



النساء في فضاء الإنترنت



المنهاج التدريبي الخاص
بالأمن الرقمي الشامل
للمدافعات عن حقوق
الإنسان

النساء فى فضاء الإنترنت

**INSTITUTE FOR
WAR & PEACE REPORTING**



© 2019– Institute For War And Peace Reporting

<https://iwpr.net/>



نَسَبُ الْمُصَنَّفِ - الترخيص بالمثل 4.0 دولي

<https://creativecommons.org/licenses/by-sa/4.0/deed.ar>

المحتويات

١٧	I	مقدمة
١٩	١	مقدمة
١٩		تعريف بالنساء في فضاء الإنترنت
٢٠		إستخدام مناهج النساء في فضاء الإنترنت
٢١		مقاربة نسوية في وضع المنهاج
٢٢		مشاركات ومدربات
٢٢		النماذج النسائية والنسوية
٢٣		جسدي وأجهزتي وقراري!
٢٣		الرعاية الذاتية النسوية والدفاع الرقمي عن النفس
٢٥	٢	تخطيط الموارد
٢٥		تقييم الحاجات والمحفزات
٢٦		أداة بناء قدرات الأمن الرقمي Digital Security and Capacity (DISC) Tool
٢٧		إستراتيجيات التقييم البديلة
٢٩	٣	شكر وتقدير

٣١	II	تمارين بناء الثقة
٣٣	٤	قواعد اللعبة
٣٤		إدارة التمرين
٣٧	٥	بينغو المدافعات
٣٨		إدارة التمرين
٤١	٦	الحلوى المخادعة
٤٢		إدارة التمرين
٤٣	٧	بمن تثقن
٤٤		إدارة التمرين
٤٧	III	إعادة النظر بعلاقتنا بالتكنولوجيا
٤٩	٨	وجهات النظر الشخصية حيال الأمن
٥٠		إدارة التمرين
٥٠		الجزء الأول - ما هي السلامة بالنسبة لكن؟ ما هو الأمن بالنسبة لكن؟
٥٢		الجزء الثاني - ما هو الأمن الرقمي بالنسبة لكن؟
٥٣		الجزء الثالث - تحديد الحوافز وأسباب الرفض والحواجز
		الجزء الرابع - المعتقدات الخاطئة المتداولة بشأن الأمن الرقمي والجنذر والتكنولوجيا
٥٣		الجزء الخامس - الملاحظات الختامية
٥٧		المراجع
٥٨		
٥٩	٩	حقوقك والتكنولوجيا الخاصة بك
٦٠		إدارة الجلسة
٦٠		الجزء الأول - ربط الحقوق بالتكنولوجيا
٦١		الجزء الثاني - مفاهيم الأمن الرقمي والحقوق الرقمية
٦٣		References

٦٥	١٠ قصتها مع التكنولوجيا
٦٦	إدارة الجلسة

٦٩ IV أسس الأمن الرقمي الجولة الأولى

٧١	١١ كيف يعمل الإنترنت؟
٧٢	إدارة الجلسة
٧٢	الجزء الأول - كيف يعمل الإنترنت - تدفق المعلومات ونقاط الضعف.
٧٣	الجزء الثاني - نقاط الضعف
٧٤	الجزء الثالث - الممارسات السليمة في الأمن الرقمي
٧٦	الجزء الرابع - الموارد والمسائل العالقة
٧٦	المراجع

٧٧	١٢ بناء كلمات سر قوية
٧٨	إدارة الجلسة
٧٨	الجزء الأول - المقدمة
٧٨	الجزء الثاني - ما أهمية كلمات السر؟
٧٩	الجزء الثالث - ماذا قد يحصل في حال تعرض كلمة سر كم للسرقة؟
٨٠	الجزء الرابع - كيفية تعرض كلمات السر للسرقة عادة؟
٨١	الجزء الخامس - كيف يمكننا جعل كلمات سرنا أقوى؟
٨٢	المراجع

٨٣	١٣ البرمجيات الخبيثة والفيروسات
٨٤	إدارة الجلسة
٨٤	الجزء الأول - تعريف بالبرمجيات الخبيثة
٨٤	الجزء الثاني - كيف يمكن أن نتعرضن للإصابة بها؟
٨٥	الجزء الثالث - مشاركة أمثلة عن نساء ومدافعات عن حقوق الإنسان

٨٧	١٤ التصفح الآمن
----	-----------------

٨٨	إدارة الجلسة
٨٨	الجزء الأول - إختيار المتصفح
٨٨	الجزء الثاني - ممارسات التصفح الأكثر أماناً
٩٠	الجزء الثالث - الأدوات والبرامج المضافة من أجل تصفح أكثر أماناً
٩٢	المراجع
٩٣	١٥ كيفية حماية حاسوبك
٩٤	إدارة الجلسة
٩٤	الجزء الأول - مقدمة
٩٤	الجزء الثاني - المحيط المادي والصيانة
٩٥	الجزء الثالث - سلامة البرمجيات
٩٧	الجزء الرابع - حماية البيانات والنسخ الاحتياطية
٩٨	الجزء الخامس - حذف الملفات إستعادتها
٩٩	المراجع
١٠١	V الخصوصية
١٠٣	١٦ إطرحي علي ما تريدينه من أسئلة!
١٠٤	إدارة الجلسة
١٠٧	١٧ الخصوصية
١٠٨	إدارة الجلسة
١٠٨	الجزء الأول - هل تتمتع فعلاً بالخصوصية؟
١٠٩	الجزء الثاني - "الاستقصاء عن الذات" Self Doxxing
١١٠	الجزء الثالث - ماذا نفعل الآن؟
١١٢	المراجع
١١٣	١٨ الجمهور الشبكي
١١٤	إدارة الجلسة
١١٥	المراجع

١١٧	١٩ التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟
١١٨	إدارة الجلسة
١١٨	الجزء الأول - أجهزتنا وبياناتنا
١١٩	الجزء الثاني - من يتعقبنا أيضاً؟
١٢٠	الجزء الثالث - الترويج لحقوق المرأة على شبكات التواصل الاجتماعي
١٢١	الجزء الرابع - إستعادة الخصوصية
١٢٢	المراجع

١٢٣ VI المناصرة الآمنة على الإنترنت

١٢٥	٢٠ مواقع إلكترونية أكثر أماناً
١٢٦	إدارة الجلسة
١٢٦	الجزء الأول - ما الأشكال الممكنة للهجمات الإلكترونية؟
١٢٧	الجزء الثاني - حماية المواقع الإلكترونية
١٣٠	المراجع
١٣١	٢١ الحملات الآمنة على الإنترنت
١٣٢	إدارة الجلسة
١٣٢	الجزء الأول - المقدمة والتخطيط الوقائي
١٣٤	الجزء الثاني - حماية الأجهزة
١٣٥	الجزء الثالث - إدارة إمكانية الوصول في الحسابات
١٣٦	الجزء الرابع - اختيار التطبيقات للحملات
١٣٧	الجزء الخامس - بناء المجتمعات من خلال فايسبوك
١٣٨	المراجع

١٣٩	٢٢ ماذا يمكن لبياناتك الوصفية (Metadata) أن تفسح عنك؟
١٤٠	إدارة الجلسة
١٤٠	الجزء الأول - ما هي البيانات الوصفية؟ Metadata
١٤١	الجزء الثاني - تداعيات البيانات الوصفية في بيئة العمل على حقوق الإنسان

١٤٢ المراجع

١٤٣ VII هواتف محمولة أكثر أماناً

١٤٥ ٢٣ ماركو بولو
١٤٦ إدارة الجلسة

١٤٧ ٢٤ الهواتف المحمولة، الجزء الأول

١٤٨ إدارة الجلسة

١٤٨ الجزء الأول - ما هي مكونات الهاتف؟

١٥٠ الجزء الثاني - الممارسة التطبيقية

١٥٠ المراجع

١٥٣ ٢٥ الهواتف المحمولة، الجزء الثاني

١٥٤ إدارة الجلسة

١٥٤ الجزء الأول - التشفير في الهواتف المحمولة

١٥٥ الجزء الثاني - استخدام برمجية جي بي جي على الهواتف المحمولة

١٥٥ الجزء الثالث - هل يقوم هاتفك بتتبعك؟

١٥٦ المراجع

١٥٧ VIII المحافظة على سرية الهوية

١٥٩ ٢٦ الصديقة السرية

١٦٠ إدارة الجلسة

١٦٠ الجزء الأول - المقدمة

١٦٠ الجزء الثاني - حان وقت اللعب!

١٦٢ الجزء الثالث - الحلقة الختامية

١٦٣ ٢٧ المحافظة على سرية الهوية

١٦٤ إدارة الجلسة

١٦٤	الجزء الأول - تعريف بالمحافظة على سرية الهوية على الإنترنت
١٦٥	الجزء الثاني - البيانات المحددة للهوية والمحافظة على سرية الهوية
١٦٦	الجزء الثالث - بعض التطبيق العملي
١٦٧	٢٨ المزيد من الهويات الإلكترونية!
١٦٨	إدارة الجلسة
١٦٨	الجزء الأول - الهويات الإلكترونية المتصلة
١٦٩	الجزء الثاني - فصل الهويات الإلكترونية عن بعضها البعض وإدارتها
١٧٠	الجزء الثالث - الممارسة التطبيقية والتوصيات
١٧٢	المراجع

IX التشفير ١٧٣

١٧٥	٢٩ تعريف بمسألة التشفير
١٧٦	إدارة الجلسة
١٧٦	الجزء الأول - هل سبق لكن أن إستخدمت التشفير؟
١٧٨	الجزء الثاني - شرح ماهية التشفير
١٧٩	المراجع
١٨١	٣٠ الإتصالات المشفرة
١٨٢	إدارة الجلسة
١٨٣	المراجع

X أسس الأمن الرقمي، الجولة الثانية ١٨٥

١٨٧	٣١ التخزين والتشفير
١٨٨	إدارة الجلسة
١٨٨	الجزء الأول - نسخ البيانات الاحتياطية والتخطيط
١٨٩	الجزء الثاني - تشفير التخزين والنسخ الاحتياطية
١٩٠	المراجع

١٩١	٣٢ نعد إلى خانة الصفر (إعادة الضبط)!
١٩٢	إدارة الجلسة
١٩٢	الجزء الأول - تبيد الخرافات
١٩٣	الجزء الثاني - ما الذي نعنيه فعليا بإعادة الضبط؟
١٩٤	الجزء الثالث - التحقق: هل نتحتج لإنشاء نسخ احتياطية؟
١٩٤	الجزء الرابع - إعادة الضبط وإعادة التشغيل Resetting & Rebooting
١٩٥	الجزء الخامس - الأنظمة التشغيلية الحية
١٩٧	الجزء السادس - الممارسة التطبيقية
١٩٨	المراجع

XI العنف على الإنترنت ضد النساء ١٩٩

٢٠١	٣٣ طيف الآراء
٢٠٢	إدارة التمرين
٢٠٥	٣٤ إنترنت نسوي
٢٠٦	إدارة التمرين
٢٠٦	الجزء الأول - التوعية
٢٠٧	الجزء الثاني - المبادئ النسوية للإنترنت
٢٠٨	المراجع
٢٠٩	٣٥ العنف الرمزي
٢١٠	إدارة التمرين
٢١٠	الجزء الأول - ما هو العنف الرمزي؟
٢١١	الجزء الثاني - تحديد حالات العنف الرمزي التي إختبرناها
٢١٢	المراجع
٢١٣	٣٦ التبليغ عن الإساءات على منصات التواصل الإجتماعي
٢١٤	إدارة الجلسة
٢١٦	المراجع

٢١٧	٣٧	تبدأ بتوثيق الحالات!
٢١٨	إدارة الجلسة
٢١٨	الجزء الأول - ما أهمية التوثيق؟
٢١٩	الجزء الثاني - كيفية توثيق الحوادث؟
٢٢١	الجزء الثالث - وضع سجلات التوثيق
٢٢٢	الجزء الرابع - ممارسات ونصائح عن كيفية الحفاظ على سجلات التوثيق
٢٢٣	٣٨	الإستقصاء عن المعلومات الشخصية الخاصة بالمتصيد
٢٢٤	إدارة التمرين
٢٢٤	الجزء الأول - ما هو الإستقصاء؟
٢٢٥	الجزء الثاني - تحديد هوية المتحرشين
٢٢٦	الجزء الثالث - أنواع مختلفة من الأشخاص ودوافع مختلفة
٢٢٦	الجزء الرابع - توثيق الحوادث والتحديات
٢٢٩	الجزء الخامس - التحضير للعمل
٢٣٠	الجزء السابع - الأدوات المفيدة
٢٣٢	المراجع

٢٣٣

XII التحادث الجنسي

٢٣٥	٣٩	حان وقت المراقبة!
٢٣٦	إدارة التمرين
٢٣٧	٤٠	التحادث الجنسي
٢٣٨	إدارة الجلسة
٢٣٨	الجزء الأول - وصف مشكلة إجتماعية -
٢٣٨	الجزء الثاني - ما هو التحادث الجنسي؟
٢٣٩	الجزء الثالث - تحادث جنسي أكثر أماناً؟
٢٤١	المراجع

٢٤٣

XIII تحديد الحل الأفضل

- ٤١ نموذج المخاطر القائمة على النوع الاجتماعي
 إدارة الجلسة ٢٤٧
 الجزء الأول - تحديد المخاطر والإحتمالات ٢٤٧
 الجزء الثاني - تحديد مدى التأثير ٢٤٩
 الجزء الثالث - وضع إستراتيجيات للحلول ٢٥٠
 الجزء الثالث - وضع إستراتيجيات للحلول ٢٥١
 المراجع ٢٥١

٢٥٣

٤٢ القرارات المرتبطة بالأمن الرقمي

- إدارة الجلسة ٢٥٤
 الجزء الأول - المقدمة ٢٥٤
 الجزء الثاني - كيف تم بناء البرمجيات التي تستخدمها؟ ٢٥٥
 الجزء الثالث - التفكير في المستخدمين؟ ٢٥٥
 الجزء الرابع - التفكير في الأدوات ٢٥٦
 الجزء الخامس - التدريب على التفكير في الحلول ٢٥٨

٢٦١

٤٣ أنا صاحبة القرار

- إدارة التمرين ٢٦٢

٢٦٥

XIV التخطيط المسبق

- ٤٤ الخطط والبروتوكولات الأمنية الخاصة بالمنظمة
 إدارة الجلسة ٢٦٩
 الجزء الأول - عودة إلى نموذج المخاطر ٢٦٩
 الجزء الثاني - الخطط في مواجهة البروتوكولات ٢٦٩
 الجزء الثالث - وضع خطة وبروتوكولات على مستوى المنظمة ٢٧٠
 الجزء الرابع - ما هي الخطوات التالية؟ ٢٧٢

٢٧٣	٤٥ خطط وبروتوكولات الأمن الرقمي: إعادة تنفيذها بعد التدريب
٢٧٤	إدارة الجلسة
٢٧٤	الجزء الأول - وضع خارطة بالهيكلية والعوائق التنظيمية
٢٧٥	الجزء الثاني - تسيير تنفيذ المنظمة
٢٧٦	الجزء الثالث - طرح المسألة

