة للأفراد إمكانيّة تشكيل وإعلان ذواتهم/ن وأنواعهم/ن الاجتماعية وجنسانياتهم/ن والتعبير عنها، بما يتضمنه ذلك من تشبيك عابر للحدود، للمطالبة بالمساءلة والشفافية وخلق فرصٍ لبناء حركة نسوية مستدامة.

٦. حوكمة الإنترنت

نسعى لتحدّي الفضاءات الأبويّة التي تسيطر حاليًا على شبكة الإنترنت، عبر تمكين عدد أكبر من النسويّات والكويريين/ات من المشاركة في صنع القرار في حوكمة الإنترنت. ونؤمن بإضفاء الطابع الديمقراطي على التشريعات وتنظيم شبكة الإنترنت، كما في توزيع الملكية والسلطة في الشبكات العالمية والمحلية.

الاقتصاد

٧. الاقتصاديات البديلة

نلتزم بمساءلة المنطق الرأسمالي الذي يدفع بالتقنيّة نحو المزيد من الخصخصة والربح وسلطة الشركات. ونعمل لخلق أشكالٍ بديلة من القوّة الاقتصادية، تقوم على مبادئ التعاون والتضامن والمشاعات والانفتاح والاستدامة البيئية.

٨. المصادر الحرة والمفتوحة

نلتزم بالخلق وبالتجريب في التقنية، لا سيّما على صعيد الأمان والسلامة الرقميّين واستخدام البرامج والأدوات والمنصات الحرّة ومفتوحة المصدر. ويلعب كل من دعم ونشر ومشاركة المعرفة في ما خصّ البرمجيات مفتوحة المصدر، دورًا محوريًا في ممارستنا الرقمية.

التعبير

٩. تعزيز الخطاب النسوي

نستخدم قوة الإنترنت لتعزيز سرديّات النساء وواقعهن المُعاش. هناك حاجة لمقاومة الدولة والمجموعات الدينية اليمينية وأي قوى متطرفة أخرى، تحتكر الخطاب الأخلاقي، فيما تُسكت الأصوات النسويّة وتضطهد المدافعات عن حقوق الإنسان.

١٠. حرية التعبير

ندافع عن الحق في التعبير الجنسي كأحد الحقوق التي لا تقلّ أهميّة عن الحق في حرية التعبير السياسي أو الديني. ونعارض بشدّة جهود الجهات الحكومية وغير الحكومية في استخدام التقنية والتشريعات أو العنف، لضبط وتنظيم ومراقبة وتقييد أشكال التعبير النسوي والكويري على الإنترنت. ونصنّف هذا الأمر، كجزء من مشروع سياسيّ أكبر من التأديب والرقابة والهيمنة الهرمية للمواطنة والحقوق.

١١. المواد الإباحية والمحتوى الضار

ندرك أنّ قضية المواد الإباحية على الإنترنت، موضوعٌ يرتبط بالوكالة والرضائية والسلطة والعمل. نحن نرفض العلاقات السببيّة الاختزالية التي تربط بين استهلاك المحتوى الإباحي والعنف ضد النساء. كما نرفض تعميم مصطلح «محتوى ضار» لوصم التعبير عن جنسانية النساء والأفراد العابرين/ات للنوع الاجتماعي. وندعم استعادة وخلق محتوى مثير وبديل للسائد- الذي يخضع للمعايير الأبويّة- يُمركز رغبات الأفراد الكويريين/ات والنساء.

الوكالة

١٢. الرضائية

نحن نطالب بتضمين أخلاقيات وسياسات الرضائية، في ثقافة وتصميم وسياسات وشروط استخدام منصّات الإنترنت. تكمن وكالة النساء، في قدرتهن على اتّخاذ قرارات مستنيرة في ما يخص جوانب حياتهن العامة أو الخاصة التي يردن مشاركتها على الإنترنت.

١٣. الخصوصية والبيانات

ندعم الحق بالخصوصية وبالسيطرة التامة على البيانات والمعلومات الشخصية على كل المستويات على الإنترنت. ونعارض استخدام البيانات من قبل الدول أو الشركات من أجل الربح والتلاعب بالمستخدمين/ات. فلطالما كانت المراقبة، الأداة التاريخية للأبوية، والتي أُستُخدمت ومازالت، لضبط وتقييد أجساد النساء وخطابهن ونشاطهن. ويتساوى قلقنا من المراقبة، بغضّ النظر عن مصدرها، سواء كانت مؤسسات حكومية أو غير حكومية أو قطاع خاص أو أفراد.

١٤. الذاكرة

يحق لنا السيطرة على تاريخنا الشخصي وذاكرتنا على الإنترنت. يشمل ذلك القدرة على الوصول لكل معلوماتنا الشخصية وبياناتنا على الإنترنت والقدرة على التحكّم في تلك البيانات، بما في ذلك معرفة من يحق له/ا الوصول إليها ووفق أية شروط وتمكيننا من محوها للأبد.

١٥. المجهوليّة

ندافع عن الحق في المجهوليّة على الإنترنت، ونرفض الادّعاءات التي تحدّ من الحق في استخدامها. تسمح المجهوليّة بحريّة التعبير على الإنترنت، بخاصة في ما يتعلّق بكسر مسلّمات وتابوهات حول الجنسانية والغيرية والتجريب في الهوية الجندرية وتحقيق الأمان للنساء والأفراد الكويريين/ات العرضة للتمييز.

١٦. الأطفال والشباب

ندعو لتضمين تجارب الشباب وأصواتهم/ن في عملية اتخاذ القرارات المتعلّقة بالأمان والسلامة على الإنترنت، ونشجّع أمانهم/ن وخصوصيتهم/ن وحقّهم/ن في الوصول للمعلومات. نعترف بحقّ الأطفال في نمو عاطفي وجنسي صحي، بما في ذلك حقّهم في الخصوصية وفي الوصول لمعلومات إيجابية حول الجنس والنوع الاجتماعي والجنسانية في المحطات الحرجة من حياتهم.

١٧. العنف عبر الإنترنت

ندعو كل المعنيين/ات بالإنترنت من مستخدمين/ات وواضعي السياسات والقطاع الخاص إلى التعامل بجدّية مع مشكلة التحرّش على الإنترنت والعنف المرتبط بالتقنية. إذ تتعرّض النساء والأفراد الكويريين/ات، لحملات تهجّم وتهديد وتخويف وسيطرة حقيقية مؤذية ومقلقة، تشكّل امتدادًا لمشكلة العنف المبني على أساس النوع الاجتماعي. إنّ مسؤوليتنا الجماعية تفرض التعامل مع هذا العنف ووضع نهاية له.

التدريب على المبادئ

النموذج الأول:
الوصول إلى الإنترنت

مُلاحظات للميسّرة

يشكّل التالي إحدى المنهجيات التي بالإمكان استخدامها لجلسة نقاش:

١. إبدئي بسؤال سريع واطلبي من كل مشاركة إجراء محادثة موجزة مع من تجاورها حول الموضوع (٥ دقائق). الأمثلة هي:

- هل يجب اعتبار الوصول إلى الإنترنت حقًا من حقوق الإنسان؟
- لماذا توجد فجوة جندرية في الوصول إلى الإنترنت؟
- ما هي قيمة فاتورة الوصول إلى الإنترنت؟ كيف تقارن هذه الفاتورة بالفواتير الشهرية الأخرى؟
- كيف تؤثر سرعة الإنترنت على استخدامك اليومي؟

٢. اطلبي من المشاركات مشاركة بعض الأفكار مع بقية المجموعة (٥–١٠ دقائق)

٣. قدّمي عرضًا موجزًا لبعض النقاشات الحالية حول الوصول إلى الإنترنت. أفضل مكان للبدء هو شرح تاريخ البنية التحتية لكابلات الإنترنت وعرض بعض الخرائط العالمية أو الاقليمية لها. سوف تُفاجأ معظم المشاركات عندما يعلمن أنّ الإنترنت يمر بكابلات كبيرة عابرة للمحيطات والأقاليم. جدي خريطة للكابلات البحرية والبرية لبلدك. حدّدي كيفيّة اتخاذ القرارات بشأن الخرائط ومن يدفع ثمنها وكيف تتم جدولة الصيانة وما إلى ذلك.

٤. اعرضي المبدأ النسوي حول الوصول إلى الإنترنت وامنحي الوقت للأسئلة والتعليقات.

محتوى العرض

المبدأ النسوي حول الإتصال بالإنترنت

يبدأ الإنترنت النسوي بتمكين عدد أكبر من النساء والأفراد الكويريين/ات من الوصول إلى الإنترنت بشكل شامل وميسّر التكلفة وغير مشروط ومفتوح ومجدي ومتساوٍ. خدمات الوصول العامة مقابل خدمات الوصول الخاصة للإنترنت

الفجوة الجندرية في الوصول إلى الإنترنت

في خضمّ هذه النقاشات، غالبًا ما تتم الإشارة إلى النساء في البلدان النامية كمجموعة مستهدفة هشّة، بدلاً من صاحبات مصلحة ممّن لديهن دور حاسم في تقرير نوع الإتصال بالإنترنت الذي يضمن الحقوق بدلاً من تقييدها.

تقدّر **The Web Foundation** أنّ «احتمال نفاذ الرجال للإنترنت، أعلى بنسبة ٢١٪ من النساء، وترتفع النسبة إلى ٥٢٪ في البلدان الأقل نمواً في العالم». هناك العديد من الأسباب الكامنة وراء الفجوة الجندرية – بما في ذلك القدرة على تحمّل التكاليف والتعليم والمهارات الرقمية ومستويات الدخل أو العيش في المناطق الريفية.

تم اقتراح إتاحة الوصول للإنترنت كحق من حقوق الإنسان لأول مرة في الأمم المتحدة، من قبل المقرّر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير في عام ٢٠١١. مع ذلك، يستمر النقاش حول معايير الإتصال بالإنترنت بين مجتمع التقنيين/ات والقطاع الخاص والحكومات والمجتمع المدني في ظل مصالح مختلفة ومتضاربة في كثير من الأحيان، لا سيّما حول ربط الـ ٤٠٪ المتبقية من سكان العالم بالإنترنت. تدّعي الشركات الخاصة أنها تربط المزيد من الأشخاص بالإنترنت عبر برامج الوصول «المجانية» مثل تطبيق **Free Basics** التابع لشركة فايسبوك أو **Google Balloons**.

إلاّ أنّ ما تقدّمه هذه الشركات عبر هذه البرامج هو إتاحة تطبيقات الشركة أو خدماتها، حصرًا. هذه ميزة مُقيّدة بشكل رهيب – من أغنى شركات العالم – أولويتها إنشاء مستخدمين/ات جدد وجمع البيانات. يضع ذلك قيودًا كبيرة على المستخدمين/ات الجدد.

يؤكّد المبدأ النسوي حول الوصول إلى الإنترنت على نوع الإنترنت الذي نريده: ميسّر التكلفة ومتساوٍ وشامل؛ خاصة بالنظر إلى الفجوة الرقميّة الجندرية الحالية التي تؤثر على مستخدمات الإنترنت اليوم.

المنطقة	مستخدمي الإنترنت من الرجال	مستخدمي الإنترنت من النساء	الفجوة الجندرية في استخدام الإنترنت
أميركا الشمالية	٪٩٥	٪٩٤	٪١
أميركا اللاتينية	٪٦٤	٪٦٠	٪١٢
أوروبا	٪٨١	٪٧٧	٪٥
الشرق الأوسط وشمال أفريقيا	٪٧٩	٪٧٧	٪٩
أفريقيا جنوب الصحراء الكبرى	٪٣٨	٪٢٨	٪٤٣
آسيا الوسطى	٪٦٤	٪٥٧	٪١٥
شرق اسيا	٪٨٦	٪٨٣	٪٢
جنوب شرق آسيا والمحيط الهادئ	٪٦٧	٪٦٠	٪١١
جنوب آسيا	٪٣٧	٪١٨	٪١٣٧

المصدر: www.webfoundation.org (مارس ٢٠٢٠)

حوكمة الإنترنت

ملاحظات للمدرّبة / الميسّرة

عند التدريب على الحقوق الرقميّة، سترغب المشاركات بتعلّم كيف باستطاعتهن التأثير فيها. فمعرفة أنّ سياسة الإنترنت يقرّرها بشر، ليس بالأمر البديهي لمعظم الناس. الغالبية تعتقد أنّ ذلك في متناول مجتمع التقنيّين/ات حصرًا. لذا، من المهم تشجيع المشاركات على إضفاء منظور نسوي على جهود المناصرة المتعلّقة بسياسات التكنولوجيا. في ما يلي، بعض الأفكار لفتح النقاش حول هذا الموضوع:

مضمون العرض

المبدأ النسوي حول حوكمة الإنترنت:

نسعى لتحدّي الفضاءات الأبويّة التي تسيطر على شبكة الإنترنت، عبر تمكين عدد أكبر من النسويّات والكويريين/ات من المشاركة في صنع القرار في حوكمة الإنترنت. ونؤمن بإضفاء الطابع الديمقراطي على التشريعات وتنظيم شبكة الإنترنت، كما في توزيع الملكية والسلطة في الشبكات العالمية والمحلية.

١. اسألي المشاركات عمّا إذا كنّ قد قرأن الشروط والأحكام (**Terms & Conditions**) الخاصة بشبكات التواصل الاجتماعي مثل إنستغرام وتويتر. إن كان لديكِ ١٠ دقائق إضافية، اطلبي منهن البحث عن هذه الشروط وقراءتها.

٢. في بضع دقائق، اطلبي من المشاركات شرح الشروط. ما الذي فاجأهن؟ هل كان من السهل فهمها؟ ما هي القواعد التي لم يكنّ على بيّنة منها؟

٣. انتقلي إلى شرح كيفيّة قيام الهيئات المختلفة (الشركات والحكومات والمجتمعات التقنيّة) باتخاذ قرارات بشأن سياساتها وبروتوكولاتها. سيكون من المفيد أيضًا المرور على تاريخ بروتوكولات الإنترنت. يهدف ذلك، إلى مساعدة المشاركات على فهم أنّ البشر (غالبًا من الرجال البيض) يتخذون قرارات، ويضعون قواعد يومية بشأن الإنترنت. وأنّه بالتالي، يمكنهن الانخراط في هذه النقاشات من منظور نسوي.

٤. اعرضي المبدأ النسوي حول حوكمة الإنترنت وامنحي الوقت للأسئلة والتعليقات.

كيف يمكنني التأثير في سياسة التكنولوجيا؟

أنشأت الأمم المتحدة منتدى حوكمة الإنترنت **www.intgovforum.org** عام ٢٠٠٦ لتيسير نقاش عالمي حول قضايا السياسات العامة المتعلّقة بالإنترنت. ويعتبر المنتدى منصّة متعدّدة الأطراف تجمع حول طاولة واحدة الحكومات والمجتمعات التقنيّة والقطاع الخاص والمجتمع المدني. ويتم الحشد لمنتدى حوكمة الإنترنت العالمي السنوي من خلال تنظيم المنتديات على المستويين الوطني والإقليمي (مثل منتدى حوكمة الإنترنت العربي).

لا تصدر عن منتدى حوكمة الإنترنت قرارات دولية ملزمة. مع ذلك، يشكّل المنتدى مساحة جيدة ومفيدة من أجل:

١. مناقشة القضايا الناشئة المتعلّقة بإدارة الإنترنت

تُحدَّد جميع ندوات وورش عمل منتدى حوكمة الإنترنت من خلال عملية تشاورية مفتوحة. هكذا، باستطاعة أيّة منظمة اقتراح قضايا معيّنة للنقاش ووضعها على جدول الأعمال وترشيح المتحدثين/ات فيها. وبالنظر إلى كون المنتدى متعدّد الأطراف، تحاول الهيئة المنظمة التأكّد من أنّ المجموعات المختلفة تتحدث مع بعضها البعض- عوضاً عن حصر النقاش في دوائر المجتمع المدني فقط.

٢. الضغط على الحكومات والشركات الخاصة في مسائل الحقوق الرقميّة

غالبًا ما يحضر وزراء الاتصالات وغيرهم من المسؤولين الحكوميين منتديات حوكمة الإنترنت الإقليمية والعالمية. ووفق المنطقة الجغرافية، قد تشهد بعض المنتديات حضورًا حكوميًّا وازنًا (مثل منتدى حوكمة الإنترنت العربي)، بينما يشهد بعضها الآخر تنظيمًا أقوى للمجتمع المدني. وجرت العادة، أن يُرسل عمالقة التكنولوجيا كفايسبوك وغوغل ومايكروسوفت، ممثلين/ات إلى هذه المنتديات. لذا، من المفيد حضور المجتمع المدني وناشطات\ نشطاء حرية الإنترنت هذه المنتديات وتنظيم الفعاليات للاجتماع مع، أو الضغط على، أو نقاش ممثلي/ات الحكومات والقطاع الخاص.

٣. الضغط على مسؤولي الأمم المتحدة من أجل سياسات عادلة للإنترنت

على الرغم من أنّه ليس بإمكان منتدى حوكمة الإنترنت إصدار وثائق مُلزمة رفيعة المستوى – إذ أنّ الدول الأعضاء في الأمم المتحدة لا تصوّت عليها – إلاّ أنّه قد يكون للبيانات أو التقارير الصادرة عن المنتدى، تأثير في مساحات أخرى تابعة للأمم المتحدة. فعلى سبيل المثال، قد يحضر أحيانًا المقرّرون الخاصّون فعاليات منتدى حوكمة الإنترنت للتعرّف على القضايا المتعلقة بالتكنولوجيا. فإن كان هدفك التأثير على الأمم المتحدة بشأن حرية التعبير أو العنف ضد النساء على الإنترنت، يمكنك التحقّق من وكالات الأمم المتحدة الحاضرة، ووضع خطط المناصرة المناسبة بناءً على ذلك.

٤. الدفع بأجندة نسويّة

لقد نما التمثيل النسائي والكويريّ في منتدى حوكمة الإنترنت بشكل كبير على مدار السنوات السابقة، لكنّه ما يزال محطّ صراع بخاصة على صعيد المنتديات العربية. وقد مارست النسويّات ضغوطات من أجل مسارات ومبادرات مختلفة في منتدى حوكمة الإنترنت، كمتابعة مدى تمثيل النساء في الندوات، وتضمين قضايا النوع الإجتماعي في جدول الأعمال. فإن كنتِ تخطّطين لحضور أحد منتديات حوكمة الإنترنت، يمكن زيارة الموقع التالي للاطّلاع على هذه الجهود:

https://www.intgovforum.org/multilingual/content/gender-and-internet-governance

لقد طوّرت منظمة **APC** مواد تعليمية حول الجنسانية وحوكمة الإنترنت، يمكن أن تساعد في فهم حوكمة الإنترنت والقضايا المتعلّقة بالمحتوى التقاطعي والجنساني.

المواد متاحة على هذا العنوان الإلكتروني:

https://en.ftx.apc.org/shelves/sexuality-and-internet-governance

منتديات المجتمع المدني

بما أنّ منتدى حوكمة الإنترنت عبارة عن اجتماع رسميّ متعدّد الأطراف، فقد قرّر المجتمع المدني عقد عدة اجتماعات سنوية أخرى للدفع قُدُماً بنقاشاتٍ حول قضايا حريات الإنترنت. إليكِ بعض المنتديات التي يمكنكِ البحث عنها والتحقّق من فرص الحضور أو المشاركة بها شخصياً أو عن بُعد.

خبز ونت – ملتقى حول الحقوق الرقميّة يركّز على منطقة الشرق الأوسط وشمال إفريقيا

/https://www.breadandnet.org

- RightsCon
- MozFest
- Internet Freedom Festival
- MisInfoCon
- RightsCon
- Internet Freedom Festival
- SXSW
- Global Privacy Summit
- re:publica
- Stockholm Internet Forum
- Privacy Risk Summit
- Allied Media Conference
- DEF CON
- Global Voices Summit

القسم الثاني:
الأمان الرقمي

للأمان الرقمي الخاص بالمجموعات **عنصرين أساسيين:**

1

السياسات العامة وهي مجموعة القواعد التي تهدف إلى الحماية الرقمية وتفصّل كيفيّة الردّ على الاختراقات.

2

الممارسات الفعلية وهي الروتين اليومي الذي يجب على الجميع اتّباعه لضمان الأمان للمجموعة أو المؤسسة أو الشبكة.

تطوير السياسات العامة

تشكّل أداة تقييم الأمان الرقمي **(CAT)** التي أعدّتها مؤسسة فورد، أداة جيدة للانطلاق في وضع السياسات المشتركة للأمان الرقمي للمجموعة:

https://www.fordfoundation.org/work/our-grants/building-institutions-and-networks/cybersecurity-assessment-tool/

تحتوي الأداة على استبيان يستغرق ملؤه حوالي ١٥ دقيقة ويشمل أربعة مجالات مختلفة من الأمان الرقمي: التشغيل والأجهزة والحسابات والمخاطر الخاصة بمجال العمل. لا تقلقي من جراء إجابتك بالكثير من الـ«لا أعرف» أو «لا أجوبة». يجب ألا تربكك الأداة. على العكس من ذلك، يجب أن تمنحكِ نظرة شاملة لجميع مجالات سياسات الأمان الرقمي التي تحتاجين إلى تطويرها. وبمجرّد الانتهاء من ملء الاستبيان، ستحصلين على عدة صفحات من الخطوات اللاحقة الموصى بها لكل قسم.

من المفيد جدًا طلب المساعدة من خبير/ة في الأمان الرقمي للمرافقة في وضع السياسات واعتماد ممارسات بديلة. ولهذه الغاية، يقدّم العديد من المنظمات والنشطاء/الناشطات دعمًا مجانيًا، قمنا هنا بتضمين قائمة مرجعيّة بهم. وحتى إذا كنتِ ضمن مجموعة ناشطة صغيرة لا تمتلك إمكانيات مادية كبيرة، ما يزال بإمكانكِ العمل بنفسك من خلال الأدوات الموصى بها هنا، وإجراء بعض الأبحاث الإضافية واختبار الحلول.

وبالنسبة للمؤسسات الأكبر حجمًا، يجب أن تهدف إلى تضمين تكاليف الأمان الرقمي في الميزانية الأساسية للمنظمة وتخصيص الموارد لذلك. فكّري بالأمر كما لو أنكِ تخصّصين ميزانية للحماية القانونية أو للمنشورات. يجب أن تشمل الخطة الطويلة الأمد وجود مستشار/ة أو موظف/ة تقني/ة للدعم الشامل، بشكل مماثل لوجود محام/ية موكل/ة أو موظف/ة.

تُفضّل معظم المجموعات النسويّة التفكير في مقاربات شاملة للأمان بدلاً من عزل الأمان التقني كمسألة منفصلة. وهذه ممارسة جيّدة لأنها تتيح لك ربط العديد من جوانب الأمان معًا، لأنها غالبًا ما تكون مترابطة بالفعل.

أمثلة من سياسات الأمان الرقمي

البيانات

ما نوع البيانات التي تخزنها منظمتك؟ كيف تحفظها بأمان؟ من لديه إذن بالوصول إليها؟ لأي غرض؟ متى يتم حذفها؟ هل تستخدم المنظمة خدمة سحابية كغوغل درايف **(Google Drive)**، على سبيل المثال؟ أو هل تستخدم تخزينًا محليًا **(local storage)** كالخادم **(server)** في المكتب؟ هل لدى المنظمة نسخ احتياطية منتظمة؟ وما هي مخاطر فقدان البيانات؟

التواصل

ما المنصات التي يجب استخدامها في التواصل (البريد الإلكتروني، الهاتف المحمول، مكالمات الفيديو، إلخ)؟ ما المنصات التي يجب ألّا تستخدمها مجموعتنا أو منظمتنا على الإطلاق؟ من لديه الإذن أو حق الوصول لمحتوى الاتصالات؟ من يمكنه رؤية السجلات **(logs)**؟

كلمات المرور

ما هي القواعد الخاصة بكلمات المرور الفردية على الشبكة؟ متى على الفريق تغيير كلمات المرور؟ أين يسمح له بتخزينها؟ ما طول كلمة المرور؟ من لديه الإذن أو حق الوصول لإعادة تعيين كلمات مرور الحسابات المشتركة؟ هل يجب علينا تسجيل الخروج يوميًا؟

الأجهزة

هل توفّر منظمتكِ أجهزة كمبيوتر أو هواتف محمولة خاصة بالعمل؟ ما هي البرامج المسموح تحميلها على هذه الأجهزة؟ هل يمكن اصطحاب هذه الأجهزة عند السفر؟ وكيف نحميها من الفيروسات؟

الموقع

كيف نحافظ على أمن موقعنا الالكتروني؟ ماذا عن الأمن المالي بحال قبلنا التبرعات على الموقع؟ كيف يمكن للناس التواصل معنا بشكل آمن؟

الاستجابة للحوادث

ماذا نفعل إذا فقد شخص ما هاتفه المحمول؟ أو عندما يتم إختراق حساب ما على وسائل التواصل الاجتماعي؟ أو إذا تعرضنا لهجوم على الإنترنت؟ كيف نتصرف إذا اكتشفنا برامج ضارة تقوم بنسخ ملفاتنا؟ أو في حال وقوع حادث في المكتب أفقدنا معلومات أو أجهزة؟

أداة بناء السياسات SOAP

https://usesoap.app/

SOAP هو مولّد مجاني لسياسات الأمان الرقمي. تطرح الأداة عددًا من الأسئلة وعند الإجابة عليها، تحصلين على مسودّة أولية للسياسات الرقمية الخاصة بكِ. تشكّل هذه الأداة بداية جيدة للمجموعات. ويوفّر موقع SOAP الدعم ونصائح حول الأقسام المختلفة لضمان أنّ العملية برمّتها سهلة قدر الإمكان.