٢٧٩ XV الرعاية الذاتية

٢٨١	٤٦ بناء الرعاية الذاتية السنوية
٢٨٢	إدارة التمرين
٢٨٥	٤٧ لمسة محبة
٢٨٦	إدارة التمرين
٢٨٩	٤٨ أنظري
٢٩٠	إدارة التمرين
٢٩٣	٤٩ التفكير في الرعاية الذاتية (استنتاجات)
٢٩٤	إدارة التمرين
٢٩٧	٥٠ فعل الرفض
٢٩٨	إدارة التمرين
٣٠١	٥١ رسالة حب إلى نفسي
٣٠٢	إدارة التمرين

٣٠٥ XVI تمارين الختام والمراجعة

٣٠٧	٥٢ الحكايات
٣٠٨	إدارة التمرين
٣٠٩	٥٣ القدر المغلي (المرجل)

٣١٠	إدارة التمرين
٣١٣	٥٤ أزهار النسويات
٣١٤	إدارة التمرين
٣١٧	٥٥ الحلقة السحرية
٣١٨	إدارة التمرين
٣٢١	٥٦ الفوازير!
٣٢٢	إدارة التمرين
٣٢٣	٥٧ سباق الأمن الرقمي
٣٢٤	إدارة التمرين
٣٢٤	الجزء الأول - الإعداد للسباق
٣٢٥	المورد الأول: ترتيب المراحل ودليل مسار الفرق
٣٢٥	المورد الثاني: الأدوات الخاصة بالحالة
٣٢٦	المورد الثالث: الحالات الأمثلة
٣٢٩	الجزء الثاني - إستعداد، تأهب، إنطلاق!
٣٣١	XVII الملحق
٣٣٣	٥٨ أداة الأمن الرقمي والقدرة الرقمية انلخاصة بمعهد صحافة الحرب والسلام
٣٤٣	٥٩ نماذج لجداول أعمال التدريبات
	نماذج لجداول أعمال لورشات عمل تتراوح مدتها بين يوم واحد ويوم واحد ونصف
٣٤٤	اليوم
٣٤٤	ورشة عمل من يوم واحد ونصف اليوم حول تقييم المخاطر
	تدريب توعوي ليوم واحد للهدافعات عن حقوق الإنسان اللواتي يتعاملن
٣٤٥	مع التحرش على الإنترنت

تدريب على تقييم المخاطر ليوم واحد للمدافعات عن حقوق الإنسان اللواتي

- ٣٤٦ يتعاملن مع التحرش على الإنترنت
٣٤٧ أمثلة عن جداول أعمال لورش عمل ممتدة على ثلاثة أيام
٣٤٧ تدريب تمهيدي ممتد على ثلاثة أيام
٣٤٨ تدريب متوسط المستوى ممتد على ثلاثة أيام
٣٤٩ تدريب متقدم ممتد على ثلاثة أيام

- ٣٥١ ٦٠ موارد إضافية
٣٥١ منظمة "حقوق البرمجة"^١
٣٥١ منظمة "انبهوا لمعلوماتكم"^٢
٣٥٢ منظمة الحقوق الرقمية^٣
٣٥٢ منظمة الإنترنت النسوي^٤
٣٥٢ موقع ويكي أمن النوع الاجتماعي من منظمة "تاكتيكل تيك"^٥
٣٥٢ مؤسسة كاريزما^٦
٣٥٣ مشروع "أنا وظلي"^٧
٣٥٣ "إنسحب من برنامج برزم"^٨
٣٥٣ منظمة "شبكة الدفاع عن الحقوق الرقمية"^٩
٣٥٣ "سيكيوريتي إن آي بوكس"^{١٠}
٣٥٤ مشروع حماية الذات من المراقبة^{١١}
٣٥٤ مشروع "لنسترجع التكنولوجيا"^{١٢}

<https://codingrights.org>^١

<https://cuidatuinfo.org>^٢

<https://derechosdigitales.org>^٣

<https://feministinternet.org>^٤

<https://gendersec.tacticaltech.org>^٥

<https://karisma.org.co>^٦

<https://myshadow.org>^٧

<https://prism-break.org>^٨

<https://r3d.mx>^٩

<https://securityinbox.org>^{١٠}

<https://ssd.eff.org>^{١١}

<https://takebackthetech.net>^{١٢}

٣٥٤	هل تخضعون للمراقبة على الإنترنت؟ ^{١٣}
٣٥٤	حماية المدافعات عن حقوق الإنسان ^{١٤}
٣٥٥	“دونس تيك” ^{١٥}
٣٥٥	“بلا خوف” ^{١٦}
٣٥٥	العنف على الإنترنت هو عنف أيضاً (فيديو) ^{١٧}
٣٥٥	نصائح سريعة بشأن المساحات ^{١٨}
٣٥٦	موقع “لفل أب” ^{١٩}

٣٥٧

XVIII مقدمة

٣٥٩	٦١ سياسة استخدام البيانات - ساير ويمين
٣٥٩	السياق
٣٥٩	نبذة عن المشروع
٣٦٠	الحق في الخصوصية
٣٦٠	القوانين
٣٦١	الامثال
٣٦١	التزام “ساير ويمين” بالخصوصية

<https://temboinalinha.org>^{١٣}

<http://consorciooaxaca.org.mx/proteccion-a-defensoras-de-derechos-humanos>^{١٤}

<http://donestech.net>^{١٥}

<http://sinmiedo.com.co>^{١٦}

<https://vimeo.com/207361788>^{١٧}

<https://cyber-women.com/ar/downloads/quick-tips-gender-sensitive-learning-spaces>^{١٨}

digital-security.pdf

<https://level-up.cc/>^{١٩}



النساء في فضاء الإنترنت

INSTITUTE FOR
WAR & PEACE REPORTING



مقدمة

باب ١

مقدمة

تعريف بالنساء في فضاء الإنترنت

خلال السنوات القليلة الماضية، بذلت جهود من أطراف متعددة من أجل وضع موارد ومناهج وممارسات أفضل، في مجال التدريب على الأمن الرقمي؛ إلا أن قلة قليلة من نتائج هذه الجهود ركزت بشكل كبير على منظور النوع الاجتماعي (الجندر). ومؤخراً، بفضل الجهود المبذولة من الحركات النسائية والنسوية حول العالم، بدأت بالظهور موارد خاصة بالأمن الرقمي تركز على مسألة النوع الاجتماعي (الجندر) ولكن ما زال التنسيق بين مختلف مكونات مجتمع الأمن الرقمي منقوصاً، وهو ضروري لتوسيع مجموعة الموارد بشكل إستراتيجي يلبي ويسد الحاجات اللازمة. لهذه الغاية، قام معهد صحافة الحرب والسلام^١ بوضع منهاج "النساء في فضاء الإنترنت" بغية تطبيق التقنيات والممارسات التي وضعتها المدافعات عن حقوق الإنسان، اللواتي قدن جهود التدريب على الأمن الرقمي في منطقة الشرق الأوسط وشمال إفريقيا. إستناداً إلى خبرتنا في العمل مع هؤلاء النساء، قمنا بوضع محتوى تدريبي خاص بهدف تقديم مقاربة وضعت

<https://www.facebook.com/iwpr.iraq/>^١

بالتعاون مع أطراف متعددة لتدريب المدافعات عن حقوق الإنسان على الأمن الرقمي من منظور نسوي، جندي وشامل. ولتفادي بذل الجهود ذاتها مرتين، قننا بإدخال المحتويات التي وجدنا أنها متجاوبة أصلاً مع حاجات المدافعات عن حقوق الإنسان مباشرة إلى المنهج مع ذكر مصدرها بالطبع، على سبيل الذكر لا الحصر، المحتوى المتوفر في منهاج "ليفل أب" LevelUp أو مثلاً المحتوى الموضوع من قبل منظمات مثل "تاكتيكل تكنولوجي كوليكثيف" Tactical Technology Collective وشبكة "أسوسياشن فور بروغريسيف كومينيوكاشنز" Association for Progressive Communications. إلا أن القيمة المضافة الأساسية لهذا المنهج تكمن في الوحدات الموضوعية خصيصاً له، والتوصيات المصممة بحيث توفر تجارب تعليمية مخصصة للمدافعات عن حقوق الإنسان، العاملات في بيئات خطرة.

إستخدام منهاج النساء في فضاء الإنترنت

تم تصميم هذا المنهج وفقاً لتوعين من المستخدمين: النوع الأول النساء المديرات الساعيات لتوفير تدريبات لمجموعات من النساء وعضوات هذه المجموعات حول الأمن الرقمي من منظور النوع الاجتماعي (الجندر). والنوع الثاني النساء اللواتي يسعين بعد الخضوع لمثل هذه التدريبات إلى نقل ما يعرفنه من معلومات حول الأمن الرقمي إلى شبكاتهن الخاصة من زميلات وناشطات. قد لا تكون كل الجلسات ذات أهمية لكل القارئات، ولكننا نشجعكن على تحديد تلك الجلسات التي تناسب جمهوركن الخاص والتركيز عليها.

يحتوي منهاج النساء في فضاء الإنترنت على ألعاب تفاعلية ومواد مرئية ومسموعة ومرسومة تقدم توجيهات للمدربات حيث يمكن استخدام وحدات هذا المنهج إما كجلسات مستقلة عن بعضها البعض، وإما كحكونات لورشة عمل تدريبية متكاملة. هذه التركيبة المكونة من وحدات مختلفة تتيح للمدربات أيضاً إمكانية إختيار محتويات معينة تناسب حاجات المشاركات في التدريب. من ناحية أخرى، يمكن للمدربات إختيار إتباع الترتيب المقترح للوحدات وتقديم محتوى المنهج كاملاً من بدايته إلى نهايته حيث سيستوجب ذلك تقريباً عشرة أيام كاملة. نحن ننصح اللواتي يرغبن في توفير مثل هذا التدريب، بتقسيم مواد إلى سلسلة من ورشات

العمل التي تعقد ضمن فترة لا تقل عن ستة أشهر حيث توفر هذه الطريقة للنساء المشاركات الوقت المطلوب لإدخال التقنيات والأدوات الجديدة إلى ممارسات أمنهن الرقي والشخصي، قبل الانتقال إلى تعلّم مهارات جديدة.

إضافة إلى ذلك، كجزء من تركيزه على الأمن الشامل، يتضمن المنهاج محتويات خاصة بالرعاية الذاتية النسوية. وتحديد حالات العنف القائم على النوع الاجتماعي (الجندر)، سواء كانت حالات رمزية أو رقيقة. الهدف من هذه الجلسات هو تمكين قدرة المشاركات على الفعل، وقدرتهن على التحكّم بأمنهن وهوياتهن. وبالتالي، لا بد من أن تكون هذه الجلسات موزعة على كل التدريبات كمساحات للعمل والتفكير الفردي والجماعي، عوضاً عن إستخدامها كوحدات مستقلة عن بعضها البعض.

وأخيراً، تتوفر تمارين عدّة في هذا المنهاج - بعضها تمارين خاصة ببناء الثقة يجب تنفيذها في بداية اليوم الأول من التدريب؛ وبعضها الآخر تمارين تعارف وكسر جليد بسيطة يمكن تنفيذها في بداية أي يوم من أيام التدريب. كما تتوفر تمارين عدّة مصممة بهدف تعزيز محتوى التدريب الخاص، يجب تنفيذها بالترتيب المحدد. يتضمن هذا المنهاج أيضاً موارد خاصة بجلسات المتابعة التي يجب تنفيذها ضمن فترة الستة أشهر المقترحة.

مقاربة نسوية في وضع المنهاج

كما ذكرنا آنفاً، يشمل هذا المنهاج على رؤية شاملة لمسألة الأمن للمدافعات عن حقوق الإنسان. بما في ذلك ثلاثية الأمن الرقي والأمن الجسدي والرعاية الذاتية؛ ولكن جوهر التدريب يركّز على الأمن الرقي. وإدخال مقاربة نسوية تراعي مسألة الجندر، وضع هذا المنهاج إستناداً إلى القيم والمبادئ الأساسية التالية والتي نشجّع المدربات على أخذها بعين الإعتبار عند التخطيط لورشات العمل المستندة إلى هذا المنهاج:

مشاركات ومدربات

بدايةً، صُمم محتوى منهاج "النساء في فضاء الإنترنت" بغية دعم ثقة النساء بالنساء في الأطر التدريبية. فغالباً ما تكون المشاركات في تدريبات حول الأمن الرقمي آيات من بيئات جغرافية وعاطفية فيها مستوى مرتفع من الإجهاد أو القلق؛ وغالباً ما تكون المدافعات عن حقوق الإنسان عرضة للتحرش والعنف على الإنترنت وفي الواقع. لا بد للنساء المشاركات أن يشعرن أن التدريب مكانٌ آمنٌ ومرح. يشعرن فيه أنهن قادرات على مشاركة مخاوفهن وشكوكهن وأحاسيسهن من دون قلق. ويتمكنن فيه من المشاركة والتفاعل مع الأخريات؛ لذلك، هذا المنهاج مخصص للمدربات النساء العاملات مع مشاركات نساء. ولكننا نشجع المدربين الرجال أيضاً على مراجعة هذا المنهاج ومبادئه الأساسية، من أجل تكييف ممارسات التدريب الخاصة بهم للعمل مع مجموعات مختلطة في ورشات التدريب.

النماذج النسائية والنسوية

يركّز هذا المنهاج على تقديم أمثلة عن هجمات رقمية من الواقع سبق وتعرضت لها المدافعات عن حقوق الإنسان والناشطات الحقوقيات والصحافيات بواسطة شهادات حيّة. إدراكاً منا أن جميع النساء المشاركات في ورشة عمل ما لا تعتبرن أنفسهن نسويات. تركّز مقارنة المنهاج لعملية التدريب على التوعية بشأن العنف الرقمي ضد المدافعات عن حقوق الإنسان، بدايةً عبر تسليط الضوء على الفروقات بين الهجمات المستهدفة للناشطين الرجال وتلك المستهدفة للناشطات النساء. وثانياً عبر طرح أمثلة عن العنف القائم على النوع الاجتماعي (الجنندر) على الإنترنت (مثلاً على منصات التواصل الاجتماعي) كوسيلة تدفع بإتجاه مساعدة النساء على تحديد حالات العنف التي يحتمل أنهن تعرضن لها في تلك الفضاءات. ومن ضمن هذه المنهجية، عرضنا دراسات حالات قريبة من حياة النساء اليومية، مما يسهل على المشاركات عملية فهم الحالات المختلفة وبالتالي فهم أهميتها في بيئتهن. رأينا أن اعتماد هذه المقاربة يمكن النساء المشاركات من ممارسة المهارات الجديدة بانتظام أكثر، وبالتالي تقديم المشورة بشأن

الأمن الرقمي للنساء الأخريات.

جسدي وأجهزتي وقراري!

تهدف الأفكار والمعلومات والممارسات الأساسية الموجودة في هذا المنهاج إلى خدمة عملية الترويج للإستقلالية الرقمية. من العناصر الأساسية في تصميم هذا المنهاج هو التركيز على "التفكير الإستراتيجي بشأن الأمن الرقمي" - أي مشاركة مفاهيم في مجال الأمن الرقمي مع المشاركات، عوضاً عن الإكتفاء بالتدريب على لأئحة من الأدوات. لذلك حُصص وقت طويل جداً لتعريف المشاركات بمفاهيم الأمن الرقمي، كالشفير وإخفاء الهوية والخصوصية والبرمجيات المفتوحة المصدر قبل التدرّب على إستخدام الأدوات المرتبطة بها. وعبر دعم النساء في عملية تحديد فهمهن الشخصي لهذه المفاهيم، سيغادرن التدريب وفي جعبتهن المعلومات اللازمة التي تمكنهن من إتخاذ قراراتهن الخاصة بشأن الأدوات الأفضل لهن.

تحليل المخاطر القائمة على الجندر ووسائل التواصل الاجتماعي من خلال الإستعانة بأمثلة من فيديوهات يوتيوب ورسائل من منصات تواصل إجتماعي متعددة ومخرجات ناتجة عن جلسات تدريبية أخرى، يهدف هذا المنهاج إلى توفير مساحة آمنة للنقاش والتفكير في العنف القائم على التكنولوجيا الذي يستهدف النساء تحديداً. وبشكلٍ خاص، تجدن كل هذه الأمثلة في وحدة العنف على الإنترنت ضد النساء؛ وتمرين نماذج المخاطر القائمة على الجندر الموجود في وحدة تحديد الحل الأفضل التي تركز على مشاركة التجارب وتحديد نقاط الضعف التي تواجهها المشاركات ليس فقط لكونهن نساء بل أيضاً بصفتهن مدافعات عن حقوق الإنسان.

الرعاية الذاتية النسوية والدفاع الرقمي عن النفس

كجزء من المقاربة الشاملة للأمن، يعتبر هذا المنهاج أن الرفاه النفسي والرعاية الذاتية عنصران أساسيان من عناصر أمن المدافعات عن حقوق الإنسان؛ وكذلك كجزء من التركيز على الإستقلالية الرقمية حيث تتوفر جلسات خاصة - كجلسة نموذج المخاطر القائمة على الجندر التي

تصلح كمثال أيضاً في هذه الحالة - الهدف من هذه الجلسة مساعدة المشاركات على الإستعداد والتعامل مع الهجمات الرقمية. يأتي هذا المنهاج ليساعد في تقديم معلومات للمشاركات لتمكّن من تحديد إستراتيجيات عدّة وإستكشافها خاصة بدفاعهن الرقمي عن أنفسهن؛ على سبيل الذكر لا الحصر، فصل الحيز الشخصي عن الحيز العام، إنشاء هويات على الإنترنت، الاستقصاء عن المعلومات الشخصية الخاصة بالمتصيد أو المتحرش، تشفير اتصالاتهن وتوثيق الحوادث الرقمية، وعبر تزويد المشاركات بفهم أفضل لبيئتهن الرقمية - من خلال كلا من المنصات التي يستخدمونها والمخاطر المتعلقة بكل واحدة منها - يمكننا تمكينهن من إعتقاد عادات جيدة في مجال الأمن الرقمي، قد تصبح بدورها جزءاً من ممارسة شاملة للرعاية الذاتية.

باب ٢

تخطيط الموارد

من الخطوات الأساسية في عملية التخطيط للتدريب، جمع نقاط البيانات اللازمة لوضع جدول عمل التدريب، حيث من شأن ذلك إكتساب فهم جيد لحاجات الأمن الرقمي الخاصة بالمشاركات والمساعدة في ضمان توفير تدريب فعّال وتجربة تعلّم لكل ما هو مناسب لأهداف وبيئة المشاركات. من شأن معرفة كيفية إستخدام المشاركات المحتملات للتكنولوجيا، وكيفية تواصلهن بواسطتها وتحديد ما يعرفه مسبقاً عن الأمن الرقمي، أن تؤثر بشكلٍ ملحوظ على نطاق المحتوى المقدم في التدريب.

تقييم الحاجات والمحفزات

يفضّل أن تجري المدربات تقييماً للحاجات قبل التدريب، من خلال العمل إما مع المشاركات في التدريب أنفسهن وإما مع عضوة ممثلة لمنظمتهم. لا تنسوا أنه إلى جانب ضرورة تقييم حاجات المشاركات بشكلٍ موضوعي، لا بد أيضاً من فهم محفزات مشاركتهن في التدريب -

هل تسعى المشاركات بشكلٍ فاعل لتحسين قدرتهن على الصمود، وأأنهن يطلبن المساعدة نتيجة حوادث تعرضن لها مؤخراً أو ما زالت مستمرة؟ إضافة إلى ذلك، من وجهة نظر عملية، من شأن معرفة الوقت المتوفر لديكن أن يساعدكن في النهاية على تحديد كم المحتوى الذي ستقدمنه في ورشة عمل واحدة (أوورشات عمل متتالية)؛ وسيوضح ذلك لكن أكثر بفضل مستوى المهارات الجماعي للمشاركات.

في حال توفرت لكنّ فرصة التفاعل والتواصل مع المشاركات بشكلٍ معمق قبل التدريب، ستجدن في ما يلي بعض الأسئلة الواجب طرحها والتي قد تساعدكن على التعرف عليهن و/أو على المنظمة التي يعملن فيها:

ما هي خلفية منظمتهن؟ ما شكل تنظيم فريق عمل منظمتهن؟ ما هي البرامج و/أو النشاطات الأساسية التي تنظمها منظمتهن؟ ما هي بعض الممارسات المرتبطة بالتكنولوجيا التي يعتمدنها؟ كيف ومن أين يحصلن على الإنترنت؟ ما هونوع وأنواع الحواسيب و/أو الأجهزة المحمولة التي يستخدمنها؟ هل يستخدمن أجهزة منفصلة للعمل والإستعمال الشخصي؟ ما هي أنظمة التشغيل التي يستخدمنها؟ من هي الحركات أو المجموعات الأخرى التي يتعاونن معها؟ قد يتم ذلك من خلال ممثل لمنظمتهن (مثلاً كأعضاء تحالف ما) أو بصفة شخصية كاشطات مستقلات. هل سبق لهن أن تعرضن لحوادث أو تهديدات مباشرة لأمنهن الجسدي أو الرقمي؟ قد يرتبط ذلك بأجهزتهن أو بمعداتهن أو بحساباتهن الإلكترونية أو بإعتداء جسدي.

أداة بناء قدرات الأمن الرقمي Digital Security and Capacity (DISC) Tool

في حال أتجحت لكنّ فرصة إجراء عملية تقييم شاملة للمشاركات في التدريب في الوقت الذي يسبق ورشة عملكن، سوف تتوفر أداة بناء قدرات الأمن الرقمي ضمن هذا المنهاج. هذه الأداة مورد قام المعهد بإنتاجه وإستخدامه مرّات عدّة عند إجراء عمليات تقييم تسبق التدريبات على الأمن الرقمي.

أداة بناء قدرات الأمن الرقمي عبارة عن إستمارة تقييم في مرحلة ما قبل التدريب، تستعين بألية إحتساب كمي لإختبار المشاركات، من أجل تحديد مستوى مهاراتهم في مجال الأمن الرقمي من جهة، ومن جهة أخرى توفر معلومات نوعية عن نقاط القوة والجلالات التي يجب تحسينها بشكلٍ مفصّل على المستوى العملي. في حال كنتن ستعملن مع مشاركات على مراحل (مثلاً، إجراء ورشات عمل عدّة على مدى ستة أشهر)، تعتبر أداة بناء قدرات الأمن الرقمي طريقة مفيدة في تعقّب تقدّم تعلمهنّ وفهمهنّ.

أداة بناء قدرات الأمن الرقمي بنسختها الكاملة متوفرة في الملاحق¹

إستراتيجيات التقييم البديلة

في حال العجز عن إجراء عملية تقييم قبل التدريب بشكلٍ مباشر، أو في حال لم تحصلن على الأجوبة على هذه الأسئلة، لا يزال بإمكانكن الحصول على بعض المعلومات الأساسية من خلال ما تعرفنه عن بيئة وظروف المشاركات:

على سبيل المثال، في حال كنتن تعرفن أن النساء الناشطات، أو المنظمات يجرين عملاً مشابهاً في المنطقة ذاتها التي تعمل فيها المجموعة أو المجموعات التي ستعملن معها، سيكون من المرجح أنها تواجه مخاطر أو هجمات مشابهة في طبيعتها لتلك التي تواجهها المشاركات في تدريبيكن. إضافة إلى ذلك، قد تتوفر بعض المخاطر أو الحوادث المعروفة التي يمكنكن ربطها بنوع العمل الذي تقوم به المشاركات في تدريبيكن (وبمكان قيامهن به). في حال كنتن ستدرين محاميات توفرن المشورة القانونية لمدافعات أخريات عن حقوق الإنسان، أو لصحافيات يفضحن فساد الحكومة، قد تتمكنن من إجراء بحوث حول بعض التكتيكات التي تستخدمها أو استخدمتها الحكومات أو بعض الجهات غير الحكومية في بلدنّ في الماضي ضد أفراد، ولا سيما النساء ممن يقمن بعمل مشابه.

¹<https://cyber-women.com/ar/DISC/>

باب ٣

شكر وتقدير

الكُتّاب: كُتِبَ المحتوى الأصلي لهذا المنهاج من قبل ألما أوغارتي بيريز وهيدمي سييرا كاسترو وإنديرا كورنيليو فيدال.

تنسيق وتنظيم: ألما أوغارتي بيريز وهيدمي سييرا كاسترو وإنديرا كورنيليو فيدال ودانيالا فالك

تنسيق وتنظيم النسخة العربية: عزة سلطان و علي سباعي و محمد المسقطي

التنسيق وصلة التواصل مع معهد صحافة الحرب والسلام: أليخاندر غارسيا

التعليم والمواءمة مع السياق المحلي: نيكولاس سيرا-لييفا و عزة سلطان

الترجمة إلى الإسبانية: ناديچ لوكاس بيريز

الترجمة إلى اللغة العربية: زياد فران و داؤد ابراهيم

تنسيق التعلّم من الند للند والجلسات التجريبية: إستيلا سوريا

خدمات إستشارية: تعاونية تييرا كومون^١

تطوير الموقع وتصميم الرسوم وإنتاج الوسائط: تعاونية كيفير^٢

المراجعات والمتعاونات: عرّة سلطان، كارول واترز، داليا عثمان من تعاونية تاكتيكل
تكنولوجي وإستريلا سوريا، إريكا سميث من جمعية "بروغريسف كوميونيكاشنز"، جييجي
ألفورد، جينيفر شولتي، لورا كوينغهام، ليندسي أندرسن، ميغان دويلوا من إنترنيوز وساندرا
أوردونيس.

تم تطوير بعض الجلسات والمعلومات الأخرى في هذا المنهاج من قبل: جمعية "بروغريسف
كوميونيكاشنز"، تعاونية تاكتيكل تكنولوجي، مؤسسة كاريزما، "موخيريس آل بوردي"، إليس
موروي من تعاونية "سوفيرسيونس"، دانا بويد، مارييل غارسييا، أليكس دون، سبيروس
موناستيريو تيس، في.

<https://tierracomun.org/>^١

<https://kefir.red>^٢



النساء في فضاء الإنترنت



تمارين بناء الثقة

باب ٤

قواعد اللعبة

- الأهداف: في هذا التمرين، ستتمن بشكلٍ جماعي بوضع اتفاقات التعايش والمشاركة الخاصة بتدريبيك أي "قواعد اللعبة" مع المشاركين.
- الطول: من 8 إلى 10 دقائق
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
 - بينغو المدافعات^١
 - الحلوى المخادعة^٢
- المواد اللازمة:
 - لوح ورقيّ (ألواح أسود أو أبيض)
 - أقلام خطاطة
 - ملصقات ملوّنة (ثلاثة ألوان - يفضل أن تكون الأحمر والأزهر والأصفر)

^١ <https://vrr.im/cf95>

^٢ <https://vrr.im/ff57>

والأخضر

- التوصيات: الجزء الثاني من هذا التمرين - "إشارات السير" - ينفذ بشكل أفضل إذا كانت المشاركات مزودات ببطاقات عليها أسماءهن يمكنهن وضع الملصقات الملونة عليها (راجع الإرشادات).

إدارة التمرين

على الرغم من أن علاقة مسبقة من نوع ما تربط عادةً كل من المشاركات ببعضهن البعض ولكن أنتن كمدربات، لا بد في أي عملية تدريبية من وضع إتفاقات تعايش متفق عليها من جميع الأطراف (سنسميها "قواعد اللعبة") تضمن بيئة مريحة يسودها الإحترام لكل المشاركات.

التجربة الحياتية والبيئة الثقافية الخاصة بكل امرأة فريدة من نوعها، وما قد يعتبر غير مهين أو مؤذٍ نهائياً لواحدة منهن قد يفسر بطرق مختلفة من قبل الأخرى. من شأن إتفاقات التعايش الموضوعة بشكلٍ جماعي أن تساعد في ضمان إحترام وإحترام التدريب لوجهات النظر المختلفة هذه وللمساحات الشخصية المألوفة المختلفة؛ على سبيل المثال، بعض النساء لا يشعرن بالإرتياح تجاه التماس الجسدي، في حين أن الأخرى قد يستخدمن ذلك كطريقة للتعبير عن أنفسهن. ولا تنسوا أيضاً على سبيل المثال أن بعض المشاركات الآتيات من خلفية تربوية تقليدية قد يشعرن بأنه عليهن طلب إذن لقضاء حاجتهن، في حين أن الأخرى قد يعتبرن أنه من الطبيعي جداً مغادرة الصالة بكل بساطة لقضاء هذه الحاجة. ستساعدكن هذه الجلسة في إنشاء إتفاقات التعايش الجماعية هذه التي من شأنها الإقرار بخيارات المشاركات مما سيسمح لهن بالشعور بالإرتياح وبالتالي سيكون أكثر إنفتاحاً على المواد التي يفترض أن يتعلمنها طيلة فترة الورشة.

الجزء الأول - قواعد اللعبة

1. إشرحن بإقتضاب الخلفية المذكورة أعلاه للمشاركات، ومن بعدها أطلبن منهن تقديم أمثلة عن إتفاقات تعايش يشعرن أنها مهمة وضرورية لضمان راحتهم طيلة فترة ورشة

العمل. يمكننا البدء بمثال تقدمه أنتن - من قبيل "نحن لا نحتاج لإذن للذهاب لقضاء الحاجة" أو "لن نقوم بمشاركة أي شيء عن هذا التدريب على وسائل التواصل الاجتماعي من دون الحصول على إذنك".