تطوير الممارسات الآمنة

لا تعني القواعد شيئًا بالطبع إن لم يتم تبنّيها وتطبيقها بشكل جماعي. تذكّري دائمًا أنّ الإنترنت مكوّن من شبكة من أجهزة الكمبيوتر وأنّ أي مجموعة تستخدم الإنترنت تُشكّل شبكة من المستخدمين/ات. يجب أن نستخدم قوّة الشبكة لصالحنا. ممّا يعني أيضًا، أنه يكفي عدم تقيّد شخص واحد في شبكتنا بالممارسة الآمنة، لكي نتعرض جميعنا للخطر.

فإذا كانت منظمتك مثلاً، تستخدم **Google Workspace** للتواصل بالبريد الإلكتروني وحفظ الملفات، يجب حماية كل حساب على **Google Workspace** بشدّة (كلمة سر قوية، مصادقة ثنائية، إلخ). يكفي ألاّ يأخذ أحد أعضاء الفريق أمنه/ا على محمل الجدّ، ليتمكّن الخصم من خرق شبكتنا والوصول إلى جميع الملفات ورسائل البريد الإلكتروني.

يتذرّع الناس بالعديد من الأعذار لإهمال الممارسات الآمنة. فقد يتكاسلون مثلاً في تسجيل الخروج من المواقع، أو في استعمال كلمة مرور طويلة، أو في تغيير كلمة المرور بشكل دوري؛ وقد يعاودون استخدام نفس كلمة المرور لمواقع عدة وغيرها من الممارسات غير الآمنة.

تتطلّب **الممارسات الآمنة** ثقافةً داعمة. إن كنّا بأغلبيتنا مثلاً نستخدم التطبيقات الآمنة، فإنّنا نشجّع بعضنا البعض على استخدامها. فكّري في إجراء تدقيقات دورية **للممارسات الآمنة**، إضافة إلى البحث عن أكثر أدوات الأمان سهولة في الاستخدام ليستمتع بها فريقك.

يشبه الأمان لعبة القطة والفأر. تحاول القطة دائمًا اتباع أساليب جديدة للإمساك بالفأر، بينما يعمل الفأر دائمًا على تطوير استراتيجيات للهروب من القطة. لا يكفي تنظيم ورشة عمل، أو استخدام أداة واحدة للاعتقاد بأننا آمنات. يجب أن يشكّل الأمان موضوعًا مستمرًا للنقاش في حركاتنا. ليست مَهمتنا أبدًا أن نكون آمنات بنسبة ١٠٠٪، وإلا فإننا لن نغادر منازلنا ولن نقوم بأيّ نشاط على الإطلاق.

هدفنا من خلال السياسات والممارسات الآمنة هو: رفع كلفة التعدي علينا. والكلفة هنا تتضمن الوقت والأموال والموارد البشرية والأجهزة. أسوأ ما يمكن فعله هو التكاسل أو التهاون بأمننا، بحيث يكون كلّ ما على خصمنا فعله هو التلصّص من فوق أكتافنا. تذكّري أنّ رياضيّات البرمجة هي من صالحنا: خطوة واحدة صغيرة (كلمة مرور إضافية مثلاً) تجبر خصمنا على استخدام خطوات أكبر بكثير (جهاز كمبيوتر باهظ الثمن) لاختراقنا.

نموذج التهديدات

تتمثّل الخطوة الأولى في التخطيط للأمان الرقمي – كفرد أو كمجموعة – في فهم المخاطر الفعلية

– ما هي مصادر المخاطر؟

– ما هي عواقب الانتهاكات؟

– ما الذي يشير إلى أنّه يتعيّن علينا الانتقال إلى خطة طوارئ أو تفعيل بروتوكول أمان؟

بدون وجود خطة، لا يمكن الاستجابة للمواقف بحكمة.

من المهم أيضًا ملاحظة نقطتين:

1

يجب مراجعة الخطط بشكل منتظم؛ يمكن أن يكون ذلك كل ثلاثة أشهر أو كل عام. تذكّري أننا في معركة مباشرة مع خصومنا. هؤلاء يطوّرون خططهم، لذا يتوجب علينا فعل الأمر عينه.

2

يجب اختبار الخطط خلال الأوقات الهادئة. عندما يكون الفريق مستعدًا لبروتوكول الطوارئ، من المحتمل أن يتعامل معه بهدوء وأن يستجيب بشكل أفضل. لا تنتظري حدوث خرق أمني لاختبار الخطة. قومي بإنشاء حالة طوارئ وهمية واختبري مدى استعداد الفريق. هذه هي أفضل طريقة للتعلّم وتعديل الخطط وتخصيص الموارد المناسبة.

من بين الأمثلة الجيّدة لتمارين نموذج التهديدات، تلك التابعة لمؤسسة EFF. المزيد هنا:

https://ssd.eff.org/en/module/your-security-plan

يمكن البدء في نموذج التهديدات من خلال الإجابة عن الأسئلة الخمسة التالية:

ماذا أريد أن أحمي؟

ممّن أريد الاحتماء؟

ما مدى تداعيات فشل الحماية؟

ما هي النسبة الواقعية لاحتمال الاختراق؟

ما مدى التزامي الفعلي بالخطوات الآمنة مقابل العواقب المحتملة؟

لنتفحّص كلّ سؤال على حدة:

ماذا أريد أن أحمي؟

قومي بوضع قائمة بجميع الممتلكات والأصول المتعلّقة بالتكنولوجيا. قد تكون هذه برامج أو أجهزة أو ملفات أو رسائل بريد إلكترونية أو هواتف محمولة أو كاميرات. قد تشكّل قاعدة بيانات ما، إحدى الممتلكات المُهمّة. فإذا كنت تعملين مع ناجيات من العنف مثلاً، تشكّل المعلومات المحفوظة في ملف إكسل **(excel sheet)** المتعلّقة بهنّ، إحدى الممتلكات الالكترونية القيّمة للغاية. ومثلها أمثلة كثيرة: قائمة المعارف؛ رسائل البريد الإلكتروني الخاصة؛ حسابات وسائل التواصل الاجتماعي؛ أجهزة الكمبيوتر المحمولة وأجهزة الشحن والهواتف المحمولة وما إلى ذلك؛ ألبومات الصور– فربما تقومين بجمع أدلّة على انتهاكات لحقوق الإنسان ولديك أدلّة فوتوغرافية؛ ربما كان لديك نسخ من شهادات أو تقارير تريدين استخدامها في قضية قضائية ما.

هذه مجرّد عيّنة من الأمثلة الكثيرة عن الممتلكات التي يجب حصرها. قومي بجدولتها: ما هي؟ أين يتم حفظها؟ من يمكنه الوصول إليها ولماذا؟ وبمجرّد حصر الممتلكات وتنظيم هذه المعلومات، يمكن إلقاء نظرة شاملة والبدء في التخطيط لكيفيّة حمايتها.

* تذكير: حدّثي قائمة الممتلكات بانتظام! قومي بوضع تنبيه شهري أو ربع سنوي لتحديث القائمة بأي بيانات أو معدّات جديدة.

ممّن أريد الاحتماء؟

الآن، بالنظر إلى كل من الممتلكات على حدة، ابدأي في تحديد ممّن تريدين حمايتها؛ من/ما هو مصدر الخطر الذي قد يرغب في اختراق الأجهزة أو الاطّلاع على الحسابات؟ إذا كنت تقومين بتوثيق انتهاكات الدولة مثلاً، قد تحاول السلطات الوصول إلى ملفاتك. وإذا كان هناك مصدر معيّن يحاول تشويه سمعتك، قد يرغب في «زرع» معلومات ضارة على أجهزتك. وقد يحاول لص التطفّل على أموالك لمحاولة سرقتك. وربما يحاول مديرك قراءة رسائل البريد الإلكترونية الخاصة بك. وقد يحاول شريكك السابق قراءة الرسائل على هاتفك المحمول... أو ربما يحاول جيش إلكتروني سرقة حسابك على تويتر.

فهم مصدر التهديد يساعدنا في إزالة الغموض عن خصومنا وقدراتهم، وعلى وضع خطط أفضل لحماية أنفسنا.

* تذكير: نعي كنسويّات أنّ العنف القائم على النوع الاجتماعي يحدث غالبًا في أكثر دوائرنا حميمية. لذا، نحن نعلم أنّ مصادر التهديد يمكن أن تشمل دائمًا الشركاء الحميمين وأفراد الأسرة والجيران وما إلى ذلك.

* تذكير: بالنسبة للنسويّات، غالباً ما يتم استخدام حياتنا الشخصيّة وأنماط حياتنا كمادة لتشويه سمعتنا. لذا، حتى وإن كان لديكِ أجهزة منفصلة للأمور الشخصية والمهنية، تظلّ أجهزتك الشخصيّة بحاجة إلى الحماية. فقد يقوم الخصوم بتسريب الصور الشخصيّة أو سجلات الدردشة لتشويهك أو «فضحك». لذا تأكدي من التفكير في هذا البعد الجندري الإضافي عند قيامك بنموذج التهديدات

ما مدى تداعيات فشل الحماية؟

يرتبط هذا السؤال ارتباطًا وثيقًا بالسؤال الأخير: ما الذي أنا مستعدة لفعله؟ من المهم للمجموعة تحديد عواقب اختراق الأمان. هل سلامة شخص ما مرتبطة بشكل مباشر بحماية بياناته؟ مثلاً، إن كنتِ تعملين مع أشخاص كويريين/ات في سياقات شديدة الصعوبة، فقد تشكّل خطة الأمان السيئة تهديدًا مباشرًا لحياة شخص ما؛ وإن كنتِ تخططين لاعتصام أو مسيرة في سياق سلطويّ، قد تقوم قوات الأمن التي تخرق اتصالاتكِ، باعتقال وسجن المنظمين/ات.

بالنسبة للبيانات الأخرى الأقل أهميّة، قد تقتصر العواقب على الإحراج أو الخسارة المالية الطفيفة؛ من المهم جداً تحديد هذه الفروقات في العواقب.

ما هي النسبة الواقعية لاحتمال الاختراق؟

من المهم التمييز بين ما قد يحدث وبين احتمال حدوثه. يقوم احتساب المخاطر على تقدير احتماليتها بناءً على المعرفة والخبرة. ففي اللحظة التي نخرج فيها من الباب كل يوم، نبدأ في مواجهة المخاطر، إلاّ أننا لا نعالج ذلك بالبقاء في المنزل... بل نتخذ خطوات مدروسة لتخفيف المخاطر وتقليلها.

تتفاوت احتمالية المخاطر بالطبع، وفق العديد من العوامل. إذا كانت المجموعة تعمل حاليًا تحت الرادار، فقد تقلّ احتمالية أن يعرف خصومك بأنشطتكِ. أما إن كانت مجموعتكِ طرفًا في سجال إعلامي وطني حول قضية «مثيرة للجدل» (قضيّة عنف قائم على النوع الاجتماعي أثارت ضجة مثلاً) وكانت الأضواء مسلّطة عليكِ، فهنالك احتمال أكبر أن يحاول خصومكِ مهاجمتكِ.

* تذكير: لا تنسي المخاطر الخاصة بالسياق – قد تكون هذه الأمور تافهة لدرجة أنك تنسين تضمينها. فإذا كنت تعيشين مثلاً في مدينة تعاني من انقطاع يوميّ في التيار الكهربائي، فأنتِ بحاجة إلى تحديد المخاطر ذات الصلة بانقطاع التيار الكهربائي.

* نصيحة: قومي بتطوير نظام خاص من الأحمر والبرتقالي والأصفر للاتفاق الجماعي على احتمالية وقوع هجمات خلال أوقات معيّنة. ضعي بروتوكولًا لرفع مستوى استعداد الفريق في الأوقات الصعبة.

ما مدى التزامي الفعلي بالخطوات الآمنة مقابل العواقب المحتملة؟

هذا هو السؤال الأخير الذي تحتاجين إلى الإجابة عنه بأقصى درجات الصدق. في كثير من الأحيان، عندما نحضر ورشة عمل حول الأمان الرقمي، نشعر بالحماس الشديد لاستخدام أدوات معقّدة. لكن بالعودة إلى مكاتبنا، نشعر بالملل أو الكسل وينتهي بنا المطاف بعدم استخدام أي شيء. إنّ الالتزام بحد أدنى من الجهد الذي تثقين بالقدرة على بذله، أهمّ من التخطيط لجهود قصوى لن يتمّ اتّباعها.

وكما ذكرنا سابقًا، يرتبط هذا السؤال ارتباطًا وثيقًا بتداعيات الخروقات الأمنية. فإذا كنتِ ترين أنّ العواقب ملحّة للغاية، ستحتاجين إلى إضافة بضع دقائق إلى ممارسات تسجيل الدخول/ الخروج اليومية؛ أو قد ترغبين في إضافة بضعة آلاف من الدولارات إلى ميزانية أمان منظمتكِ لشراء أجهزة أفضل أو أنظمة حماية أكثر قوّة. معًا، يجب تحديد كم الوقت والتكلفة والعناء الذي ترغبون في بذله لضمان أمان الشبكة.