٢. على لوح ورقي أو لوح أسود أو أبيض، أكتبين كل إتفاق ننتق عليه المجموعة فوراً، وما أن تشعرن بأنها كافية، إقرأن كل الإتفاقات بصوت عالٍ - إستلن المشاركات إن كانت قواعد التعايش الخاصة بالمجموعة هذه تناسبهن. ما لم يُذكر ذلك سابقاً أو في حال عرضين ذلك كمثال أولي عن الإتفاقات هذه، من شأن الإتفاق حول إستخدام الحواسيب والهواتف خلال الجلسات أن يساعدكن أيضاً.

٣. ذكرن المجموعة بأن هذه الإتفاقات ستنقى معروضة وواضحة طيلة فترة التدريب، وأنهن قادرات على تعديلها في أي وقت كان بعد المناقشة والإتفاق على ذلك مع كافة أعضاء المجموعة. إحرصن أيضاً على إعطاء المشاركات خيار تقديم الإقتراحات مباشرة إليكن أو من دون الكشف عن هويتهن، في حال لم يشعرن بالإرتياح للقيام بذلك بشكل علني.

الجزء الثاني - "إشارات السير"

٤. بعض الإتفاقات على لأثحتكن قد توفر مستويات متفاوتة من الراحة ضمن المجموعة. بالنسبة لهذه الإتفاقات، تلك المرتبطة بالتماس الجسدي أو التصوير، يفضل أن تقدمن للمشاركات طريقة لتحديد معايير الراحة الخاصة بهن لمشاركتها مع بعضهن البعض.

٥. وزعن المصصقات الملونة لكل مشاركة من المشاركات، مع الحرص على إعطائهن مصصقات عديدة من كل لون. إشرحن لهن أن المجموعة ستقوم بتمرين صغير اسمه "إشارات السير" لبعض اتفاقات التعايش الموجودة على اللائحة (حددن الاتفاقات التي تقصدنها).

٦. من خلال الإستعانة بمثال عن إتفاق مرتبط بالتماس الجسدي ينص على: "قبل المباشرة بأي تماس جسدي مع مشاركة أخرى، علينا أن نحرص أن ذلك لا يضايقها" أو ما شابه، على المجموعة تحديد معنى لكل ملصقة ملونة مرتبطة بذلك الإتفاق - على سبيل المثال:

الأحمر/الزهري: “التماس الجسدي يضايقيني قليلاً، الرجاء إحترام ذلك”
الأصفر: “لا أمانع التماس الجسدي ولكن أطلبن الإذن مني أولاً.”
الأخضر: “لا أمانع التماس الجسدي على الإطلاق.”

٧. على المشاركات عندها إختيار ملصقة ملونة خاصة بهن تناسب والتعريف المتفق عليه، والذي يتطابق مع مستوى راحتهن الشخصية. ومن ثمّ لصقها على بطاقات أسمائهن. لا حاجة لأن تطلبن من كل مشاركة إخبار الجميع عن اللون الذي اختارته فالجميع قادر على رؤية الألوان التي اختارتها الأخريات.

٨. أكتبن التعريفات والألوان على ورقة جديدة على اللوح الورقي لكل قاعدة سينطبق عليها ذلك - لا يجب أن يتجاوز عددها الإثنان أو ثلاثة. في حال وجود أكثر من إثنين أو أكثر، أطلبن من المشاركات كتابة حرف خاص بكل واحدة منها (مثلاً: “تاء” للتماس الجسدي أو “صاد” للصور).
المراجع:

باب ٥

بينغو المدافعات

- الأهداف: ستبدأ أنتن والمشاركات بالتعريف عن أنفسكن لبعضكن البعض في تمرين كسر الجليد هذا، المصمم على شكل لعبة تفاعلية تشجع المشاركات على التعرف على بعضهن البعض بدون الإكتفاء بمعرفة الأسماء.
- الطول: من 12 إلى 15 دقيقة (وفقاً لعدد أعضاء المجموعة)
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
 - الحلوى المخادعة^١
 - المواد اللازمة:
 - جداول بينغولكل مشاركة (معبئة مسبقاً بأسماء المشاركات)
 - بطاقات كرتون بيضاء
 - أقلام/أقلام رصاص (العدد الكافي لكل المشاركات)

^١<https://vrr.im/ff57>

إدارة التمرين

قد تكون عملية تذكر الأسماء والتعرّف على الوجوه عملية صعبة بالنسبة لبعض الأشخاص مقارنة بالأشخاص الآخرين. تمرين "كسر الجليد" هذا سيساعد المشاركات على تذكر هذه التفاصيل وفي الوقت عينه سيتيح لمن التعرف بشكل أفضل على من سيعملن معهن طيلة فترة التدريب!

١. أطلبن من كل المشاركات كتابة أسمائهن على بطاقة كرتون بيضاء ومن ثمّ إجمعنها ما إن ينتهي الجميع من الكتابة.

٢. بعدها، وزعوا أوراق البينغو على الجميع التي أعدت مسبقاً بأسماء كل المشاركات (راجعن المثل الوارد أدناه) - يمكنكن أيضاً إضافة أسماء وكن على الأوراق إذا أردتن ذلك. مثال عن ورقة بينغو معدة مسبقاً:

شميرة	زينة	شفيفة
فاطمة	منى	جوليت
صوفيا	فرح	نهي
ليلي	سارة	ماريا

٥٣. إشرحن للمجموعة قواعد سير اللعبة:

ستقرآن بصوت عالٍ، واحدة تلو الأخرى، محتوى بطاقات الكرتون التي كتبت فيها المشاركات أسماءهن؛

أثناء قراءة تكن للأسماء، ستقوم المشاركات بوضع دائرة حول كل إسم وارد على أوراق البيبنغو الموجودة معهن.

المشاركة الأولى التي تنتهي من وضع دوائر على سطر أفقي أو عمودي من الأسماء عليها أن تصرخ كلمة "بيبنغو!" وستعلن الفائزة.

٤. أطلبين من الفائزة قراءة اسم المشاركة الأولى من الصف الرابع بصوت عالٍ - على المشاركة المذكورة الوقوف وترداد أسمها ومن ثم إضافة تفصيل ما (اخترن هذا التفصيل مسبقاً وأطلعنهن بذلك كجزء من إرشاداتكن) على سبيل المثال نشاط تحب أن تقوم به في أوقات فراغها، أو فيلها المفضل أو أغنيها المفضلة أو طبقها المفضل، إلخ.

٥. ستكرر الفائزة العملية ذاتها في الخطوة رقم 4 إلى أن تقوم كل مشاركة يرد اسمها في السطر الفائز بالتعريف عن نفسها. وفي الوقت عينه الذي ينادى فيه كل اسم، خذن بطاقة كرتون مطابقة من الرزمة التي إستخدمتها في الخطوة رقم 3 وضعنها جانباً.

٦. بعد أن تنتهي الفائزة من منادة الأسماء الواردة في السطر الفائز، إشكرنهن ومن ثم إقرآن الأسماء الواردة على بطاقات الكرتون المتبقية لديكن لكي تتسنى لكل المشاركات فرصة التعريف بأنفسهن أمام المجموعة.

٧. ما أن تنتهي كل المشاركات من التعريف بأنفسهن، سيحين دوركن! رددن اسمكن للمجموعة وشاركن تفصيلاً ما عن أنفسكن وأيضاً إختتمن الترين بتذكير المجموعة بأنكن ستبدأن بحوض غمار مغامرة جديدة معاً، وأن معرفة والتعرف على كل عضوة من عضوات المجموعة ضروري لضمان نجاح مغامركن.

إختياري: بنهاية الترين، إمنحن كل مشاركة ورقة لاصقة بيضاء وقلم خطاط لكي يتمكن من كتابة بطاقة اسمهن - من شأن ذلك أن يساعد المشاركات على تذكر أسماء بعضهن

البعض من جهة، ومن جهة أخرى يساعدكن أيضاً على ذلك (وهذا عنصر إيجابي
دوماً في عملية التدريب!)

باب ٦

الخلوى المخادعة

- الأهداف: ستبدأ أن تتن والمشاركات بالتعريف عن أنفسكن لبعضكن البعض خلال تمرين كسر الجليد هذا، المصمم على شكل لعبة تفاعلية تشجع المشاركات على التعرف على بعضهن البعض بدون الإكتفاء بمعرفة الأسماء.
- الطول: من 5 إلى 8 دقيقة (وفقاً لعدد المشاركات في المجموعة)
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
- جلسات/تمارين ذات صلة:
 - قواعد اللعبة^١
- المواد اللازمة:
 - كيس أو كيسين من قطع الخلوى الصغيرة

^١<https://vrr.im/e441>

إدارة التمرين

١. قدم الحلوى لكل المجموعة وقلن لهن أن يأخذن ما طاب لهن منها. بعض المشاركات ستأخذن عدداً كبيراً والبعض الآخر ستأخذن عدداً أقل. ويمكنكن أيضاً أخذ بعضٍ من الحلوي.

٢. ما إن يأخذ الجميع بعضاً من قطع الحلوى، إكشفن عن "الخدعة" للجميع ، حيث لكل قطعة أخذتها، عليهن مشاركة صفة شخصية واحدة أو تفصيل مثير للإهتمام عنهن مع بقية المجموعة. قد تكون هذه التفاصيل أو الصفات ما يلي:

أمنيات أو أهداف شخصية

أمر ما يمتعن به في عملهن

بلد أو مكان يرغبن في زيارته

إختياري: في حال توفرت لديكن تشكيلة متنوعة من قطع الحلوى، أو قطع حلوى مغلقة بألوان مختلفة، عندها يمكنكن تحديد فئة معينة لكل نوع أولون. وبواسطة الغلافات الملونة مثلاً، يمكنكن القيام بما يلي:

الغلاف الأحمر = أمنيات أو أهداف شخصية

الغلاف الأخضر = أمر ما يمتعن به في عملهن

الغلاف الأزرق = بلد أو مكان يرغبن في زيارته

باب ٧

بمن نشقن

- الأهداف: في هذا التمرين، ستوجهن المشاركات في عملية تفكير يهدف تحديد الحلفاء والخصوم المفترضين في كل بيئة من بيئاتهن الفردية. سيساعدكن تحديد الحلفاء والخصوم في هذا التمرين السريع في تسيير تدريب ملائم أكثر لمشاركاتكن، بما أنكن ستتمكنن من مواءمة محتوى الجلسات المختلفة بشكل أفضل مع بيئاتهن الخاصة.
- الطول: 15 دقيقة
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
 - نموذج المخاطر القائمة على النوع الاجتماعي^١
 - الخطط والبروتوكولات الأمنية الخاصة بالمنظمة^٢
 - خطط وبروتوكولات الأمن الرقمي: إعادة تنفيذها بعد التدريب^٣

<https://vrr.im/c0c31>

<https://vrr.im/f75c2>

<https://vrr.im/60273>

- المواد اللازمة:
- أوراق كبيرة متعددة من أوراق اللوح الورقيّ.

إدارة التمرين

- ٠١ إعطين كل مشاركة ورقة من أوراق اللوح الورقيّ، وإعطين المجموعة الجملة التالية كمقدمة لوضع التمرين في سياقه الصحيح:
لا أحد يثق بالجميع، ولكن لا أحد لا يثق بشخصٍ واحدٍ على الأقل
- ٠٢ إعطين الجميع 5 دقائق للإجابة عن الأسئلة التالية بشكلٍ فرديّ، وأثناء قيامهن بذلك، أطلبن منهن أيضاً تحديد ما إذا كانت إجابتهن على كل سؤال ستتغير إذا أُجبن عليها في بيئتهن الشخصية في مقابل الإجابة عنها في سياق عملهن/نشاطهن:
بن ثقفن؟
بن تعتقدن أنكن قادرات على الوثوق في ما يتعلق بمعلوماتكن؟
بن تعتقدن أنكن غير قادرات على الوثوق في ما يتعلق بمعلوماتكن؟
من هي الجهات التي تعتقدن أنها تتجسس عليكن؟
من هي الجهات التي تعتقدن أنها لا تتجسس عليكن؟
الأمثلة عن أشخاص أو خصوم قد يذكرون في الإجابات تشمل الجهات الحكومية (مثلاً: الأجهزة الأمنية الحكومية)، الشركات الخاصة (مثلاً فايسبوك أو غوغل)، مقدمو خدمات الإنترنت، الشركاء/ات والأصدقاء/ات المقربون أو حتى الزملاء/ات.
٠٣ ما إن ينتهي الوقت المخصص، قسمن المشاركات إلى مجموعات صغيرة من 3 إلى 4 أشخاص كحد أقصى لمناقشة إجابتهن مع بعضهن البعض - بعد مرور 10 دقائق، على كل مجموعة أن تشارك مع المجموعات الأخرى ما ناقشته.

٤. والآن، يمكننا إختتام التمرين شارحات أنه خلال هذا التدريب - إستناداً إلى الخصوم الذين بدأت المجموعة بتحديدن في هذا التمرين - أنكن ستصبحن قادرات على تسليط الضوء على الممارسات والأدوات التي تعتبر أكثر مواءمة وصلة ببيئاتهن الخاصة.



النساء فى فضاء الإنترنت



إعادة النظر بعلاقتنا
بالتكنولوجيا

باب ٨

وجهات النظر الشخصية حيال الأمن

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

<https://vrr.im/bd0d1>

<https://vrr.im/11512>

<https://vrr.im/c0c33>

- أوراق مسطرة أو غير مسطرة بقياس (أ4) (إعطين أكثر من ورقة واحدة لكل مشاركة)
- شرائح (فيها النقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
- أوراق اللوح ورقية

إدارة التمرين

الجزء الأول - ما هي السلامة بالنسبة لكن؟ ما هو الأمن بالنسبة لكن؟

١. أطلب من المشاركين توزيع أنفسهم على مجموعات من 3 إلى 4 مشاركات كحد أقصى، وإعطينهم 15 دقيقة لمناقشة الأسئلة التالية مع بعضهم البعض:

ما هي السلامة بالنسبة لكن؟

ما هو الأمن بالنسبة لكن؟

ما الذي يجعلك تشعر بالأمن والأمان؟

في أي مجالات تعتقد أنه يمكن تطبيق هذين المفهومين؟

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

٢. بعد ذلك، عرف المشاركين بواسطة شرائح معروضة أو أوراق اللوح الورقي بالمقارنة الشاملة للتدريب. إحرص على شرح أهمية الأمن الرقمي والرعاية الذاتية والأمن الجسدي بالنسبة للعملية الشاملة (يمكنك الاستعانة أو نسخ الرسم البياني التالي كطريقة بسيطة لشرح ذلك):

٣. في الكثير من الحالات، يتحمل أن تعمل مع مشاركات يحضرن التدريب من أجل

عناصر الأمان الشامل الثلاث

الأمان الرقمي



الرعاية الذاتية الأمان الشخصي

عناصر الأمان الشامل الثلاث

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

الجزء الثاني - ما هو الأمن الرقمي بالنسبة لكن؟

٤. أطلبين من كل مشاركة التفكير في ما تعني لها مسألة الأمن الرقمي. وأطلبين منهن أن يعملن كل واحدة وحدها على تدوين بعض الجمل يشرحن فيها مفهومهن الشخصي لها. وقبل أن يبدأن بذلك، إشرحن لهن - بحسب الظروف كالتجربة الشخصية أو الأولويات أو القضية/النشاط أو بلد الأصل - أن معنى المفاهيم الخاصة بهن قد تختلف من شخص لآخر (وقد تشمل عناصر أخرى كـ بعض القيود القانونية،...إلخ). ولمساعدة كل متدربة على تطوير مفهومها الخاص، يمكنكن البدء بإطلاعهن على مفهومهن الخاص على سبيل المثال.
٥. ما إن ينتهي الوقت المخصص لذلك، إسألن المشاركات ما إذا كنّ راغبات في مشاركة ما كتبنه مع بقية المجموعة - ليس من الضروري أن تشاركن جميعهن ما كتبن، فبعضهن قد لا تشعرن بالضرورة بالراحة إذا قن بذلك.
٦. من بعد قيام بعض المتطوعات بمشاركة مفاهيمهن، سلطن الضوء على بعض العناصر الأساسية التي قدمنها، كعادتنا وأجهزتنا والشبكات والمجموعات التي ننتمي لها والبيئة التي نعيش فيها والمعلومات التي نمتلكها ومكان تخزيننا لها. وإشرحن للمشاركات أن الأمن الرقمي مرتبط بنا كأفراد وكبشر قبل أي إعتبار آخر (لا سيما الأدوات والتكنولوجيا).

الجزء الثالث - تحديد الحوافز وأسباب الرفض والحوافز

٧. بعد تقسيم المجموعة إلى مجموعات صغيرة من 3 إلى 4 مشاركات كحد أقصى، أطلب من المشاركين مناقشة حوافزهم ومخاوفهم والحوافز الموجودة بالنسبة لمن المرتبطة بمسألة الأمن الرقمي عبر الإجابة عن الأسئلة التالية:

ما السبب الذي يدفعهم للتعرف أكثر على مسألة الأمن الرقمي؟

ما هي الأسباب الشخصية التي دفعتهم لحضور ورشة العمل؟

ما الذي يتوقع الحصول عليه من هذا التدريب؟

هل لديهم أسباب شخصية تدفعهم إلى رفض الأمن الرقمي؟

ما هي التحديات التي واجهتها في التعلم عن الأمن الرقمي؟ أو ما الذي يشعرون أنه منعهن من تعلم ذلك من قبل؟

٨. ما أن ينتهي الوقت المخصص لذلك، أطلب من كل مجموعة مشاركة أفكارها ومناقشاتها مع الأخريات - كمدربات، هذه لحظة مهمة لأنه من أجل مواءمة جلسات تدريبيكن بطريقة مرتبطة فعلاً ببيئة مشارككن، لا بد لكن أن تتبين جيداً للحوافز وأسباب الرفض والحوافز المحددة التي تشاركها المشاركات.

الجزء الرابع - المعتقدات الخاطئة المتداولة بشأن الأمن الرقمي والجنذر والتكنولوجيا

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

٠١ "الأمن الرقمي صعب".

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

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

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

في الواقع، معظم ممارسات الأمن الرقمي الأساسية والجوهرية لا تعتمد كثيراً على أدوات الأمن الرقمي. فتغيير كلمات السرّ الخاصة بحساباتكن بشكل دوري، والتحقق من إعدادات الخصوصية الخاصة بالحسابات التي تستخدمها أصلاً، وحماية أجهزتك بكلمات سرّ والقيام بنسخ احتياطية بشكل دوري لبياناتكن، ممارسات مرتبطة بعاداتكن وسلوككن أكثر مما هي مرتبطة بالتكنولوجيا والأدوات بذاتها.

مسيرة الأمن الرقمي التي سنبدأ بنحوض غمارها الآن، هدفها تزويدكن بالمعلومات التي تحتاجن إليها لإتخاذ القرارات الصحيحة المناسب بشأن أمنكن الرقمي والتي تركز بشكل أكبر على تعلم المزيد عن المنصات التي تستخدمها أصلاً، وتداعيات

اختيار أدوات أو ممارسات معينة على أنفسنا وعلى عملنا، وعلى تحسين الطرق التي نستخدم فيها التكنولوجيا في حياتنا اليومية.

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

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

٤. “لا أعرف شيئاً عن الأمن الرقمي!”

قد يفاجئكن ذلك، ولكن معظمنا سبق له أن فكّر في ممارساتنا من دون إدراك ذلك - على سبيل المثال، عدد لا بأس به منكن يستخدم كلمات السرّ لحماية هواتفكن أو حواسيبكن المحمولة أصلاً؛ وقد يستخدم بعضكن تطبيقات أو أدوات مختلفة للتواصل مع الآخرين بشأن مسائل معينة؛ وعدد قليل منكن قد تستخدم أسماء مستعارة أو هوية منفصلة للعمل عن تلك التي تستخدمها في حياتهن الشخصية.

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

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

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

الأمن الرقمي لا يقتصر فقط على ما تقمن به على الإنترنت - فالممارسات خارج الإنترنت، كالإطلاع بشكلٍ دوري على المعلومات (الأرقام والصور والمستندات والملفات الصوتية وملفات الفيديو... إلخ) التي خُزنت من قبلكن على حاسوبكن وهواتفكن الذكية (و“غير” الذكية) ومفاتيح اليواس بي، بالإضافة إلى الإدراك الجسدي لمكان وجود أجهزتك أو لمن لديه إمكانية الوصول إليها مهمة بالقدر ذاته - حتى لو لم تكن متصلة بالإنترنت. لا بد أيضاً من معرفة التطبيقات والبرمجيات المثبتة على أجهزتك - لأنه أحياناً، من أجل الوصول إلى معلومات معينة على الأجهزة، قد نضطر لتثبيت تطبيقات جديدة أو إنشاء حسابات جديدة من دون أن ندرك.

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

كما ورد في الشرح المقدم في مشروع “تاكتيكل تكنولوجيا” - Tactical Tech nology “أنا وظلي” [1]:

الخصوصية ليست إختباء - بل هي إستقلالية وقوة وقدرة على التحكم؛ هي مرتبطة بقدرتك على اختيار كيف تقدمن أنفسكن للعالم

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

بطريقة أو بأخرى، نتخذ قرارات بشأن أنواع المعلومات التي نشاركها ومع من نشاركها كل يوم. عليكن أيضاً الأخذ بعين الإعتبار أنه قد لا يوجد الآن شيء تخفيه، ولكن قد يتغير ذلك في المستقبل - لذا قد ترغبين في الإستعداد لهذه الإمكانية!

هل شعرتن يوماً باليأس أو الانكسار لدى سماعكن عن المراقبة الرقمية أو تكتيكات التحرش الرقمي المستخدمة من قبل الحكومات أو المجموعات الأخرى ضد المدافعات عن حقوق الإنسان؟ طبعاً في سياق نشاطاتكن، من الطبيعي أن تواجهن مثل هذه اللحظات، وليس فقط في سياق الأمن الرقمي أو التهديدات على الإنترنت - لهذا السبب سنبدأ هذه العملية الشاملة. معاً سنبنين مقارنة من مستويات متعددة تساعدنا على حماية أنفسنا وحماية معلوماتنا.

الجزء الخامس - الملاحظات الختامية

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

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

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

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

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

والأدوات التي سيطبقنها خلال تقدمكن معاً في المسيرة التدريبية. يجب أن تتضمن مثل هذه الخطط الأهداف الشخصية التي ستشجعهم على التقدّم بسرعتن الخاصة.

المراجع

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

باب ٩

حقوقن والتكنولوجيا الخاصة بكن

- الأهداف: يتخلل هذه الجلسة نقاش حول العلاقة بين الحقوق والتكنولوجيا - ستساعدن حينها المشاركات على تحديد التهديدات المحدقة بحقوقهن ومن ثم سيتعرفن على بعض مفاهيم الأمن الرقمي الأساسية ذات الصلة.
- الطول: 50 دقيقة
- الشكل: جلسة
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- بمن نثقن?^١
- وجهات النظر الشخصية حيال الأمن^٢
- كيف يعمل الإنترنت?^٣
- الخصوصية^٤

<https://vrr.im/bd0d1>

<https://vrr.im/93392>

<https://vrr.im/7ba93>

<https://vrr.im/819e4>

- المحافظة على سرّية الهوية^٥
- تعريف بمسألة التشفير^٦
- إنترنت نسوي^٧
- المواد اللازمة:
 - أوراق لوح ورقّي.
 - أقلام خطاطة ملوّنة
 - نسخ عن تقارير ومقالات عن الحقوق الرقّية من بلدان أو مناطق المشاركات (نسخة واحدة لكل 3 إلى 4 مشاركات)
 - التوصيات: أوراق لوح ورقّي. أقلام خطاطة ملوّنة نسخ عن تقارير ومقالات عن الحقوق الرقّية من بلدان أو مناطق المشاركات (نسخة واحدة لكل 3 إلى 4 مشاركات)

إدارة الجلسة

الجزء الأوّل - ربط الحقوق بالتكنولوجيا

١. قسّم المشاركات إلى مجموعات صغيرة من 3 إلى 4 أشخاص كحدّ أقصى، ومن ثمّ أعطِ كل مجموعة ورقة كبيرة أو ورقّتين كبيرتين من أوراق اللوح الورقيّ وبعض الأقلام الخطاطة. ستحتضن كل مجموعة بعشر دقائق للتفكير في لائحة من حقوق الإنسان - مهمة الاختيار والتعريف بهذه الحقوق تعود إليّ إختيار كل مجموعة - عليهنّ كتابتها على ورقة اللوح الورقيّ.
٢. بعد أن تنتهي مهلة العشر دقائق هذه، ستطلبن من كل مجموعة النظر إلى اللائحة التي قامت المجموعة بوضعها - يتوجب عليهنّ الآن مناقشة علاقة حقوق الإنسان هذه بالتكنولوجيا خلال عشر دقائق أخرى (على سبيل المثال، "ما أثر التكنولوجيا على حقوق الإنسان؟"). لتوضيح المسألة، يمكنكّن تقديم مثال عبر رسم الصلة بين التكنولوجيا وحقوق الإنسان واردة على لائحة إحدى المجموعات. يمكنهنّ كتابتها على ورقة كبيرة

<https://vrr.im/70ff>

<https://vrr.im/f5d4>^٦

<https://vrr.im/d7d1>^٧

- أخرى إذا أردن ذلك، ولكن ذلك ليس ضرورياً.
٣. بعد أن تنتهي مدة العشر دقائق الأخرى، شارك مع كل مجموعة رزمة معدة سابقاً من التقارير والمقالات عن الحقوق الرقمية (راجع قسم المواد اللازمة). إعطين كل مجموعة مدة 15 دقيقة ليقرن خلالها بقراءة بعض تلك التقارير والمقالات ومن ثم ليفكرن في التهديدات الرقمية/على الإنترنت المرتبط بحقوق الإنسان التي أوردنها في اللائحة خلال المرحلة الأولى من الجلسة. إشرح للشاركات أن التقارير التي تم تقديمها لهن هي مجرد أدوات إرشادية ففي حال كن يعرفن بحالات أو تهديدات أخرى، يمكنهن إضافتها أيضاً.
٤. ما إن تنتهي مدة الخمسة عشرة دقيقة، إعطين المشاركات إستراحة قصيرة ومن ثم أطلبن من كل مجموعة تقديم عملها لبقية المشاركات بشكل مقتضب.
٥. بعد أن تنتهي كل مجموعة من عملية العرض، إبدأن النقاش مع المشاركات عن مدى سهولة شعور المدافعات عن حقوق الإنسان باليأس أو الانكسار حين تواجههن مخاطر وتهديدات مختلفة- في حال سبق لكن أن أجريتن هذا النقاش خلال جلسة وجهات النظر الشخصية حيال الأمن من هذه الوحدة، يمكن تكبيرهن بكل بساطة بهذا النقاش.
٦. إحرصن على أن يتوفر لكن ما يكفي من الوقت (يفترض أن تكفي مدة من 15 إلى 20 دقيقة) لإختتام هذا الجزء من الجلسة عبر تقديم بعض الأمثلة عن ممارسات أو أدوات متاحة لمواجهة هذه التهديدات. في حال سبق لكن أن قمتن بـ"جلسة" وجهات النظر الشخصية حيال الأمن" من هذه الوحدة، لا تنسين أن تفكرن أيضاً بالحوافز وأسباب الرفض والحواجز التي حددتها المشاركات أثناء وضع التوصيات.

الجزء الثاني - مفاهيم الأمن الرقمي والحقوق الرقمية

٧. الآن وبعد تغطية بعض ممارسات وأدوات الأمن الرقمي الأساسية للتعامل مع التهديدات الرقمية المحدقة بحقوق الإنسان التي تمت مناقشتها في الجزء الأول، إشرحن للمشاركات أنكن ستقدمن لهن بعض مفاهيم الأمن الرقمي الجوهرية بالإضافة إلى تداعيات ملهوسة

على الحقوق: المحافظة على سرية الهوية والخصوصية والتشفير. في بعض البيئات، قد يكون إدخال مسألة الالتفاف والإفلات من المراقبة (circumvention) أيضاً ضرورياً كأحد هذه الأمثلة.

٨. إبدآن بتذكير المشاركات بمدى أهمية قيامن بهذه الخطوة الضرورية بإتجاه معالجة مسألة أمنن الرقمي عبر هذا التدريب، وأنهن الآن سيبدآن بمسيرة تعلم كيفية مواجهة بعض التهديدات المحدقة بهن:

في حال سبق لكن أن غطيتن جلسة وجهات النظر الشخصية حيال الأمن من هذه الوحدة، إستدكرن بعض وجهات النظر والتعريفات الخاصة بالأمن الرقمي التي تمت مشاركتها خلال المرحلة الثانية والثالثة والرابعة من تلك الجلسة. في حال لم تقمن بعد بتقديم جلسة وجهات النظر الشخصية حيال الأمن من هذه الوحدة، من المفيد الآن مناقشة وسائل الأمن الرقمي بشكلٍ عام مع المشاركات إستناداً إلى خبرتكن الخاصة.

٩. أطلبن من المشاركات التطوع لمشاركة تعريفهن الخاص لما تعنيه لهن الخصوصية، ومن ثمّ تابعن بالسؤال عن آرائهن بالوضع الحالي للخصوصية في زمن الإنترنت. وبعدها، إشرحن لهن ماهية الخصوصية الرقمية - وأثناء هذا الشرح، إحرصن على إيجاد طرق لتشجيع المشاركات على إستعادة حقهن بالخصوصية.