* تذكير: كل خطوة إضافية نحو الأمان، تضاهي ألف خطوة يحتاج القراصنة إلى اتخاذها في خطة هجومهم. يعدّ الفارق بين كلمة السر المكونة من ٨ أحرف وكلمة السر المكونة من ٢٤ حرفًا مجرد ثوانٍ بالنسبة لك، ولكنه يعني استنزاف المزيد من الموارد والوقت للخصم.

المبادئ الشاملة للأمان الرقمي

إتقان استعمال الأدوات الآمنة أمر مهم بالطبع. لكن الأدوات الموصى بها للأمان الرقمي دائمة التغيّر. قد يكون ذلك بسبب توقّف الفريق المبرمج عن تطوير الأداة، وعدم القيام بتدعيم نقاط ضعفها؛ أو تم شراؤها من قبل حكومة أو شركة (مثل تليغرام **(Telegram**؛ أو تم إحداث تغيير في سياستها **(**مثل واتساب **Whatsapp)**؛ بالفعل، كل أداة أو خدمة، لها معجبيها ومنتقديها. إذن، ما السبيل إلى معرفة الأداة التي يجب استخدامها؟ ولأي غرض؟

إليك مبدأين شاملين مهمّين للمساعدة على اختيار الأدوات التقنية الأنسب لك:

١. اختاري برنامجًا مفتوح المصدر:

تتمّ كتابة جميع البرامج باستخدام لغة برمجة تحدّد للشيفرة أو الكود **(code)** ما يجب فعله وكيفيّة التفاعل مع المستخدم/ة. تتّبع تفاعلاتنا مع البرنامج المنطق نفسه: نُدخل مُدخلاً ما (مثلاً، نسأل الآلة الحاسبة: ١ + ١ = ؟) يعالج البرنامج هذا الطلب (يتحقق من الإجابة في قاعدة البيانات المشفّرة الخاصة به) ويوفّر المُخرج (الإجابة على الشاشة «٢»).

كيف يمكننا معرفة ما إذا كان البرنامج فعلاً يقوم فقط بالمعالجة التي يعرضها لنا ولا يقوم مثلاً، بتفعيل الميكروفون أو الكاميرا سراً؟

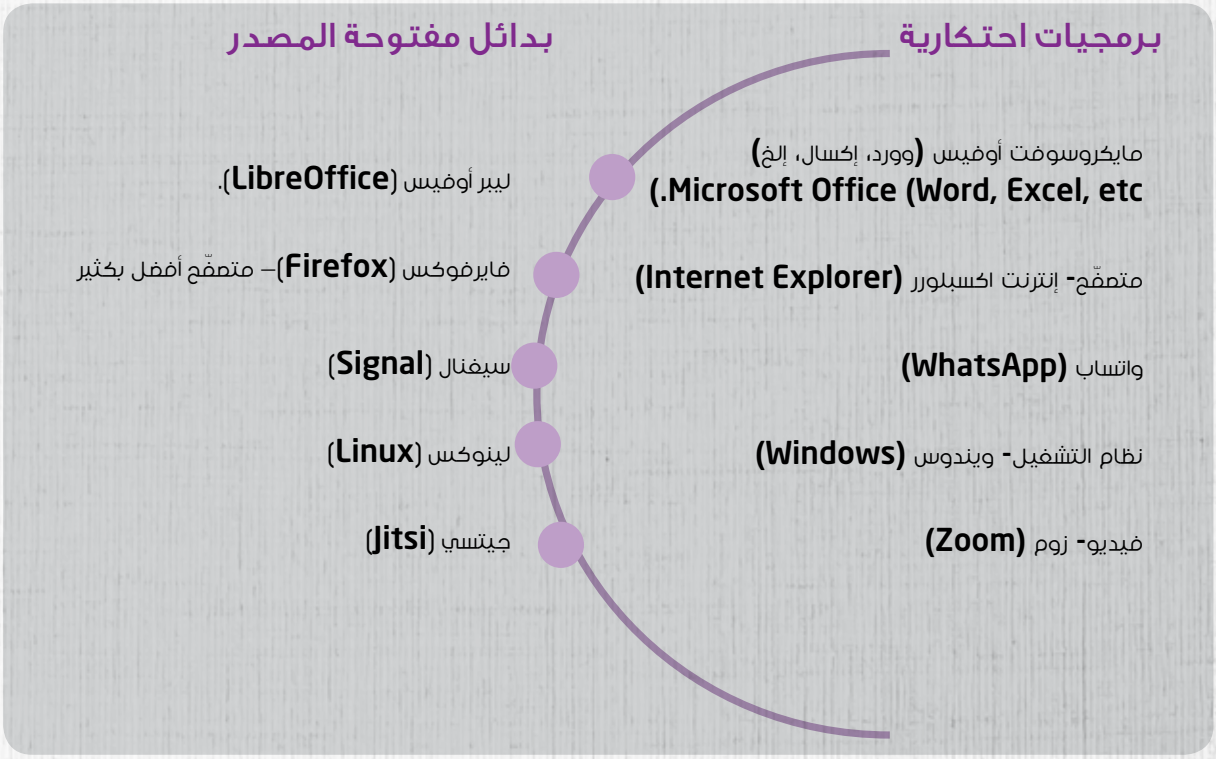
الطريقة الوحيدة لمعرفة ما يفعله البرنامج على وجه اليقين هي من خلال الاطلاع على الكود أو البرمجة **(source code)**، أي «وصفة» البرنامج الأصليّة. إن كان المصدر مُقفل، نسمي ذلك مصدرًا مغلقًا أو، كما هو الحال غالبًا: برمجيات احتكارية. هذا يعني أنه محميّ بحقوق الطبع والنشر و/أو مغلق؛ لا يسمح لنا برؤيته؛ لا يمكننا تغييره أو نسخ أجزاء منه؛ ولا يمكننا التحقّق بنسبة ١٠٠٪ من قيامه بما يقول أنه يقوم به؛ علينا في هذه الحال، أن نثق في المبرمج/ة أو الشركة؛ مع أنّ الأمر يمكن أن يعرّضنا لضرر ومخاطر كبيرة.

في المقابل، مع برامج مفتوحة المصدر، تتم مشاركة الكود بشكل علني وشفاف. في كثير من الأحيان، يُسمح للمبرمجين/ات الآخرين/ات تعديله لإنشاء كود جديد ووظائف إضافيّة **(add-ons)** أو تعديلات. إمكانية رؤية الكود يسمح لنا بالوثوق به. لذلك، فإنّ البرامج مفتوحة المصدر هي خيارات بديلة موصى بها دائماً.

منذ الأيام الأولى للبرمجة، عمد الأشخاص الذين/اللواتي يؤمنون بحريّة وإتاحة الكود، خدمةً للصالح العام، ولتوفير الأمان والثقة أيضاً، إلى تنظيم أنفسهم/ن في إطار حركة البرمجيات الحرّة والمفتوحة المصدر.

سوف تدرك النسويّات المناهضات للرأسمالية إمكانات البرمجيات الحرّة والمفتوحة المصدر كمشروع تحرّري، بخاصة أنّ البرمجيات تصبح أكثر فأكثر وسيلةً لتنظيم العمل وللإنتاج أيضاً. لاتقلقي بشأن قراءة لغة الكود بنفسك. فهناك مئات الآلاف من ناشطي/ات البرمجيات الحرّة والمفتوحة المصدر حول العالم ممّن يقومون/يقمن دائمًا بالتحقق من الكود وإبقائنا على اطلاع دائم.

إنّ كونك مثلاً غير متخصصة بالهندسة، وغير قادرة على بناء جسر بنفسك، لا يعني بتاتًا أنه لا يمكنك تكوين رأي حول سياسة وتصميم الجسور لإفادة المجتمع والصالح العام.



٢. تشفير كلّ شيء

لقد استخدمت التشفير طوال حياتك، غالبًا في شكل كلمات مرور. لكن حتى كطفلة في المدرسة، ربّما قمت بتمرير قصاصة ورقية إلى زميلتك في الصف. ومن الأرجح أن تكوني قد كتبتها بطريقة مشفّرة لكي لا تتمكّن المعلّمة من فهمها متى اعترضت الرسالة. هذا هو أساس التشفير: نتفق أنا وإنت على مفتاح سرّي لنفهم بعضنا البعض من دون أن يفهم الآخرون ما نتحدث عنه.

في بعض الأحيان، قد يكون من السهل على شخص ما تخمين المفتاح. قد يستغرقه الأمر بضع ثوانٍ أو بضع ساعات. يمكنه/ا التخمين عن طريق التجربة والخطأ أو من خلال استراتيجية أكثر ذكاءً. لقد لعبنا جميعًا مثل هذه الألعاب الذهنية كأطفال، محاولين فك كود رسالة سرية.

الآن، استبدلي العقل البشري (ومحدوديته) بكمبيوتر فائق السرعة يمكنه التخمين بشكل أسرع بمليار مرة من العقل البشري.

وإذا كانت كلمة المرور عبارة عن كلمة كاملة من القاموس الانكليزي، مثلاً، يستطيع الكمبيوتر السريع ايجادها في بضع دقائق فقط. كما وبإمكان برنامج الاختراق المتطور تجربة كل عنوان كتاب وكل عنوان أغنية وكل اسم مشهور وكل اسم بلدة أو قرية أو موقع على وجه الأرض، في غضون ساعات قليلة فقط. مهمّتك الآن هي أن تكوني أكثر ذكاءً من هذا الكمبيوتر.

غنيّ عن القول، أنك بحاجة إلى استراتيجية كلمات مرور ذكية للحفاظ على أمان الحسابات والأجهزة. فوضع سياسة لكلمة المرور لمجموعة / تنظيم / شبكة يساعد على توحيد المعايير. من المهم أيضًا فهم المبادئ الأساسية لكلمات المرور، لكي تعرفي لماذا عليك استخدام المصادقة الثنائية مثلاً، وليس فقط وجوب استخدامها.

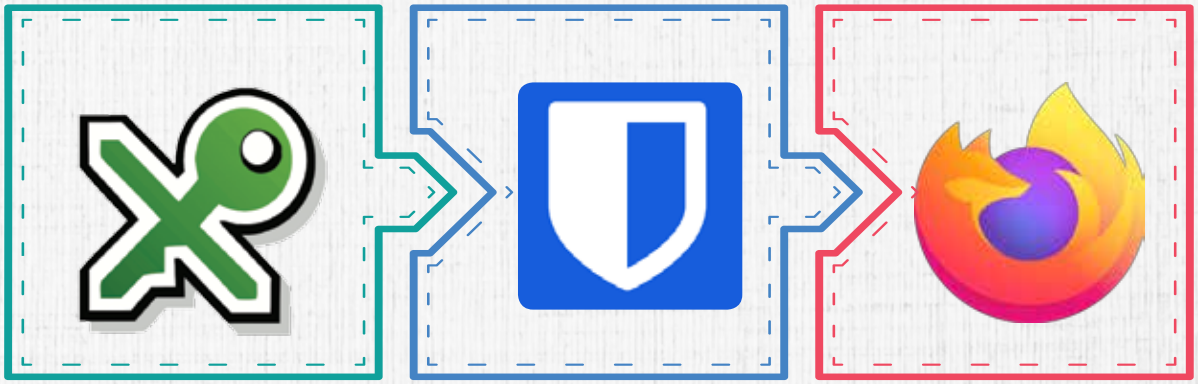
عبارات مرور، لا كلمات مرور

«عبارة المرور» هي طريقة ذكية لنتذكّر أنّ طول كلمة المرور هو الميزة الأهم. يجب عدم التضحية بتاتًا بطول كلمة المرور. تجبرك معظم الخدمات على استخدام أشكال خاصة مثل ٪ $ #! بالإضافة إلى الأرقام (١، ٢، ٣...) والأحرف الكبيرة، ولكنها تسمح بـ ٨ أحرف لكلمة كحد أدنى. هذه ليست ممارسة ذكية. استهدفي كلمات مرور مكوّنة من ١٦ حرفًا أو أكثر. استهدفي جمل طويلة. ونظرًا لأننا نتحدث باللغة العربية، من المفيد استخدام عبارات عربية كونها غير متوفّرة في قاموس اللغة الإنجليزية.

إدارة كلمات المرور

هناك برامج تعمل كخزنة لكلمات المرور ممكن أن تكون مفيدة جدًا إن كنتِ ترغبين في اعتماد عبارات مرور قويّة ومعقّدة. إنّ ذلك يحلّ مشكلة تذكّر العديد من كلمات المرور الطويلة. من المهم جدا عدم القيام باستخدام كلمة مرور موحّدة للحسابات المتعدّدة؛ فإن تمّ اختراق أحدها، ستكون جميع الحسابات الأخرى مهدّدة بالاختراق أيضاً.

يحلّ هذه البرامج مشكلة الذاكرة هذه عن طريق مطالبتكِ بتذكّر كلمة مرور طويلة واحدة. يتيح ذلك إمكانية فتح «خزنة» تحوي جميع كلمات المرور الطويلة للحسابات الأخرى المحفوظة؛ من ثمّ يمكن نسخ كلمات المرور المناسبة ولصقها في المتصفّح.



https://www.mozilla.org/en-US/firefox/

أضاف **FireFox**

كلمة مرور رئيسية أو أساسية إلى إعدادات متصفحه. يمكن استخدامه لتخزين كلمات المرور في **FireFox** بشكل أكثر أمانًا.

https://bitwarden.com/

BitWardn

هو برنامج جديد لإدارة كلمات المرور وهو يكتسب شعبية.

https://www.keepassx.org/

KeePassX

هو برنامج شهير لتخزين كلمات المرور يمكن تشغيله أيضًا من محرك أقراص خارجية مثل الـ**USB**.

ممارسة التواصل الآمن عبر الإنترنت

الحماية من الفيروسات

يعتمد أمان جهازك، بشكل أساسي، على عمل البرنامج بالطريقة التي ترغبين بها. وهذا هو سبب قلقنا من الفيروسات. إذ ما إن تتمكّن برمجيّات خبيثة **(malware)** من اختراق الجهاز، حتى تهدّد كلّ شيء، بصرف النظر عن إجراءات الأمان الأخرى. كلّ الأجهزة معرّضة لخطر البرمجيات الخبيثة وإن بدرجات متفاوتة؛ وبخاصة، أجهزة الكمبيوتر التي تعمل بنظام **Windows**.

يوفّر **Security-in-a-Box** موردًا رائعًا، يفصّل الحماية ضد البرمجيّات الخبيثة، يمكنك الاطّلاع عليه من خلال الرابط التالي:

https://securityinabox.org/en/guide/malware/

كمدرّبة / ميسّرة، بشكل عام، يجب أن تبقي على اطّلاع دائم بممارسات البرمجيّات الخبيثة وحيلها الجديدة. ولمعرفة كيفيّة التعامل مع هذه البرمجيّات، يوصي خبراء الأمان بالتالي:

١. تثقيف المستخدمين/ات حول كيفيّة عمل البرمجيّات الخبيثة.

٢. دعم المستخدمين/ات في استخدام برامج مكافحة الفيروسات وتحديث أدوات الأمان.

٣. تعليم المستخدمين/ات كيفيّة التخلّص من التهديدات عند العثور عليها.

٤. تشجيع المستخدمين/ات على الانتقال إلى أدوات أكثر أمانًا وأقلّ خطورة، متى توفّر ذلك.

فهم البرمجيات الخبيثة

البرمجيّات الخبيثة هي المصطلح العام الذي يشمل الفيروسات وبرامج التجسّس والديدان (worms) وأحصنة طروادة (Trojans). يمكنك شرحها بأنّها كود (code) يتسلّل إلى جهازك من أجل إلحاق ضررٍ ما. قد يكون في بعض الأحيان، جزءًا من عمليّة احتيال كبيرة، كسرقة معلومات بطاقة ائتمانية أو كلمات المرور. ويكون في أحيان أخرى، لهذه البرمجيّات دوافع أقلّ خطورة، كتخويف المستخدمين/ات، أو إظهار مهارات القرصنة. يمكن للحكومات استخدام البرمجيات الخبيثة الموجَّهة، للتجسّس على المواطنين/ات مثلاً. ويمكن للّصوص نشر البرمجيّات الخبيثة لإقناعك مثلاً، بتحويل الأموال تحت ذرائع كاذبة. كما يمكن لشركات الكمبيوتر، أيضًا، نشر البرمجيّات الخبيثة لإقناعك بإجراء عمليات شراء معيّنة.

تنتشر البرمجيّات الخبيثة عبر الإنترنت من خلال رسائل البريد الإلكتروني أو عمليات التحميل (downloads). إحدى الطرق الشائعة هي التصيّد الاحتيالي، حين يحاول أحد القراصنة خداعك للقيام بتثبيت برمجيّات خبيثة بنفسك باستخدام الخداع والنفاق.

تجنّب البرمجيّات الخبيثة

باعتماد ممارسات أمان جيّدة، يمكن اتخاذ خطوات وقائية للحماية من البرمجيّات الخبيثة. في ما يلي، بعض النصائح:

- حدّثي نظام التشغيل (Windows،Mac، Android، iOS) بشكلٍ مستمر. تحاول هذه الشركات حماية برامجها من البرمجيّات الخبيثة المعروفة. لذا، فإن النظام المحدّث، سيستفيد حكمًا من تحديثات الشركة. تجنّبي استخدام نظم تشغيل «كراك» لأنه يجعلك عرضة للبرمجيّات الخبيثة.
- حدّدي يومًا كلّ بضعة أشهر لتنظيف جهازك. قومي بإلغاء البرامج التي لم تعودي تستخدميها. واعملي على تحديث أكثر البرامج استخدامًا، مثل المتصفّح أو تطبيق البريد الإلكتروني. وقومي بتحديث تطبيقات الهاتف المحمول أو ببرمجتها على التحديث التلقائي.
- كوني حذرةً دائمًا من تحميل البرامج من المواقع غير الرسمية. فهذه طريقة شائعة يحاول القراصنة خداعك بها. تحقّقي دائماً من عنوان الـ URL الذي تقومين بالتحميل منه، وتجنّبي استخدام مواقع طرف ثالث. وإن راودك شكٌّ ما، لا تقومي بتحميل المادة. ينطبق الأمر نفسه على مرفقات البريد الإلكتروني والروابط المرسلة إليك عبر الرسائل. فإن بدت مريبةً، لا تقومي بفتحها. ينطبق الأمر نفسه أيضًا على الـ (USB)، أو الأقراص الصلبة (hard-drives)، التي أصبحت أقل شيوعًا إلاّ أنّها قد تحتوي أيضًا على محتوى خبيث.

- يمكن أن تخفي عناوين الـ **(shortened URL)** المختصرة خلفها روابط خبيثة، يصعب الحكم عليها بمجرّد النظر إليها. إن كنتِ تشكّين في أحد العناوين المختصرة، استخدمي

/https://www.checkshorturl.com
لتبيان مضمونه.

برامج مكافحة الفيروسات

يمكنك بذل أقصى جهدك للحماية من البرمجيّات الخبيثة، لكن ما تزال هنالك حاجة إلى استمرار تفعيل برنامج مكافحة الفيروسات وفحص الجهاز بانتظام. لا يوجد حاليًا برنامج مفتوح المصدر، موصى به، لمكافحة الفيروسات.

إن كنتِ تستخدمين **Windows**، فإنّ آلية الحماية المُضمّنة فيه، **(Windows Defender)**، تُعدّ خيارًا جيدًا عند تحديثه. في ما يلي بعض الخيارات لبرامج أخرى، **يمكنكِ استكشافها:**

AVIRA https://www.avira.com

AVG /https://www.avg.com

AVAST https://www.avast.com

Malware Bytes https://www.malwarebytes.com

التعافي من الفيروسات

أثناء الاستخدام اليومي، يمكن ملاحظة علامات تشير إلى احتمال إصابة الجهاز بفيروس. هل تباطأ فجأة؟ هل تتصرّف البرامج بطرق غريبة؟ هل تظهر نوافذ غريبة؟ إن تملّكتك شكوك، قومي على الفور بإجراء مسحٍ لمكافحة الفيروسات. اقطعي الاتصال بشبكة الإنترنت. سيتولّى برنامج مكافحة الفيروسات، غالبًا، معالجة المشكلة. يمكنك أيضًا إعادة الجهاز إلى إعدادات المصنع لمسح جميع المعلومات منه (لا تنسي نسخ الملفات المهمّة أولاً). إن كنت بحاجة إلى المزيد من المساعدة، قومي بالتواصل مع خبير/ة أو مع خط ساخن.

التصفّح الآمن

يعدّ التصفّح طريقة شائعة جدّا للإصابة بالبرمجيّات الخبيثة. غالبًا ما يستخدم القراصنة المواقع الالكترونيّة المزيّفة أو مواقع التصيّد الاحتيالي، لإدخال برمجة خبيثة في المتصفّح أو الجهاز. لذا، فإنّ تأمين المتصفّح وتطوير ممارسات آمنة، أمران شديدا الأهميّة.

نوصي باستخدام **Mozilla Firefox** للتصفّح الإلكتروني اليومي لأنّه مجانيّ ومفتوح المصدر ومزوّد بإضافات ممتازة للمساعدة في زيادة الخصوصية والأمان. وعند التدريب حول التصفّح الآمن، من الجيّد القيام بتمرين عمليّ حول تحميل **Firefox** واستبدال جميع المتصفّحات الأخرى به.

* تذكير: ينطبق هذا أيضًا على الهاتف المحمول! قومي بتحميل تطبيق Firefox للمحمول، لنظامَي Android أو iOS واستخدميه لتصفّح أكثر أمانًا من خلال الهاتف المحمول.

قومي بتحميل أحدث إصدار من **Firefox** من خلال الموقع الرسمي

https://www.mozilla.org

أثناء وجودك على موقع **Mozilla Foundation**، تفقّدي الأدوات الأخرى المفيدة للخصوصية والأمان، التي تمّ تطويرها.

من الجيّد أن تظلّي كمدرّبة على اطلاع دائم بأحدث الإضافات التوسعيّة **(Plug-ins)** والوظائف الإضافيّة **(Add-ons)** الخاصة بالأمان. وكبداية، إليكِ اثنتان من الإضافات الموصى بهما:

HTTPS Everywhere

(https://www.eff.org/https-everywhere)

Privacy Badger

(https://www.eff.org/privacybadger)

* نصيحة: إن كنتِ تشكّين في موقع ما للتصيّد الاحتيالي، يمكنكِ استخدام هذه الأداة: https://www.phishtank.com/ للتحقّق ممّا إذا كان موقعًا خبيثًا يحاول سرقة المعلومات أو تحميل فيروس مثلاً.

يمكن تصميم تدريب حول استخدام **Firefox** يتضمّن التالي:

١. التحميل على أجهزة الكمبيوتر والتلفون المحمولة

٢. استبدال خدمات تبويب (**Bookmarks**) المتصفحات الأخرى وحذفها

٣. تثبيت الإضافتين الموصى بهما أعلاه (وغيرها إن كان الوقت يسمح)

٤. ضبط إعدادات الخصوصيّة

٥. تعيين محرّك البحث الافتراضي

محركات بحث تحمي الخصوصيّة

يوصي الخبراء باستخدام **DuckDuckGo** كمحرّك بحث افتراضي لأنه لا يتتبّع مستخدميه أو يبيع بيانات البحث الخاصة بهم/ن بالطريقة التي تعمل بها معظم محركات البحث التجارية (مثل **Google** أو **Bing**).

إعدادات الخصوصيّة والأمان

تقدم إعدادات **Firefox** عددًا من الخطوات لزيادة الخصوصيّة أثناء استخدام المتصفّح. تذكري أن تبقي على اطلاع دائم بأي تغييرات تطرأ على الإعدادات الجديدة أو القديمة! يمكن للمشاركات تفعيل ميّزات للحدّ من التتبّع من خلال المواقع التي تجمع (ثم تبيع) البيانات وتراقب السلوك على أنظمتها. تسمّى هذه الميزة «عدم التعقب» وهي مفيدة بالرغم من أنّ الشركات ما تزال تجد طُرقًا لتجاهلها.

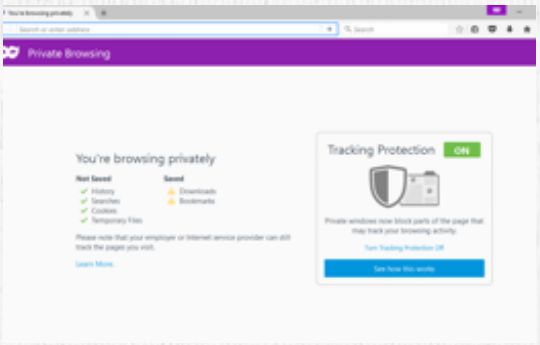
يتوفّر للمستخدمين/ات أيضًا اختيار مدى حفظ سجلّ التصفح. يمكن تغيير ذلك في الإعدادات، بالإضافة إلى الخيارات المتعلّقة بنظام تحديد المواقع. من الجيّد مرافقة المشاركات في الورشة في كلّ خيار، ومطالبتهن بإجراء تغييرات فوريّة أو التفكير بها والعودة إليهن لاحقًا.

ينطبق الأمر نفسه على اتخاذ القرارات بشأن إعدادات الأمان. نوصي بتحديد المربّعات التي تمكّن **Firefox** من تحذيرك عندما تحاول مواقع معيّنة، تثبيت وظائف إضافية، أو متى تُعرف بأنّها مواقع خبيثة أو مشبوهة.

ربما تَسأل المشاركات أيضًا عن موضوع حفظ عمليّات تسجيل الدخول في المتصفّح. يكمن الخيار الأكثر أمانًا، بالطبع، في عدم حفظ أي عمليات تسجيل دخول. إلاّ أنكِ قد ترغبين في عمل استثناءات لبعض المواقع الأقلّ استخدامًا. في هذه الحالة، نوصي باستخدام «خزنة» كلمات المرور المُدمجة في **Firefox** والذي تطلب منكِ كلمة مرور رئيسية، لكي تتمكني من رؤية عمليّات تسجيل الدخول المحفوظة. هذا مهمّ جدًا، إذ لا يستغرق فتح تسجيلات الدخول المحفوظة سوى بضعة ثوان، في حال كنتِ قد غادرتِ الغرفة لبضع دقائق، بعد فتح اللابتوب.