١٠. كررن المرحلة التاسعة ولكن عاجلن مفهوم المحافظة على سرية الهوية هذه المرة - أطلبن من المشاركات تفسير ما يعنيه لهن مفهوم المحافظة على سرية الهوية، وإشرحنه أووضحن بإيجاز أي شكوك قد تساور المشاركات بواسطة أمثلة ممكنة أو مناسبة قدر الإمكان. ويتوجب عليكن مرة أخرى إيجاد طرق لتشجيع المشاركات على إستعادة حقهن بالمحافظة على سرية الهوية، وإحرصن أيضاً على توضيح الفوارق بين الخصوصية والمحافظة على سرية الهوية كمفهومين منفصلين.

١١. بعد الإنتهاء من النقاشات والشروحات السابقة عن الخصوصية والمحافظة على سرية الهوية، إنتقلن إلى التعريف بمفهوم التشفير - إشرحن لهن أنهن سيتعلمن عن هذا المفهوم إلى جانب غيره من المفاهيم خلال التدريب. وأن بعض الممارسات والأدوات التي سيغطيها التدريب تتضمن التشفير بطرقٍ مختلفة. قدمن لمحة عامة موجزة عن بعض هذه

الممارسات والأدوات وقن يربطها بالنقاشات السابقة حول الحقوق الرقمية والخصوصية والمحافظة على سرية الهوية.

١٢. لإختتام هذه الجلسة، إقترح بعض المنظمات التي تقدم الدعم والمناصرة للحقوق الرقمية في بلدان أو مناطق المشاركات، لكي يتمكن من البحث عنها والتعرف عليها بأنفسهم - على سبيل المثال، في حال كنتن تعملن مع "فروتلاين ديفندرز" - Frontline Defend- "إلكترونيك فرونتيرز فاوندإشن" EFF، لجنة حماية الصحفيين CPJ، "أيفكس" ers، " منظمة تاكتيكل تكنولوجيا كوليكثيف - Tactical Technology Collec- ifex، منظمة تبادل الإعلام الاجتماعي SMEX، "آي ركس" IREX، و"إنترنيوز" tive. Internews

References

- <https://www.derechosdigitales.org>
- <https://r3d.mx>
- <https://karisma.org.co>
- <http://acceso.or.cr>
- <https://articulo19.org>

باب ١٠

قصتها مع التكنولوجيا

- الأهداف: تقدّم هذه الجلسة للمشاركات نظرة تظهر الأدوار القيادية التي تولتها المرأة على مدى التاريخ وتطوّر التكنولوجيا الحديث بهدف القضاء على أي تمييز جنسدي مضرّ.
- الطول: 20 دقيقة
- الشكل: جلسة
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
 - إنترنت نسوي^١
 - الحكواتيات^٢
- المواد اللازمة:

^١ <https://vrr.im/d7d1>

^٢ <https://vrr.im/1295>

- صور نساء مختلفات من عالم التكنولوجيا (مع الأسماء)
 - نبذة عن كل امرأة (كمرجع للدرجات)
 - خيط أو حبل (بطول متر واحد)
 - مشابك/ملاقط ملابس أو ملاقط حديدية (واحد أو اثنين لكل صورة)
- التوصيات: المستند التالي عبارة عن مرجع غنيّ بقصص متنوعة عن نجاحات النساء في التكنولوجيا مناسب لهذه الجلسة (باللغة العربية): <https://www.cyber-arabs.com/wp-content/uploads/2018/02/10-سي-ف-ت-دئ-ار-ء-اس-ن-اي-ج-ول-ون-ك-ت-ل-ا.pdf>

إدارة الجلسة

١. إشرحن للمشاركات أن هذه الجلسة ستكون بمثابة تمرين للمجموعة لإنشاء ذاكرة جماعية تقرر وتتعترف بالنساء الرائدات في مجال التكنولوجيا على مدى التاريخ. أطلبن من المجموعة: كم مرة سمعن أن نجاح النساء في عالم التكنولوجيا غير ممكن؟ كم مرة سمعن أنه لا مكان لنا في الحيز العام أو الحيز الأكاديمي بل فقط وراء الكواليس أو بعيداً عن الأنظار؟
٢. أطلبن من المجموعة الجلوس على شكل دائرة (على الأرض أو على الكراسي) وإبدأن الجلسة بمقدمة موجزة عن تقسيم الأدوار بحسب الجندر في مجال التكنولوجيا - ما هو؟ وماذا نعرف عنه؟
٣. أطلبن من المشاركات مشاركة قصصهن مع التكنولوجيا التي تظهر قوتهن وقدرتهن على المقاومة. يمكنكن البدء بطرح الأسئلة التالية على المجموعة - ماذا تعني التكنولوجيا لكن؟ هل هي أمرٌ إيجابيٌّ أم سلبيٌّ؟ ومن بعد ذلك، شاركن قصصكن الشخصية أو قصة ملفتة عن التكنولوجيا كمثال - قد يشجع ذلك المشاركات على الشعور بالإرتياح والإفتاح.

٤. بعد أن أتيحت الفرصة لكل واحدة ترغب بمشاركة قصتها، إجلبن الصور والنبذات المرافقة للنساء الرائدات في مجال التكنولوجيا التي ستقدمها للمجموعة. رتبين الصور والنبذات على الطاولة أو على الأرض من دون ترتيب معين، ومن ثم إطرحن على المجموعة السؤال التالي - من تعتقدن أنها بدأت أولاً في عالم التكنولوجيا؟

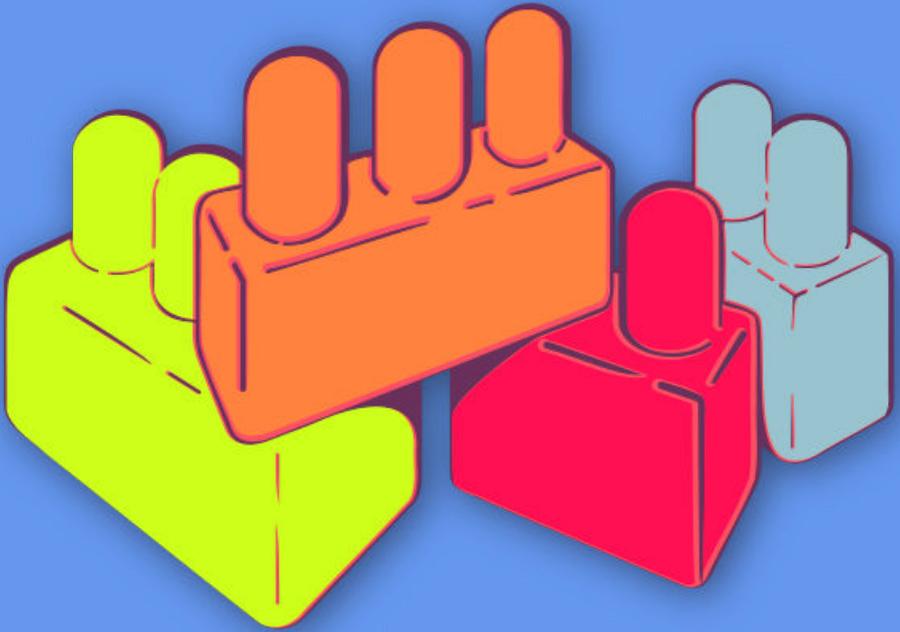
٥. بواسطة الملاقظ/المشابك الحديدية أو الخشبية ثبتن الصور على الجبل، وأطلبن من المجموعة العمل معاً على ترتيب النساء بالترتيب الزمني الصحيح من أجل إنشاء جدول زمني خاص بقصة أو تاريخ النساء مع التكنولوجيا؛ على سبيل المثال، من الممكن ترتيبها وفقاً لتواريخ ولادتهن أو وفقاً للسنة التي حققن فيها إنجازهن الأول في مجال التكنولوجيا - إحرصن أن تكون المعلومات اللازمة المتاحة للمجموعة لكي تتمكنن من القيام بالتمرين!

٦. بعد أن تنجز المجموعة التمرين، على المشاركات حينها شرح الجدول الزمني الذي وضعنه - أطلبن منهن إطلاعكن على عدد النساء وقصصهن التي يعرفنها أصلاً وعلى اللواتي تعرفن عليها خلال هذه الجلسة. يجب أن يبقى الجدول الزمني معلقاً في مكان ظاهر في قاعة التدريب طيلة فترة ورشة العمل - ولإختتام الجلسة يمكنكن أن تطلبن من المجموعة قراءة معلومات عن تلك النساء المذهلات وقصصهن لبضع دقائق بصمت. اختياري: بما أن الجدول الزمني سيبقى معلقاً طيلة فترة التدريب، يمكنكن إجراء هذه التمرين بطريقة أخرى عبر إختتامه بعد أن تنتهي المشاركات من عملية شرح الجدول الزمني الخاص بهن. ما أن يجلس الجميع، يمكنكن أن تبدأن بمشاركة نبذة المرأة الأولى على الجدول الزمني وتحدثن عنها وعن أهمية قصتها.

في بداية كل يوم من أيام التدريب (بحسب عدد الأيام وعدد المشاركات)، أطلبن من مشاركة أو مشاركتين القيام بالأمر ذاته عن المرأة التالية أو المرأتين التاليتين على الجدول الزمني - بهذه الطريقة، بنهاية هذا التدريب، ستتاح لكل مشاركة فرصة المساهمة في التدريب عبر قيادة جلسة صغيرة، ومن ثم تقمن بمشاركة قصص كل النساء على الجدول الزمني.



النساء فى فضاء الإنترنت



أسس الأمن الرقمي الجولة
الأولى

باب ١١

كيف يعمل الإنترنت؟

- الأهداف: إطلاع المشاركين على كيفية فهم تدفق المعلومات عبر الإنترنت والثغرات ونقاط الضعف المختلفة والممارسات الأمنية الجيدة المناسبة لكل نقطة من نقاط السلسلة.
- الطول: 60 دقيقة
- الشكل: جلسة
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- حقوقن والتكنولوجيا الخاصة بكن^١
- المواد اللازمة:
- أقلام خطاطة
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
- كيف يعمل الإنترنت؟ لافتات عليها صور للأجزاء المختلفة من السلسلة التي تمر بها رسالة بريد إلكتروني ما حين تُرسل من حاسوب إلى آخر(عدد 2 * أجهزة

^١ <https://vrr.im/1151>

- + (حاسوب/هاتف محمول) + عدد 2 مودم + عدد 2 عمود هاتف/ألياف بصرية
- تحت الأرض + عدد 2 مقدم خدمة الإنترنت + عدد 1 خوادم غوغل + عدد
- إثنين أو أكثر بريد + إلكتروني وهمي)
- أوراق توزع فيها إقتراحات لممارسات الأمن الرقمي
- ورقة تستخدم كلوح - ورقة كبيرة (4 أمتار)، وورقتين أصغر حجماً (متر واحد)
- شريط لاصق
- شرائح (مع النقاط المفتاحية الواردة أدناه)
- مكبرات للصوت
- التوصيات: إحرصن على الإجابة على كل أسئلة المشاركات. يجب أن يحصلن بنهاية
- الجلسة على إجابات وافية لمخاوفهن بشأن الثغرات/نقاط الضعف التي تملعن عنها وأن
- يشعرن بأنهن يمتلكن الآن المعلومات اللازمة للتحرك على أساسها. تفادين إنشاء جو
- يثير الخوف أو الإجهاد أو القلق - قدمن المعلومات والموارد الكافية بالإضافة إلى
- فرص تدريبية إضافية (إذا أمكن)

وضعت هذه الجلسة من قبل كل من مارييل غارسيا Mariel Garcia من منظمة سوشل تي أي سي SocialTIC وسيروس موناستيريوتيس Spyros Monastiriotes من منظمة تاكتيكل تكنولوجي كوليكثيف Tactical Technology Collective

إدارة الجلسة

الجزء الأول - كيف يعمل الإنترنت - تدفق المعلومات ونقاط الضعف.

١. سيبدأ هذا الجزء من ورشة العمل بلعبة. ستعطي المشاركات أوراق تمثل جزءاً من السلسلة التي يسلكها تدفق المعلومات على الإنترنت (المودم، الحاسوب مبنى الشركة المقدمة لخدمة الإنترنت... إنلخ) وسيطلب منهن ترتيب أنفسهن وفقاً للترتيب الذي يعتبرن أنه يمثل الترتيب الصحيح للطريق الذي تسلكه رسالة بريد إلكتروني عبر الإنترنت للوصول إلى حاسوب آخر.

٥٢. بعد أن ترتب المجموعة مواقعها، ستقوم الميسرات بتصحيح الأخطاء في حال وجودها وستشرح العملية الكاملة للجميع. بعد ذلك، سيطلب من متطوعة إعادة الشرح. يوصى بتقديم الشرح الكامل ثلاث مرات على الأقل؛ ولكن من أجل تقديم التمرين بطرق مختلفة، تستطيع الميسرة تغيير رسوم البريد الإلكتروني المستخدمة وتغيير النقطة التي يبدأ منها الشرح. على المدربات أيضاً منح الوقت الكافي لتبديد الشكوك المرتبطة بهذه العملية.

٥٣. يمكنكين أيضاً استخدام فيديو كهذا

<https://www.youtube.com/watch?v=xYKKro8UMp0>

https://www.youtube.com/watch?v=uKNECbLR_tw

لمساعدة المشاركات على تحديد الأخطاء التي ارتكبتها في الترتيب الذي وضعه بأنفسهن. إختياري: لتكثيف هذا التمرين لدى إجرائه مع مجموعات أكبر - بدل إعطاء ورقة واحدة لكل شخص، اعطين ورقة واحدة لكل شخصين؛ بالنسبة للمجموعات الأقل عدداً، يمكنكين وضع الأوراق على الأرض ومناقشة الترتيب الصحيح في ما بينهم.

الجزء الثاني - نقاط الضعف

٥٤. بعد الإنتهاء من العملية السابقة، سيطلب من المشاركات لصق كل ورقة على ورقة كبيرة جداً ستترك على الأرض. عندها، ستقوم الميسرات بإعادة شرح السلسلة، وهذه المرة سيشرن ويفسرن نقاط الضعف الموجودة في كل مرحلة دون خلق حالة من الخوف الشديد وسط المشاركات (الجدير بالذكر هنا أنه من الممارسات السليمة أثناء التدريب هي المحافظة على ثقة وهدوء المشاركات). سيتم ذكر بعض نقاط الضعف أدناه. يمكن أيضاً إضافة ممارسات أو تهديدات أخرى قابلة للتطبيق في بيئتكين أو لا بد من إطلاع المشاركات عليها. يمكن أيضاً تقديم بعض الأمثلة عن الممارسات التي تعتمد عليها جماعات أخرى تعملن معها لمساعدة المشاركات على التفكير في بعض الممارسات السليمة أو الخاطئة التي يقمن بها.