وضع التصفّح الخاص

يعدّ التصفّح الخاص، طريقة جيّدة لمنع **Firefox** (أو أي متصفّح آخر) من تخزين البيانات حول عمليّة تصفّحك، مثل عنوان الـ **URL** الذي قمتِ بزيارته. مع ذلك، فهو لا يمنع الموقع نفسه من تتبّع سلوكك. لمعرفة متقدّمة حول المجهوليّة الإكترونيّة، راجعي الصفحة التالية لمتصفّح **TOR**.



وظائف Firefox الإضافيّة (add-ons)

الوظيفة الإضافية لـ**Firefox** هي برنامج يضيف ميزات جديدة في شكل إضافات توسعيّة وملحقات. إليكِ توصيتان لاستخدامهما في التدريبات:

HTTPS Everywhere

HTTPS Everywhere هي وظيفة إضافية تساعد **Firefox** على الاتصال الآمن بمواقع داعمة للتشفير. اعملي على التأكّد من أنكِ تستخدمين دائمًا اتصال **HTTPS** بدلاً من **HTTP** (الأقل أمانًا). إن لم يكن لديك **S** في النهاية، يعني ذلك أنّ اتصالك بالموقع غير مشفّر، وأنّ المعلومات التي ترسلينها وتتلقّينها من الموقع، يمكن تتبّعها بواسطة مزوّد خدمة الإنترنت أو أجهزة المراقبة.

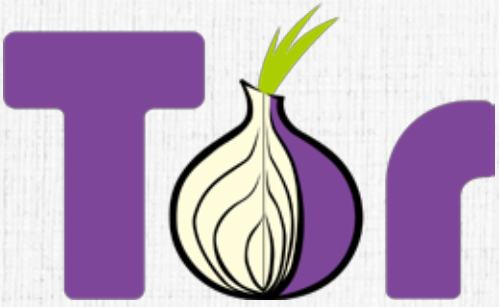
Privacy Badger

Privacy Badger هي وظيفة إضافية للمتصفّح، تمنع الشركات الخارجية من تتبّع الأنشطة عبر الإنترنت. وهو متاح لمتصفّحات **Firefox** و**Tor** و**Chrome.** بمجرّد أن تعلمي مدى التتبّع الذي يتم على خلفيّة زيارة بسيطة لموقع ما، سترغبين في تفعيل هذا الخيار.

تذكير: قومي دائما بتحديث الوظائف الإضافية والمتصفّح. ضعي تذكيرات منتظمة لحذف الوظائف الإضافية غير المستخدمة، كل بضعة أشهر، لتجنّب أي ثغرات أمنيّة.

متصفّح TOR

لتصفّح ذو خصوصيّة متقدمة، يمكنك تحميل واستخدام متصفّح **TOR**، وهو مشروع مصمّم لحماية مستخدمي/ات الإنترنت من المراقبة والتتبّع. يقوم **TOR** بترحيل وتشفير الاتصال بمواقع إلكترونية– أثناء التصفّح– من خلال نقاط مختلفة في شبكة **TOR**. لذا، لا يمكن للمتعقّبين معرفة بياناتك الفعليّة. ستظهرين كمستخدمة إنترنت عشوائية، في موقع عشوائي. إن قامت الحكومة أو مزوّد خدمة الإنترنت مثلاً، بحظر مواقع إلكترونيّة معيّنة لجميع «الأي بي» **(IPs)** في مصر، على سبيل المثال، فإنّ **TOR** سينقلك عبر عنوان «أي بي» في أستراليا (عشوائي)، ممّا سيمكّنك من الوصول إلى هذه المواقع. تتم صيانة شبكة **TOR** بواسطة آلاف الخوادم التي يديرها متطوعون/ات حول العالم.



يُعدّ متصفّح **TOR** أيضًا، طريقة رائعة لضمان مستوى إضافي من الحماية للمجهوليّة. إن كنتِ تقومين بنشر محتوى حساسًا عبر الإنترنت، يمكنك تسجيل الدخول إلى حساباتك المجهولة عبر **TOR**، للتأكّد من التمتّع بخصوصية على المتصفّح.

القسم الثالث:
العنف على الإنترنت

العنف ضد النساء بواسطة التكنولوجيا هو مظهر حديث من مظاهر كراهية النساء التي تواجهها النسويّات كلّ يوم. لكنه أيضًا نتاج مألوف للمعايير الأبويّة. لا تحتاج النساء لأكثر من التعبير عن رأي على الإنترنت ليتم قذفهن بهجمات ذات طابع جندري وجنسي. وأكثر ما يبرز هذا الأمر، عندما تتحدث النساء عن قضايا نسويّة أو يفضحن متحرشين أو يتحدين السلطة. يمكننا أن نرسم أوجه تشابه قويّة بين الفضاءات المتصلة بالإنترنت وغير المتصلة به- بين العامة والخاصة- في كيفيّة إدامة كراهية النساء.

حلّلت النسويّات، لقرون عدة، كيف أن التصميم الذكوري للأماكن العامة يجعل الشوارع والساحات غير آمنة للنساء. لقد فعلن الشيء نفسه في المجالات الخاصة مثل المنازل والمدارس وأماكن العمل، متسائلات دومًا: من يتحكّم بالتصميم؟ ومن يضع قوانين هذه المساحات التي تسمح بالعنف ضد النساء – لا بل تسهّله؟ ويصحّ الأمر نفسه على الإنترنت. سواءٌ كانت النساء مرئيات بشكل كبير، أو مجهولات الهوية تمامًا، فهنّ يختبرن يوميًا العنف الذكوري.

نقاط هامّة للتذكّر

إنّ العنف على الإنترنت الذي يستهدف النساء أو الأقليات حقيقي ومرعب.

حتى أوائل عام ٢٠١٠، كان الكثير من الناس يجادلون بالقول بأنّه نظرًا لكونه عنفاً «افتراضيّاً»، فهو ليس مقلقاً مثل العنف «الواقعي.» لحسن الحظ، تم دحض هذه الفكرة مرارًا وتكرارًا، ولكن على حساب النساء اللواتي اضطررن لتحمّل حملات تشويه مروّعة، وتهديدات على المنصات العامة أو الخاصة. عند تيسير ورشة عمل حول هذا الموضوع، من المهم أن تأخذي ذلك بعين الاعتبار.

يمكن أن يكون للعنف ضد النساء على الإنترنت تأثير الصدمة.

قد يجادل بعض الناس بأنّ العنف على الإنترنت أمر شائع جدًا، ولا ينبغي أن تكون له تبعات مدمّرة. يزعمون أنّه من الطبيعي أن تتلقّى النساء رسائل مهينة، أو محتوى جنسي غير مرغوب فيه. إلاّ أنّه لمجرد كونه منتشراً، لا يعني أنّه لا يسبب صدمة أو يحفّزها.

عند التحضير لورشة عمل حول هذا الموضوع، تعاملي مع العنف على الإنترنت بالطريقة نفسها التي تتعاملين بها مع أي نقاش حول العنف: أي بعناية وبحرص لكونه موضوعاً محفّزاً للنساء اللواتي مررن به- بغضّ النظر عن الشكل والمدى.

تجنّبي لوم الضحية أو الأفكار التي تحدّ من تعبير النساء

إنّ تحديد ما نشاركه أو نقوله أو كيفيّة الظهور على الإنترنت، هو أمر متروك لقرار كل فرد. ليس الهدف أبداً كمدربّة / ميسّرة إخبار النساء كيفيّة التعبير عن أنفسهن على الإنترنت. كوني متيقّظةً للتدخل في مناقشة تجمع المشاركات يلمن نساءً أخريات على خلفيّة نشر صور أو آراء معيّنة. حرية التعبير ليست المشكلة هنا؛ كراهية النساء هي المشكلة. تتمثّل مَهمّتنا كميسّرات في تشجيع المشاركات على فهم كيفيّة عمل العنف على الإنترنت عبر التجارب المختلفة والتفكير معًا في المقاومة والاستراتيجيات الشافية.

لا يوجد حل شامل للعنف على الإنترنت.

في الواقع، هناك مروحة من الاستراتيجيات لمعالجة كلّ من حالات العنف والبنية التحتية التي تسمح بهذا العنف. ذلك مشابه للطريقة التي نتعامل بها مع العنف الأسري أو عنف الشريك. في بعض الأحيان يكون الطريق القانوني خيارًا جيدًا؛ وتكون التدخلات المجتمعية في أحيانٍ أخرى أكثر فائدة؛ وفي بعضها الآخر، يكون من الجيّد الاستلقاء لفترة من الوقت؛ أحيانًا يكون تعزيز المحتوى النسوي أكثر استراتيجية، وغالبًا ما يكون الحل مزيجًا من النشاط القصير والطويل الأمد.

الرضائية ضرورة

يمكن للثقافة السائدة على الإنترنت أن تتسرّع أحيانًا في اتخاذ تجربة صادمة ما، مادة لدراسة حالة، قد يرى النشطاء فيها فرصة لإثارة القضية إعلاميًا؛ أو تقديم صورة شخص ما للجمهور باعتباره/ا أحد/ى الناجين/ات من العنف. من المهم التشديد على أهمية الرضائية خلال ورشة العمل. لا ينبغي أبدًا إخضاع الناجيات لضغوطات الرقابة العامة. تُنسِب الثقافة على الإنترنت «بطولة» معيّنة إلى سرديّة الناجيات– إلاّ أنّ هذا لا ينبغي أبدًا أن يكون على حساب اتخاذ الفرد للقرار المستنير، أو على حساب الأمان الشخصي.

فهم العنف القائم على النوع الاجتماعي على الإنترنت

ستتمكّنين من الاستفادة من تجارب المشاركات الشخصيّة مع العنف على الإنترنت. إلاّ أنّه من المهم أيضًا أن تتعرّفي، كمدرّبة، على الجوانب المختلفة لهذا الموضوع. **ويتضمّن ذلك:**

١. **الإلمام بالسياق:** تختلف التجارب مع العنف وفق الثقافة أو الجغرافيا أو البيئة القانونية أو اللغة. لذا، من المهم أن تكوني مُلمّةً بالسياق.

٢. **مواكبة التطورات:** تتغيّر التجارب أيضًا بمرور الوقت، حيث تستكشف النسويّات طرقًا جديدة للتواصل والتنظيم عبر الإنترنت وتحدّي كراهية النساء، لذا من المهم أن تكوني على اطلاع بتلك السياسات والاستراتيجيات.

استطلاع المدافعات الإقليميات عن حقوق الإنسان (٢٠٢١)

أجرت منظمة **Fe-Male**، عام ٢٠٢١، استطلاعًا عبر الإنترنت مع مدافعات عن حقوق الإنسان من منطقة الشرق الأوسط وشمال إفريقيا، لفهم التجارب المباشرة مع العنف على الإنترنت والأمان الرقمي. التقرير الكامل متاح على **www.fe-male.org** وهو يعدّ مرجعاً جيّدًا لفهم العنف القائم على النوع الاجتماعي على الإنترنت.

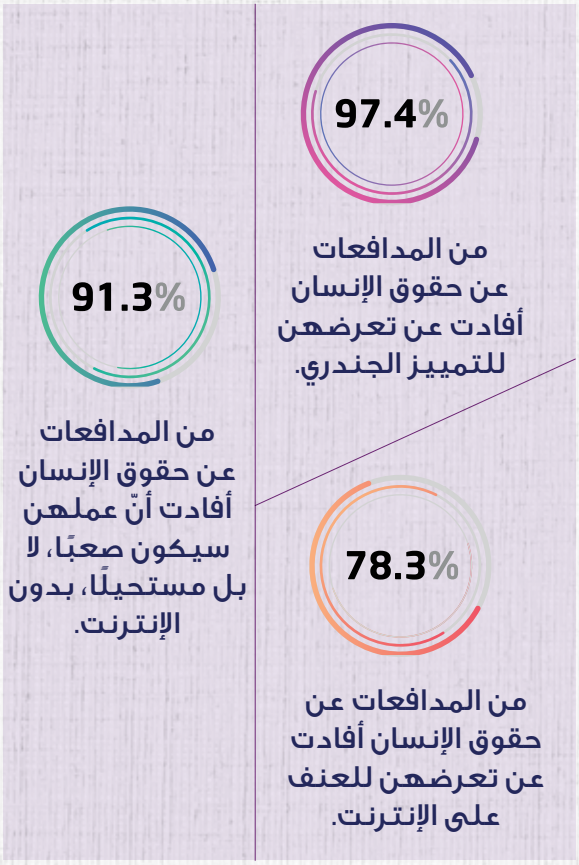
أبرز ما بيّنه الاستطلاع من نتائج، هو التناقض الصارخ بين أهميّة الإنترنت للنشاط النسوي، في مقابل مستوى العنف المقلق الذي تتعرض له الناشطات على الإنترنت.