الجهاز رقم 1 (حاسوب/هاتف): انعدام الأمن المادي؛ فقدان المعلومات
المودم رقم 1: القدرة على رصد وسرقة المعلومات الصادرة عبر إشارة شبكة الإنترنت
اللاسلكي (Wifi sniffing)؛ انعدام التشفير

عمود الهاتف/الألياف البصرية تحت الأرض رقم 1: لا يوجد

الشركة المقدمة لخدمة الإنترنت: طلبات البيانات والبيانات الوصفية من الحكومات
المحلية/الوطنية خوادم غوغل: المراقبة الدولية؛ انعدام أمن كلمة السر ورسائل التصيد،
طلبات من الحكومات الوطنية

عمود الهاتف/الألياف البصرية تحت الأرض رقم 2: لا يوجد

المودم رقم 2: مشاكل أمنية جراء استخدام شبكات اتصال أشخاص آخرين (مثلاً
مقاهي الإنترنت)

الجهاز رقم 2: البرمجيات الخبيثة؛ عمليات الحذف غير الآمنة

الجزء الثالث - الممارسات السليمة في الأمن الرقمي

٥. بعد التركيز على نقاط الضعف، سيحين الوقت لتقسيم المجموعة إلى مجموعات أصغر،
كل مجموعة قادرة على اعتماد إحدى نقاط الضعف المناقشة في التمرين السابق وإقترح
حلول مبتكرة لها. ولجعل ذلك أقل صعوبة للمشاركات الأقل خبرة. ستعطي كل مجموعة
ورقة عليها حل مقترح لبدء النقاش.

بنهاية التمرين، ستعطي المجموعات مدة من 30 ثانية إلى دقيقة لتقديم أفكارها (وفي
الوقت عينه تقوم إحدى الميسرات بتدوين الملاحظات وتدخل إضافات إلى ما سبق
وتم التحدث عنه). ستنتقل الميسرات بين المجموعات لتقديم شروحات موجزة والإجابة
على الأسئلة، وتحفيز النقاشات بين جميع المشاركين.

مع تقدّم سير النشاط، لا بد للميسرات من شرح أساسيات كل حلّ. إضافة إلى ذلك،
بحسب مستوى التفاعل وسرعة ورشة العمل، قد لا تكون تغطية جميع المقترحات

ممكنة.

بعض المقترحات التي تعتبر مشاركتها مهمة:

إنعدام الأمن المادي: يفضل التخفيف من عرض الأجهزة في منظماتك للغرباء
إنعدام الأمن المادي: وضع كلمة سر على الحواسيب في المكتب وفي المنزل فقدان
معلومات: المحافظة على نسخة احتياطية في مكان غير المكتب أو المنزل فقدان معلومات:
تحديد شخص مسؤول عن النسخ الاحتياطية للجميع في المنظمة رصد وسرقة المعلومات
عبر إشارة شبكة الإنترنت اللاسلكي WiFi sniffing: إزالة جميع الافات التي يرد عليها
كلمة سر شبكة الإنترنت اللاسلكي الخاصة بالمنظمة رصد وسرقة المعلومات عبر إشارة
شبكة الإنترنت اللاسلكي WiFi sniffing: تغيير كلمة سر شبكة الإنترنت اللاسلكي
الخاصة بكن بشكل دوري (يفضل مرة كل أسبوعين) إنعدام التشفير: البدء في
إستخدام أدوات وتقنيات تشفير مأمونة إنعدام التشفير: الإطلاع على قسم التشفير
على موقع "سيكيوريتي إن آي بوكس Security in a Box طلبات البيانات والبيانات
الوصفية من الحكومات المحلية/الوطنية: العمل مع منظمات الدفاع عن الحقوق الرقية
لمعرفة الطرق القانونية التي يمكن من خلالها حماية أنفسكن. طلبات البيانات والبيانات
الوصفية من الحكومات المحلية/الوطنية: التعرف على القوانين النافذة في بلدكن التي
تتناول موضوع التدخل في الإتصالات. المراقبة الدولية: الإنتقال إلى إستخدام خدمات
آمنة لإجراء عمليات البحث وإرسال الرسائل وإستضافة المواقع والاتصالات بشكل
عام. انعدام أمن كلمة السر: استخدام كلمات سر طويلة ومعقدة! انعدام أمن كلمة
السر: استخدام خدمة "كي باس" KeePass لعدم نسيان كلمات السر المتعددة التي
تستخدمها التصيد: التفكير قبل الضغط على أي زر (يجب أن تفكرن في المنصات
التي تدخلن فيها معلومات تسجيل الدخول الخاصة بكن) إستخدام شبكة الإنترنت
اللاسلكي الخاصة بالآخرين: تسجيل الدخول على حساباتكن الشخصية دوماً بشكل
يدوي بدلا من حفظ كلمات السر الخاصة بكن على هذه الشبكات. كما يجب تذكر
تسجيل الخروج من الحسابات الخاصة بكن بعد الإتهاء من استخدامها. إستخدام شبكة
الإنترنت اللاسلكي الخاصة بالآخرين: الإلتباه للأمر التي يجب ألا تثرنها أو تبحثن عنها

في محركات البحث حين تستخدم شبكة الإنترنت اللاسلكي الخاص بأشخاص آخرين برمجيات خبيثة: تثبيت برمجيات مكافحة للفيروسات وتشغيلها يدوياً مرة في الأسبوع حذف غير آمن: استخدام زر + Cmd النقرة اليمنى لإفراغ سلّة المهملات على حاسوب ماك حذف غير آمن: استخدام برمجيات الحذف الآمن مثل برمجية "إرايزر" Eraser أو برمجية "سي سي كلينر" CCleaner

الجزء الرابع - الموارد والمسائل العالقة

٦. الهدف من هذا الجزء من الجلسة هو جمع الأسئلة المرتبطة بالأمن الرقمي التي ربما لم تطرح حتى الآن خلال ورشة العمل، بالإضافة إلى مناقشة مواضيع مرتبطة بالمجتمع المحلي الخاص بالمشاركات. هذا وقت مناسب لتوفير الموارد للجميع لتعلم المزيد والبقاء على إطلاع بالمستجدات في مجال الأمن الرقمي. ستجمع الميسرات الأسئلة من الحضور وتلّح إلى الإجابات المحتملة وتذكر المراجع التي يمكن استخدامها لإيجاد الإجابات. 7.

المراجع

- <https://securityinabox.org>
- <https://myshadow.org>

باب ١٢

بناء كلمات سرّ قوية

- الأهداف: في هذه الجلسة، ستتمن مع المشاركات بمراجعة تداعيات سرقة كلمة سرّ، وكيفية تعرضها للسرقة عادةً، وكيفية إنشاء كلمات سرّ أقوى، واكتساب عادات أفضل خاصة بكلمات السرّ.
- الطول: 45 دقيقة
- الشكل: جلسة
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- كيف يعمل الإنترنت؟^١
- كيفية حماية حاسوبك^٢
- المواد اللازمة:
- جهاز عرض
- شرائح

^١<https://vrr.im/7ba91>

^٢<https://vrr.im/ac952>

- أوراق
- إمكانية اتصال بشبكة إنترنت لاسلكي/إنترنت من أجل تنزيل برمجية "كي باس"
KeePass

تستند هذه الجلسة إلى وحدة "ممارسات كلمات السرّ الآمنة" الموضوعية من قبل تشيكاكي سينكو Cheekay Cinco وكارول واترز Carol Waters وميغان ديبلو Megan DeBlois لصالح "ليفل أب" LevelUp

إدارة الجلسة

الجزء الأول - المقدمة

١. إبدأن هذه الجلسة بطرح الأسئلة التالية على المشاركين:
 - متى كانت المرة الأخيرة التي قن بها بتغيير أي من كلمات سرّهن؟
 - هل لديهن كلمات سرّ مختلفة لحساباتهن المختلفة؟
 - هل كلمات سرّهن مكتوبة على أوراق ملصقة في مكان ما؟
 - هل قن بتخزين كل كلمات السرّ في أحد المستندات؟
 - هل هواتفهن مزودة بكلمة سرّ؟

الجزء الثاني - ما أهمية كلمات السرّ؟

٢. قبل أن تبدأن بالتحدث عن أهمية كلمات السرّ، أطلبن من المشاركين وضع لائحة بكل المعلومات المحمية بواسطة كلمة سرّ. ما هي المعلومات المتوفرة لديهن على حسابات بريدهن الإلكتروني وحساباتهن على مواقع التواصل الاجتماعي وهواتفهن المحمولة؟ ماذا قد يحصل في حال تمكن شخص آخر من الوصول إلى تلك المعلومات؟

٣. والآن، شاركن مع المشاركات بعض الأسباب التي تبرر أهمية كلمات السرّ:

توفر كلمات السرّ إمكانية الوصول إلى عدد من الحسابات المهمة كحساب البريد الإلكتروني والحسابات المصرفية ومواقع التواصل الاجتماعي، إلخ.

غالباً ما تحتوي هذه الحسابات على معلومات حساسة، ونحن في الغالب نتصرف على سجيئتنا ونتفاعل بتلقائية مع الآخرين بواسطة خدمات رقمية متنوعة ونقوم بتبادل معلومات عديدة حساسة - وقد يتضمن ذلك إرسال رسائل عبر شبكات التواصل الاجتماعي أو إرسال رسالة بريدية إلكترونية أو إجراء عمليات شراء على الإنترنت... إلخ.

الحصول على كلمات سر الأشخاص الآخرين تسمح بإنتحال صفاتهم/ن الشخصية - فأي شخص قادر على الوصول إلى كلمة سر حساب ما، يمكنه فعلياً التصرف على الإنترنت وكأنه صاحب الحساب.

تمنح كلمات السرّ أيضاً إمكانية الوصول إلى عدد من الأمور الأخرى - نقاط التواصل مع شبكة الإنترنت اللاسلكية وفك كلمات سر الأجهزة المحمولة وتسجيل الدخول إلى الحواسيب وفك تشفير الأجهزة والملفات وغيرها.

الجزء الثالث - ماذا قد يحصل في حال تعرض كلمة سرّكم للسرقة؟

٤. في هذا الجزء من الجلسة، سنقوم بتوزيع الأوراق على المشاركات وسنطلب منهن وضع لأحة بكل المنصات التي يتذكرن أنه لديهن حسابات عليها. والآن أطلبن من المشاركات وضع لأحة بما قد يحصل في حال إستحوذ أحدهم على كلمة سرّهن وتمكن من الدخول إلى حساباتهن أو أجهزتهن:

قد تتعرض معلومات أو ملفات مهمة للسرقة (للسنخ) أو للخذف؛ في حال تعرضها للسرقة، قد لا تلاحظن ذلك مباشرة. وقد تكون المعلومات المسروقة أي شيء مثل مستندات أو ملفات مهمة أو حساسة جداً أو قائمة جهات إتصال أو رسائل بريدية إلكترونية.

قد نعرض أموال وحسابات بنكية للسرقة أو الصرف من خلال إمكانية الوصول إلى البطاقات الائتمانية أو معلومات الدخول على الحسابات المصرفية.

يمكن إستخدام حسابات البريد الإلكتروني أو مواقع التواصل الإجتماعي لإرسال الرسائل المزججة أو لإنتحال شخصيتك أو شخصية أصدقائك أو أفراد عائلتك أو زملائك.

قد تصبح إمكانية الدخول إلى حساباتك محتجزة إلى أن تقم بدفع شكل من أشكال "الفدية" - قد يتضمن ذلك، دفع المال أو منح إمكانية وصول إلى جهات إتصال أو إلى حسابات أخرى.

قد يستخدم شخص ما كلمة السرّ الموجودة بحوزته للوصول إلى إتصالاتك ونشاطاتك ومراقبتها من دون علمك.

قد تؤدي إمكانية الوصول إلى بريدك الإلكتروني إلى تعرض حساباتك الأخرى للخطر، إذ تستخدم لإعادة ضبط كلمات سرّ الحسابات الأخرى من خلال طلب روابط إعادة ضبط كلمات السرّ، وفي نهاية المطاف يصبح من المستحيل عليك الوصول إلى حسابات أخرى كثيرة في حال لم تغيّر كلمة السرّ.

الجزء الرابع - كيفية تعرض كلمات السرّ للسرقة عادةً؟

٥. شاركن بعض الممارسات الشائعة التي قد تؤدي إلى حصول أشخاص آخرين على كلمات سرّك:

حين تشاركها مع الآخرين، أو تخزنها بطريقة سهلة الكشف - من ضمن الأمثلة الشائعة، كتابة كلمة السرّ الخاص بتسجيل الدخول إلى حاسوبك على ورقة صغير ملصقة على الحاسوب نفسه أو بالقرب منه. حين يرى أحدهم كلمة السرّ أثناء إدخالها على شاشتك ويكتبها أو يحفظها عن غيب.

في حال إستخدام مقدم لخدمة البريد الإلكتروني من دون بروتوكول طبقة المنافذ الآمنة

(https) على مدى الجلسة، أو إستخدامه فقط على صفحة تسجيل الدخول، حيث يعرض ذلك كلمات السرّ والمعلومات الحساسة الأخرى للكشف أمام أي شخص لديه إمكانية الوصول إلى الرابط بعد تسجيل الدخول. يمكن الوصول إلى جهاز يدوياً، أما كلمات السرّ فيمكن الحصول عليها من خلال خاصيتي "احفظ كلمة سري" "Save My Password" أو "تذكرني" "Remember Me" الموجودتين على مواقع إلكترونية من خلال أي متصفح - يصبح ذلك ممكناً بشكلٍ خاص في حال لا يتم إستخدام تشفير شامل للقرص على أي جهاز. البرمجيات الخبيثة كبرمجيات "كي لوغر" keylogger التي تعمل على توثيق كل نقرة على لوح المفاتيح على جهاز ما ومن ثم إرسالها لطرف آخر يريد هذه المعلومات. هذه البرمجيات الخبيثة ليست قادرة على كشف كلمات السرّ وحسب بل قد تصل أيضاً إلى معلومات حساسة أو شخصية. من الممكن أيضاً إختراق المنصات أو نقاط الضعف الموجودة في أنظمتها مما يتسبب بكشف معلومات مستخدميه.

الجزء الخامس - كيف يمكننا جعل كلمات سرنا أقوى؟

٠٦. إشرح للمشاركات أنه في حال إستخدامنا كلمات السرّ ذاتها لكل الحسابات، وتعرض إحداها للسرقة، ستصبح كل حساباتنا مكشوفة. شاركن بعض ميزات كلمات السرّ الأكثر أمناً وقوة مع المجموعة:

الطول: بكل بساطة، كلما زاد طول كلمة السرّ كلما صارت أفضل! يوصى بإستخدام 14 حرفاً كحد أدنى للحصول على كلمات سرّ قوية وفي حال إستخدام 20 حرفاً تصبح كلمة السرّ أقوى بكثير.

التعقيد: إستخدم من كلمة سرّ فيها أحرف وأرقام مع أحرف كبيرة وصغيرة مع تشكيلة غنية من الأرقام والرموز.