فقد أفادت ٩١,٣٪ من المدافعات عن حقوق الإنسان في الاستطلاع أنّ عملهن سيكون صعبًا، لا بل مستحيلًا، بدون الإنترنت. فمعظمهن يستخدم الإنترنت لتنظيم الحملات، وزيادة الوعي بقضايا النوع الاجتماعي؛ والغالبية الساحقة من هذه الأنشطة (٨٢,٦٪) مرئية لجمهور الإنترنت، منها ٥٢,٢٪ مرئية للغاية. وتتّفق ٩٧٪ من المستجيبات على أنّ «الإنترنت مجال عام هامّ للنهوض بالقضايا التي يعملن عليها.»

يوضح هذا، بلا أدنى شك، مدى أهمية وجود إنترنت مفتوح ومجاني وآمن بالنسبة للمدافعات عن حقوق الإنسان في منطقة الشرق الأوسط وشمال إفريقيا. مع ذلك، فإنّ الثمن الذي يدفعنه على المستويين الشخصي والمهني في مقابل نشاطهن الرقمي يثير مخاوف جديّة. فقد أفاد ٧٨,٣٪ منهن عن تعرضهن للعنف على الإنترنت؛ أكثر هذه التجارب شيوعًا، كانت الرسائل ذات المحتوى الجنسي والعنصري والمعادي للمثلية (٥٥,٧٪)؛ فيما أفاد ٣٠,٤٪ بأنّهن تلقّين اعتداءات مباشرة أو تهديدات بالعنف، وواجه ٩,٦٪ إجراءات قانونية بسبب نشاطهن الإلكتروني.

عندما سُئلن عن تجارب الاعتداءات على الإنترنت ذات الطابع الجندري بشكل خاص، أفاد ٩٧,٤٪ من المستجيبات عن تعرضهن لشكل واحد، على الأقل، من التمييز الجندري؛ من بينها ٥٣,٩٪ تلقّين اعتداءات متحيّزة جنسيًا (كالوصم بالعهر، أو التلاعب النفسي) و(٤٤,٣٪) تلقين تعليقات على المظهر أو نمط الحياة أو اللباس و(٣٨,٣٪) تلقين تهديدات ذات طابع جنسي.

أبرز النتائج



تجارب مع العنف على الإنترنت

اختار أكثر من نصف المستجيبات الإسهاب في الحديث عن تجاربهن، وعن تعرّض الكثير منهن لأشكال متعدّدة من العنف. وأفادت إحدى المستجيبات:

«تعرّضتُ لاعتداءات على الإنترنت ولتحرّش جنسي وتهديدات بالاغتصاب وقد أغلقت حسابي على إنستغرام مرّتين، من ثمّ لم يعد بإمكاني تسجيل الدخول بسبب البلاغات. كما تمّ بسبب البلاغات أيضاً، تعطيل حساب منظمتي على تويتر، وحُذفت مقاطع الفيديو المنشورة على فايسبوك باستمرار، وتمّ حظر حساب منظمتي على فايسبوك ١٣ مرة. [لقد قاموا] بإنشاء حسابات مزيّفة باسمي على فايسبوك، أبلغت عنها مرات عدة، إلّا أنّه لم يتم حذفها بعد. وقد استخدموا اسمي لنشر أخبار كاذبة عني، فضلاً عن تهديدات لحياتي وابتزاز جنسي وعدائية ووصم بالعهر، بشكل يومي.»

كما أفادت العديد من المستجيبات أيضًا عن إحباطهن من نظم المنصّات في ما خصّ التبليغ عن محتوى ضار، ومن عدم تمكّنهن من الوصول إلى حساباتهن أو حسابات مؤسساتهن بسبب حملات التبليغ. هذا، بالإضافة إلى اختبارهن للقرصنة كشكلٍ من أشكال الانتقام من المحتوى النسوي أو السياسي.

«تم اختراق حساب الإنستغرام الخاص بالمنظمة لمدّة يوم كامل، فيما لدينا بيانات سريّة بالأشخاص الذين يتواصلون معنا مباشرة، ممّن لا يودّون تعرّض محتواها للكشف أو التلاعب.»

وتجدر الإشارة أيضًا إلى أنّ عددًا كبيرًا من المستجيبات ناقشن الهجمات المطوّلة على الإنترنت التي استمرّت لأشهر أو سنوات، لا كحالات فردية. وقد شهدت تصاعدًا في مناسبات مختلفة وارتبط معظمها بالمحتوى الذي نشرته المدافعة عن حقوق الإنسان حول قضايا نسويّة.

«تلقّيت على مدار أكثر من عام، تهديدات مباشرة بالقتل والترهيب، امتدت إلى التعرّض للاختطاف من حزب سياسي نافذ، تلتها دعوى قضائية ضدّي في المحكمة العسكرية وتهديدات بالسجن.»

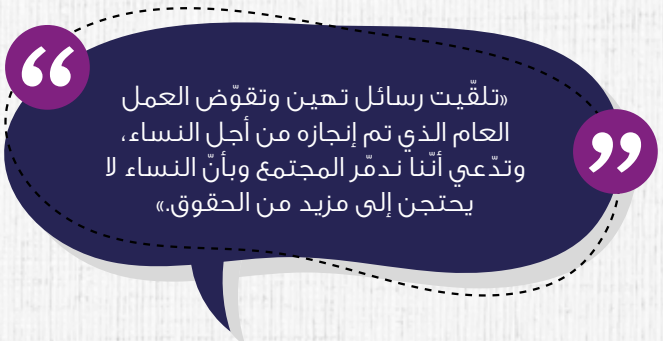
«أتلقى رسائل خاصة مستمرّة تتضمن عُريًا ومحتوى جنسيًا وتحرّشاً.»

تمت الإشارة بشكل واسع، إلى التشهير بالمدافعات عن حقوق الإنسان، كتكتيك متحيّز جنسيًا يهدف إلى الإسكات، بما في ذلك إنشاء حسابات مزيّفة أو نشر شائعات كاذبة.

امتدت هذه الاعتداءات لتشمل أيضًا أطفال المدافعات عن حقوق الإنسان، حيث أفادت إحداهن عن تلقي «رسائل مهينة تهاجم حياتي الشخصيّة وابني وحياتي المهنية.» فيما ذكرت أخرى أنها تلقّت تهديدات تتعرّض لابنتها البالغة من العمر ١٠ سنوات، إثر مقابلة إعلامية حول حقوق النساء الجنسيّة.

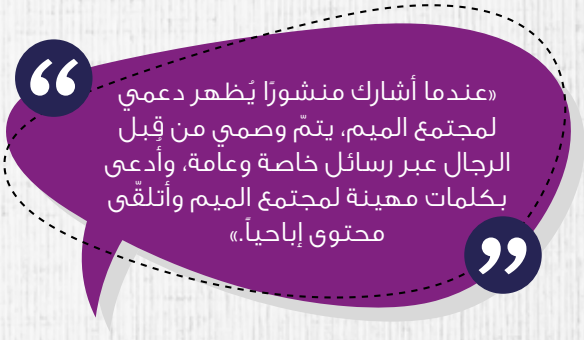
أفادت إحدى النساء بالتالي:

كما يلجأ المهاجمون عادة، إلى الأعراف الاجتماعية الأبويّة لمهاجمة المظهر الشخصي أو أنماط حياة الناشطات النسويّات، متّهمين إياهن بتدمير الثقافة وتحريض النساء.



هكذا، فإن النساء اللواتي يتحدثن علنًا ضد التحيّز الجنسي والتمييز، يتحمّلن العبء الأكبر للحملات الضارة ضدّهن على الإنترنت– باستخدام الأدوات ذاتها التي يشجبنها. لا وجود لخط فاصل بين الحياة الشخصيّة للمدافعات عن حقوق الإنسان ومحتوى منشوراتهن العامة على الإنترنت. في الواقع، تتمثّل الاستراتيجية الشائعة للمهاجمين بفضح، أو التهديد بفضح البيانات الشخصيّة للنسويّات، كشكلٍ من أشكال الاعتداء.

فيما تم ذكر المحتوى الجنساني كمحرّض على التعليقات الكارهة للنساء، إلّا أنّ المدافعات عن حقوق الإنسان اللواتي يتركّز نشاطهن على قضايا حقوق الإنسان الأوسع نطاقاً، أبلغن أيضًا عن تعرضهن لهجمات منحازة جنسيًّا، لمجرد كونهنّ نساء يتحدثن علانية:



«ركّزت الدولة على اضطهاد المدافعات عن حقوق الإنسان وحَمَلتهن على توقيع تعهّدات بالتوقّف عن استخدام تويتر. لا هَمَّ إن كان حسابك خاصًا أو عامًا أو عدد متابعيك، فجميع النسويّات يتعرضن لتهديد شديد.»

آثار العنف على الإنترنت

تؤثر الهجمات على النشاط النسوي على الإنترنت، على رفاه المدافعات عن حقوق الإنسان، بشكل كبير. غالبًا ما تؤثر حملات التشهير على وصولهن إلى الوظائف أو الشبكات الاجتماعية، فضلاً عن الأضرار النفسية والاجتماعية الشديدة بموازاة الشعور بالمراقبة المستمرّة، ممّا يدفع أيضًا بالنساء بعيدًا عن فضاء الإنترنت العام.

> «أتلقّى رسائل مؤذية، تتضمّن غالبًا إهانات جنسية. أحاول تجاهلها، لكني أمضي اليوم كلّه قلقةً منها.»

> «تمّ استدعائي لاستجوابات أمنية، حيث تمّ تهديدي. يتملّكني شعور دائم بأنني مراقَبة.»

مساحات آمنة عبر الإنترنت

عند الحديث عن العنف، من المهمّ التفكير في مقابله الإيجابي: الأمان. ماذا يعني الأمان بالنسبة للمشاركات؟ كيف نحدّد المساحة الآمنة عبر الإنترنت أو تلك المباشرة؟

لدى **APC** برنامج حول إنشاء مساحات آمنة عبر الإنترنت متوفّر هنا:

https://en.ftx.apc.org/books/creating-safe-online-spaces

يمكن تكييف أحد التمارين الواردة فيه، وإليكِ أحد الأمثلة:

تمرين تفكيك مفهوم الأمان

الوقت المطلوب: ٤٠ دقيقة

المواد المطلوبة: ألواح ورقية وأقلام وورق لاصق كبير

الهدف الرئيسي من التمرين هو أن تعبّر المشاركات عن تعريفهن الخاص للمساحة الآمنة، والخروج بفهم مشترك لهذه المساحة. قد تستخدم المجموعة هذا التمرين كخطوة أولى في تصميم مساحات جديدة عبر الإنترنت معًا، أو في إعادة تصميم مساحة موجودة، مع مراعاة القيم المشتركة للأمان.

التخيّل الفردي:

(١٠ دقائق) اطلبي من المشاركات إغلاق أعينهن والتفكير في مكان/ وزمان/ ظرف معيّن شعرن فيه بالأمان. شجّعيهن على أن يكنّ محدّدات في تخيّلهن ووصفهن للمكان والأشخاص والمناخ والألوان والمشاعر إلخ. يمكنك أيضًا الطلب من المشاركات التعبير عن ذلك من خلال الرسم.

مناقشة ضمن مجموعات صغيرة:

(١٥ دقيقة) في مجموعات صغيرة مكوّنة من ثلاثة إلى خمسة أشخاص، اطلبي من المشاركات أن يشاركن تخيّلاتهن. امنحيهن وقتًا كافيًا للمشاركة والتفكير الفردي.

المجموعة الكاملة:

(١٥ دقيقة) للمعالجة، دوّني كلمة «الأمان» في منتصف اللوح الورقي، وابدئي خريطة ذهنية لأفكار المشاركات حول سؤال: **«ما الذي جعلكِ تشعرين بالأمان؟»**

ستتوصلين، بنهاية التمرين، إلى قائمة بالكلمات والعبارات والمفاهيم التي تعرّف كلمة **«أمان»**.

* ملاحظات للمدرّبة/الميسّرة:

- ابحثي عن القواسم المشتركة في ردود المشاركات وتوقفي أيضًا عند الاختلافات في ردودهن.
- انتبهي وأبرزي المعايير التي يمكن تطبيقها في المساحات عبر الإنترنت.
- قومي دائمًا باستخلاص الدروس المستفادة من النشاط لتعزيز المفاهيم.

إدارة حسابات وسائل التواصل الاجتماعي

يعدّ قرار استخدام شبكات التواصل الاجتماعي مثل فايسبوك أو إنستغرام أو تيك-توك أو تويتر أمرًا صعبًا بالنسبة للعديد من الناشطات النسويات. من ناحية، هناك وصول **(reach)** هائل. ومن ناحية أخرى، لهذه الشركات سياسات إشكاليّة، كونها تركّز فقط على جني الأرباح؛ فيتم جمع المحتوى النسوي عبر الإنترنت كبيانات، ليتمّ بيعها للمعلنين.

يمكن إضافة قسم حول أمان الحساب في التدريب، للتأكّد من أنّ المشاركات يتخذن قرارات مستنيرة بشأن استخدامهن لوسائل التواصل الاجتماعي، على الصعيدين الشخصي و المهني.

تذكير: إن كنتِ تعملين في منظمة نسويّة، لا تنسي أنّ الصفحات الشخصيّة عرضة أيضًا لهجمات كراهية النساء، لا صفحات المنظمة حصرًا.

مناقشة: تحديد ما تريدين مشاركته عبر الإنترنت

شجعي المشاركات على التفكير في قراراتهن الخاصة بشأن ما يخترن مشاركته عبر الإنترنت ولمن. في ما يلي بعض المحفزات لبدء النقاش:

1. اسألي المشاركات: هل تقمن بنشر المعلومات التالية عبر الإنترنت؟ هل من الضروري ذلك؟ كيف تتفاوضين حول مشاركة البيانات هذه؟

- تاريخ الميلاد
- أرقام الاتصال الهاتفية
- العناوين/ المواقع
- تفاصيل حول أفراد الأسرة
- الميول الجنسية أو تاريخ المواعدة
- التعليم والتاريخ الوظيفي

٢. اطلبي من المشاركات التفكير في السؤال التالي: هل قام صديق أو جهة ما، بمشاركة معلومات عنكِ عبر الإنترنت، لم توافقي على نشرها مسبقًا؟ هل قاموا بذلك عن قصد أو بغير قصد؟

٣. اطلبي من المشاركات التفكير في إحدى المعلومات الشخصيّة التي تخصّهن، والتي يتعذّر العثور عليها عبر الإنترنت. من دون كشفها، اطلبي منهن مشاركة المجموعة في كيفية نجاحهن بتجنّب نشرها.

٤. اطلبي من المشاركات البحث عن أسمائهن على غوغل (باستخدام التصفّح الخاص، لتجنّب البحث المخصّص). ماذا يظهر لهن؟ ما الذي يزعجهن بشأن ما يظهر؟ نقاش.

ME AND MY SHADOW
TAKE CONTROL OF YOUR DATA

تدريب إضافي: إن كان هناك وقت كافٍ في التدريب، اطلبي من المشاركات رسم خريطة لهويتهن الرقمية. ما هي المجموعات التي يرتبطن بها؟ ما هي الكلمات المفتاحيّة المرتبطة بهن؟ ما الذي يمكن للجمهور اكتشافه بشأن بياناتهن الشخصيّة؟

تقدم **Tactical Tech** موردًا رائعًا على

/https://myshadow.org

للقيام «بديتوكس (detox) رقمي» للبيانات عبر الإنترنت. يمكن أيضًا استخدام قسم «المدرّب/ة» في الموقع للحصول على موارد إضافية لتضمينها في ورشة العمل.

حماية حسابات وسائل التواصل الاجتماعي

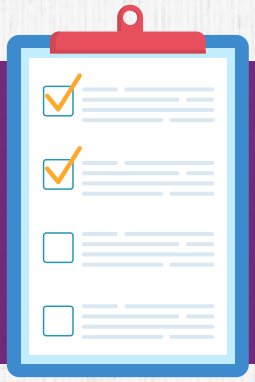
بالإضافة إلى الإجراءات التي تمّت مناقشتها في القسم ٢، يمكن تيسير جلسات تركّز على حماية حسابات وسائل التواصل الاجتماعي. تقدّم معظم الشركات (بما في ذلك فايسبوك وغوغل) «اجراءات أمان» خاصة بها، تساعد في حماية الحسابات عبر خطوات مختلفة. قد يبدو ذلك معقدًا نوعًا ما بالنسبة لبعض المشاركات. لذا، قد يكون من الجيّد مرافقتهن خطوة بخطوة، في إطار ورشة العمل، لبناء ثقتهن في التعامل مع هذه الأمور بأنفسهن.

يحتاج فايسبوك على وجه الخصوص، اهتمامًا مستمرًا، كونه موقع التواصل الاجتماعي الأكثر استخدامًا اليوم. ضمن «أمان وخصوصيّة الحساب»، يمكن للمشاركات الاطّلاع على الخيارات المختلفة المتاحة، والقيام باختيارات حول الجماهير والبيانات. من المهم تذكير المشاركات بأنّهن لا يستطعن حماية بياناتهن من الشركة نفسها، أو من معلنيها. لذا، فإن مشاركة المعلومات– حتى وإن كانت خاصة– على فايسبوك، يجب أن تنبع من قرار مستنير. ومع ذلك، يمكنهن حماية بياناتهن من الظهور لجمهور الإنترنت أو قوائم الأصدقاء.

تتيح غوغل أيضًا قائمة التحقّق من الخصوصيّة في الحساب. يمكن أن ينبّهكِ إلى كلمات المرور الضعيفة المرتبطة بالحساب أو تاريخ التصفّح، أو مصادقات النسخ الإضافية الاحتياطية. من الجيّد وضع تذكير للتحقّق من هذا الخيار بشكل منتظم.

* تذكير: إن تلقيتِ بريدًا إلكترونيًا أو إشعارًا بالحاجة إلى تأمين الحساب، تحقّقي مرتين وثلاث مرات من صحة عنوان الـ URL للشركة المُرسلة. يجب أن يوجّهك العنوان إلى **facebook.com** أو **google.com** حتى يكون أصليًا. يشكّل التحذير الأمني ممارسة تصيّد احتيالي شائعة جدًا. راجعي قسم التصيّد لتسترجعي كيفيّة التحقّق من الروابط المشبوهة.

التحقّق المزدوج



التحقّق المزدوج

(Two-factor authentication) مهمّ للغاية، لأنه يضيف إلى مستويات الأمان للوصول إلى الحساب، كما أنّه يمكّنك من استرداده إن فقدتِ كلمة المرور، أو تمّت سرقتها. تأكّدي من مطالبة جميع المشاركات بتفعيل هذه الميزة على جميع حساباتهن.

يستخدم خبراء الأمان في الواقع، التحقّق الثلاثي للحصول على أمان أفضل: شيء تعرفينه، شيء ما أنت عليه، شيء تملكينه. بالنسبة لمعظم الشركات عبر الإنترنت، فإنّها توفّر لكِ إمكانيّة إدخال عنصرين من هذه الثلاثة:

شيء تعرفينه= كلمة المرور

شيء تملكينه= هاتفكِ المحمول الذي يتلقّى رسالة نصيّة قصيرة أو إشعار أو كود

يعدّ التحقّق المزدوج طريقة جيدة أيضًا، للتنبيه إذا ما حاول أحدهم اختراق الحساب. إذا تلقيتِ رسالة تحتوي على كود تحقُّق لم تقومي بطلبه، تأكدي من تغيير كلمة المرور فورًا.

استراتيجيّات الاستجابة للعنف

من المهم أن نتذكر أنّ الاستجابات للعنف عبر الإنترنت، لا تقلّ أهمية في جانبها الاجتماعي عن جوانبها التقنية. فكما يقول المثل: لا يوجد حلٌّ تقني لمشكلة اجتماعية.

لذا، من المهم التفكير مع المشاركات، حول الاستراتيجيات المختلفة في الاستجابة للعنف عبر الإنترنت. ومن المهم أيضًا أن تتذكّري وتذكّري المشاركات، أنّه لا وجود لحلّ أوحد يناسب الجميع. الإنترنت عبارة عن شبكة من الأشخاص، والاستجابة الذكية الوحيدة تأتي من خلال شبكة من الأشخاص- وليس من خلال مسارات فردية. إليكِ تمرين جيّد للتفكير في الاستجابة للعنف عبر الإنترنت:

نداء للمساعدة

الوقت: ٦٠ دقيقة

المواد المطلوبة:
لوح ورقي وأقلام تحديد

تشارك الميسّرة السيناريو التالي مع المجموعة:

لقد استيقظتِ هذا الصباح، على رسالة في بريدكِ الإلكترونـي، موجّهة إلى الجميع، من قبل شخص ما في هذه الغرفة، جاء فيها:

«صديقاتي، لقد فتحتُ هاتفي الليلة الماضية لأجد المئات من الإخطارات والرسائل القصيرة المليئة بالتهديدات البغيضة والعنيفة. ذلك، لأنني قمتُ بنشر مقال نسويّ على حائطي. لا أعرف كيف انتشر، أو من هم هؤلاء الناس، أو ماذا حدث. أنا خائفةٌ جدًا. لا أعرف كيف أتصرّف. الرجاء المساعدة.»

اطلبي من كل مشاركة أخذ ٥ دقائق لصياغة ردّ على الإيميل. يجب أن تفكّر كل مشاركة في ما ستقوله، وفي نوع المساعدة أو النصيحة التي يمكنها تقديمها. عندما يصبحن جاهزاتٍ جميعًا، اطلبي منهن مشاركة ردودهن في الجلسة العامة.

تسجّل الميسرة الكلمات الأساسية التي تمّت مشاركتها وتكتبها على لوح ورقيّ مشترك. ضعي علامة نجمة بجوار كلمة مفتاحيّة بحال تكرّرها أكثر من مرة. عند الانتهاء، سيكون لديكِ على الأرجح، مجموعة متنوّعة من الاستجاباتِ والاستراتيجيات التي قد تشمل:

- استخدام خيارات الإبلاغ أو الحظر من المنصة
- توثيق الإساءة بلقطات الشاشة (**screenshots**)
- تقديم الدعم الشخصي والعاطفي
- الإستراتيجيات القانونية أو إبلاغ الشرطة
- استراتيجيات الأمان لتأمين الحساب أو تعطيله مؤقتًا
- استراتيجيات المناصرة لتعزيز المحتوى
- استراتيجيات التضامن لإظهار الدعم الشعبي

ستظهر أيضًا بعض الخلافات داخل المجموعة حول الاستراتيجيات المختلفة. على سبيل المثال:

- هل يجب تحويلها إلى قضية عامة وإبرازها في وسائل الإعلام؟ أم إبقاءها بعيدة عن الأضواء كي لا نساهم في انتشارها أكثر؟
- هل يجب أن نواجه المهاجمين بالتعليقات، أم يجب تجاهلهم؟
- هل يجب إعادة مشاركة المحتوى، أم يجب حذفه؟
- هل يجب علينا استدعاء الشرطة، أم يجب أن نتعامل من خلال أدواتنا المتاحة؟

من الجيّد تيسير نقاش حول هذه الخيارات: لماذا، ولِمَ لا؟ تذكّري النصائح التي ذكرناها في بداية هذا الجزء. موافقة الناجية أمر أساسي دائمًا. في بعض الأحيان، تكون المقاربات المتعدّدة صحيّة. وفي أحيان أخرى، تتناقض مع بعضها البعض وتصبح عديمة الفائدة. تشعر بعض النساء براحة أكبر في المواجهة العامة، في حين تفضّل نساء أخريات عدم الانخراط.

ما يجب التأكيد عليه، هو قوّة الشبكة في الاستجابة لهذه التهديدات، واعتماد السبل المحدّدة على الوضع القانوني أو السياسي في كلّ سياق.

موارد

خطوط المساعدة في الأمان الرقمي

توفّر **Access NOW** دعمًا للأمان الرقمي على مدار الساعة طوال أيام الأسبوع، بما في ذلك باللغة العربية من مكتبهم في تونس. زوري :

https://www.accessnow.org/help/

لمزيد من المعلومات حول الخدمات،

أو أرسلي بريدًا إلكترونيًا إلى

help@accessnow.org

للحصول على الدعم.

توفّر **SMEX** مكتب دعم حول السلامة الرقمية في حالات الطوارئ

يمكنك مراسلتهم على **Signal** أو **Whatsapp** على

+961 81 633 133

أو عبر البريد الإلكتروني

helpdesk@smex.org

توفّر منظمة **APC** مجموعة رائعة من الموارد حول السلامة الرقميّة تسمّى (أمان التبادل التقني النسوي) قومي بزيارة

http://en.ftx.apc.org/

للحصول على منهج يتكوّن من عدة وحدات للمدربين/ات اللواتي يعملن مع نشطاء حقوق النساء والحقوق الجنسية لاستخدام الإنترنت بأمان وإبداع واستراتيجية.

تقدم **Tactical Tech** قاعدة بيانات تعليمية كبيرة في إطار دليل النوع الاجتماعي والتقنيّة على:

/https://gendersec.tacticaltech.org

والذي تم تطويره بشكل جماعي مع العديد من المدربين/ات من جميع أنحاء العالم.

يعمل مشروع ديمقراطية الإنترنت في الهند على تحقيق المنظور النسوي الرقمي في المجتمع من خلال استكشاف ومعالجة اختلالات القوّة في مجالات المعايير والحوكمة والبنية التحتية. يقدم المشروع موردًا حول النوع الاجتماعي والمراقبة عبر الإنترنت هنا:

https://genderingsurveillance.
/internetdemocracy.in

يقدم معهد صحافة الحرب والسلام ترجمة عربية لدليل حول الأمن الرقمي على الموقع:

/https://cyber-women.com

FE-MALE

LOUD- PROUD- FEMINISTS

بيروت، سامي الصلح شارع الجامعة اللبنانية – كلية الفنون،
مقابل حديقة فرن الشباك العامة، بناية الحايك، الطابق الأرضي

009611380873

info@fe-male.org

www.fe-male.org

FeMaleComms