التغيير المستمر: غيّر كلمات سرّك بشكلٍ دوريّ، لا سيما تلك الخاصة بحساباتك الحساسة، ولا بد من تغييرها في حال وصلتكن رسائل بريدية موثوق بها (ليست رسائل

تصيّد) تذكركن بأن حسابات المستخدمين آخرين وكلمات السرّ لديهم تعرّضت للسرقة. استخدام جمل سرّ بدلا عن كلمات السرّ (تخيلن كلمات سرّ مرتبطة ببعضها ضمن جملة) مثال أخرى عن ممارسة كلمات سرّ قوية - إلیکن بعض الأمثلة:
SayNoToSexualHarassmentInMiddleEast ("لا للتحرش الجنسي في الشرق الأوسط")

MyRightToDecentShelter ("حقني في مسكن لائق)

لم) WeDidNotChooseToBecomeRefugeesWeWereForcedToComeHere
نختر أن نصبح لاجئين/ات، بل أجبرنا على المجيء إلى هنا)

٧. أطلبين من المشاركات التفكير لبضع دقائق قبل البدء بإنشاء بعض الأمثلة عن كلمات السرّ القوية. ذكرن المشاركات أنه يتوجب عليهن التفكير في مدى حساسية المعلومات الموجودة في حساب معين أثناء تفكيرهن في طول وتعقيد كلمات سرّهن - قد يرغبن في استخدام أقوى كلمات السرّ لأهم حساباتهن، وفي الوقت عينه استخدام أقلها تعقيداً (مع المحافظة على قوتها) للحسابات الأقل أهمية.

المراجع

<https://level-up.cc/curriculum/protecting-data/creating-and-managing-strong-passwords/input/safer-password-practices/>

باب ١٣

البرمجيات الخبيثة والفيروسات

- الأهداف: تعالج هذه الجلسة أساسيات ماهية البرمجيات الخبيثة، وكيف يمكن أن تصبح الأجهزة المستخدمة معرضة لأنواع مختلفة من البرمجيات الخبيثة، في سياق المخاطر المحدقة عادةً بالمدافعات عن حقوق الإنسان.
- الطول: 30 دقيقة
- الشكل: جلسة
- مستوى المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
 - كيف يعمل الإنترنت؟^١
 - كيفية حماية حاسوبك^٢
 - لنعد إلى خانة الصفر (إعادة الضبط)!^٣
- المواد اللازمة:

^١<https://vrr.im/7ba91>

^٢<https://vrr.im/ac952>

^٣<https://vrr.im/6a403>

- شراخ (مع النقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز العرض
- التوصيات: يفضل أن تتبع هذه الجلسة، جلسة كيفية حماية حاسوبك، الموجودة في هذه الوحدة أيضاً.

إدارة الجلسة

الجزء الأول - تعريف بالبرمجيات الخبيثة

- ٠١ إشرح للمشاركات ماهية البرمجيات الخبيثة وراجع معهن بعض أنواع البرمجيات الخبيثة الموجودة - كحد أدنى، يوصى بأن تغطي البرمجيات التالية:
 - حصان طروادة (Trojan Horse)
 - برمجيات التجسس (Spyware)
 - برمجيات الفدية (Ransomware)
 - برمجيات تسجيل نقرات/ضربات لوحة المفاتيح (Keylogger)
- تعرض معظم المدافعات عن حقوق الإنسان لبرمجيات الفدية وتسجيل النقرات الخبيثة بشكل متزايد؛ في حال كنتن تعملن مع مجموعة من النساء لا بد من معالجة هذه البرمجيات بالذات. على نحو مماثل، إحرصن بشكل عام على إدراج دراسات حالات وأمثلة عن برمجيات خبيثة تواجهها المشاركات في تدريبكن ضمن بيئتهن.

الجزء الثاني - كيف يمكن أن نتعرضن للإصابة بها؟

- ٠٢ فسن بعض الطرق الشائعة التي قد تصبح أجهزتك من خلالها مصابة ببرمجية خبيثة، وما هي الممارسات غير الآمنة التي قد تؤدي إلى مثل هذه الإصابات. لا بد أيضاً من شرح الأهداف أو المحفزات المختلفة التي تدفع إلى نشر البرمجيات الخبيثة:

تنشر بعض البرمجيات الخبيثة على نطاق واسع من دون هدف محدد. تستهدف أنواع أخرى الناشطات أو الصحافيات أو المناضلات بشكلٍ خاص من أجل الإستحواذ على بياناتهن أو اتصالاتهن.

بعض الأنواع الأخرى تستهدف أفراداً يعرف عنهم إرتباطهم بعدد من الناشطات أو الصحافيات أو المناضلات على أمل إصابة أهداف متعددة ضمن الشبكة.

الجزء الثالث - مشاركة أمثلة عن نساء ومدافعات عن حقوق الإنسان

٣. إختتمت الجلسة بمشاركة بعض الأمثلة عن سيناريوهات إصابة ببرمجيات خبيثة تواجهها عادةً النساء والمدافعات عن حقوق الإنسان؛ يمكننا مشاركة دراسات حالات معينة من مدونات أو مقالات أو تجربة شخصية عن نساء أو مدافعات عن حقوق الإنسان تعرضن لهذه التجربة . تذكرن أن لا تكشفن عن هوية الشخص المعني إلا إذا كان لديكن إذن صريح منها بالإفصاح عن أسمها.

إليكن بعض الأمثلة عن حالات عامة، وقد تعرفن حالات مشابهة في بيتكن أيضاً:

تلقت امرأة رسالة بريد إلكتروني عن فرص الحصول على تذاكر مجانية لحضور حفلة موسيقية؛ تسبب الرابط الموجود في الرسالة بإصابة هاتفها الذكي ببرمجية خبيثة.

إمرأة ناشطة تلقت رسالة مما يبدو أنه عنوان البريد الإلكتروني الخاص بزميلتها، بعد النقر على الرابط في البريد الإلكتروني، بات القرص الصلب في حاسوبها "مشفرًا" وظهرت رسالة على شاشاتها تطالبها بتسديد مبلغ مالي مقابل أن تستعيد إمكانية الوصول إلى معلوماتها.

باب ١٤

التصفح الآمن

- الأهداف: توفر هذه الجلسة مقدمة حول ممارسات تصفح الإنترنت الآمنة، بما في ذلك لمحة عامة عن البرامج المضافة والمنافع الأخرى الممكن استخدامها لإنشاء بيئة تصفح أكثر أماناً.
- الطول: 45 دقيقة
- الشكل: جلسة
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- كيف يعمل الإنترنت؟^١
- كيفية حماية حاسوبك^٢
- المواد اللازمة:
- شرائح (مع النقاط المفتاحية الواردة أدناه)

^١ <https://vrr.im/7ba91>

^٢ <https://vrr.im/ac952>

- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز العرض
- إمكانية اتصال بشبكة إنترنت لاسلكي

إدارة الجلسة

الجزء الأول - إختيار المتصفح

٠١ إبدأن الجلسة بسؤال المشاركات عن متصفحات الإنترنت التي يستخدمها والخيارات الأخرى التي سمعن عنها. قدمن لهن متصفح فايرفوكس Firefox - إشرحن فوائده استخدامه وناقشن بإيجاز الفرق بينه وبين المتصفحات الشائعة الأخرى من قبيل غوغل كروم Google Chrome أو إنترنت إكسبلورير Internet Explorer.

إختباري: عند العمل مع النساء الناطقات باللغة العربية، قد تجدن هذا الفيديو مفيداً لبدء النقاش.

<https://www.youtube.com/watch?v=cTrN1OAMYkM>

الجزء الثاني - ممارسات التصفح الأكثر أماناً

٠٢ نتوفر بعض ممارسات التصفح الأكثر أماناً التي يمكنن مناقشتها مع المشاركات - ومع أنكن غير مضطرات للتحدث عنها جميعها معهن، يوصى بأن تشاركن ما يكفي لإعطاء المشاركات خيارات متنوعة (لا تنسين أيضاً أن تحرصن على أن يكون المحتوى مناسباً ومهماً لبيئة المشاركات).

٠٣ إشرحن للمجموعة أنكن ستقمن بمراجعة بعض ممارسات التصفح الآمن معهن، ولكن لن تركزن الآن على أدوات محددة غير المتصفحات بحد ذاتها. بعض المشاركات قد يرغبن منذ هذه اللحظة بتغيير المتصفحات التي يستخدمها ولكن الأخباريات قد لا يكن جاهزات لذلك - لذا قبل مناقشة بعض الأدوات المحددة كالبرامج المضافة إلى

المتصفحات، لا بد من إبقاء تركيز النقاش على الممارسة في البداية.
إليكن بعض الممارسات التي يمكنكين طرحها للنقاش:
البقاء متيقظات تجاه محاولات التصيد والتصيد المستهدف.
حجب الإعلانات المضمنة (embedded ads) والإعلانات المفاجئة. (pop-up ads)
معرفة كيفية عمل ملفات تعريف الارتباط (كوكيز) - إحرصن على التحدث عن
مدى تسهيلها للتصفح ولكن أيضاً عن سلبياتها.
تعطيل ومحو ملفات تعريف الارتباط من المتصفحات.
محو سجل التصفح؛
عدم حفظ كلمات السرّ في إعدادات متصفحكن.
التحقق من البرامج المضافة التي قمتن بإضافتها إلى متصفحكن.
تشغيل خيار "عدم التتبع" (Do Not Track) في متصفحكن.
استخدام بدائل عن محرك بحث غوغل (مثل دك دك غو Duck Duck Go)
معرفة من يقوم بالتتبع على الإنترنت ولماذا؟ (كلا الرابطين الموردين أدناه جيدين عن
هذه المسألة <https://trackography.org/>
و [\(https://www.mozilla.org/es-MX/lightbeam/\)](https://www.mozilla.org/es-MX/lightbeam/)؛
ناقشن الفرق بين HTTP و HTTPS؛
ما هي الشبكات الإقترابية الخاصة ومتى يجب إستخدامها؟
كيف يعمل بالظبط التصفح المتخفي (Incognito Mode or Private Browsing)،
ومتى يجب إستخدامه؟

الجزء الثالث - الأدوات والبرامج المضافة من أجل تصفح أكثر أماناً

٤. إشرح، بعد أن عالجتن بعض الممارسات الأساسية للتصفح الآمن، أنه يمكن أيضاً اقتراح أدوات معينة - البرامج المضافة بالتحديد - التي قد تساعد أو تسهل عملية اعتماد بعض تلك الممارسات تلقائياً.
٥. قدمن لهن الأدوات التالية، شارحن لهن كيفية عمل كل واحدة منها، ولا تنسين أيضاً مشاركة الروابط اللازمة لتنزيلها مع المشاركات. لا بد أن تفهم المشاركات أهمية وفائدة كل أداة تمت مشاركتها معهن؛ ففي حال لم تشرحها بشكل واضح، قد يؤدي ذلك إلى إتخاذ المشاركات قرارات مبنية على معلومات خاطئة بشأن خصوصيتهن أو إخفاء هويتهم على الإنترنت.

أدوات متصفح سطح المكتب

أداة "نوسكربت" ^٣ (NoScript)

أداة "آدبلاك بلس" ^٤ (AdBlock Plus)

أداة "برايفيسي بادجر" ^٥ (Privacy Badger)

أداة "إيتش تي بي إس إفريوير" ^٦ (HTTPS Everywhere)

أداة "كليك أند كلين" ^٧ (Click & Clean)

متصفح "تور" ^٨ (Tor)

<https://noscript.net/>^٣

<https://adblockplus.org/es/>^٤

<https://www.eff.org/es/privacybadger>^٥

<https://www.eff.org/https-everywhere>^٦

<https://www.hotcleaner.com/>^٧

<https://www.torproject.org/download/download-easy.html.en>^٨

أداة "يولوك" (uBlock)^٩
أداة "ديسكونكت" (Disconnect)^{١٠}
أداة "يوماتركس" (uMatrix)^{١١}

أدوات متصفحات الهواتف المحمولة

أداة "إيتش تي بي إس إفريوير" (HTTPS Everywhere)^{١٢}
مكافح الفيروسات "أفاست" Avast^{١٣}
أداة "أورفوكس" (Orfox)^{١٤}
أداة "أوربوت" (Orbot)^{١٥}
متصفح "تور" (Tor)^{١٦} لهاتف آيفون

ممارسات وميزات أخرى

التصفح المتخفي (Incognito Mode/InPrivate Mode)

غالبًا ما تسبب هذه الميزة بالإلتباس لأنها غير مفهومة بشكل مناسب - وقد لا يتوفر لدى المشاركين فكرة واضحة عن كيفية عمل التصفح المتخفي كميزة من ميزات المتصفحات ومتى يكون استخدامها مفيداً. فسّرنا هنا كيفية عمل ميزة التصفح (والميزات المشابهة)، وقد من هنا بعض الأمثلة عن الحالات التي قد تكون فيها هذه الميزات مفيدة فعلياً.

<https://www.ublock.org/>^٩
<https://disconnect.me/>^{١٠}
<https://addons.mozilla.org/es/firefox/addon/umatrix/>^{١١}
<https://www.eff.org/https-everywhere>^{١٢}
<https://www.avast.com>^{١٣}
<https://guardianproject.info/apps/orfox/>^{١٤}
<https://www.torproject.org/docs/android.html.en>^{١٥}
<https://mike.tig.as/onionbrowser/>^{١٦}

الممارسات الآمنة على شبكة الإنترنت اللاسلكي

ختاماً، ناقشنا لبعض الوقت، وقد من شرحاً إذا أمكن، لبعض الممارسات الآمنة الأساسية الخاصة بالإتصال بشبكات الإنترنت اللاسلكي - يتضمن ذلك ممارسات كتغيير كلمات السر المحددة مسبقاً الخاصة بالمودم، وشرح كيفية مراقبة الأجهزة المتصلة بشبكة الإنترنت اللاسلكي الخاصة بهن.

المراجع

- https://myshadow.org/ckeditor_assets/attachments/189/datadeto_xkit_optimized_01.pdf
- <https://myshadow.org/train>
- <https://myshadow.org/how-to-increase-your-privacy-on-firefox>
- <https://securityinabox.org/en/guide/firefox/linux/>

باب ١٥

كيفية حماية حاسوبك

- الأهداف: تحديد الممارسات السليمة للمحافظة على سلامة حواسيبنا.
- الطول: 50 دقيقة
- الشكل: جلسة
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
- جلسات/تمارين ذات صلة:
 - كيف يعمل الإنترنت؟^١
 - البرمجيات الخبيثة والفيروسات^٢
 - التصفح الآمن^٣
 - التخزين والتشفير^٤
- المواد اللازمة:
 - شرائح (مع النقاط المفتاحية الواردة أدناه)

^١ <https://vrr.im/7ba91>

^٢ <https://vrr.im/47e52>

^٣ <https://vrr.im/aee73>

^٤ <https://vrr.im/0ccc4>

- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز العرض
- نسخ مطبوعة عن نموذج متابعة النسخ الاحتياطي الوارد أدناه
- التوصيات: يوصى بأن تقم بشرح مباشر - بواسطة جهاز عرض متصل بحاسوبك
- عن الأدوات التي تختزن التحدث عنها في هذه الجلسة، لكي تتمكن المشاركات من المتابعة والتدريب على إستخدامها على حواسيبهن الخاصة من خلال إستخدام ملفات غير مهمة أنشئت لأغراض هذه الجلسة (وليس ملفات أو بيانات مهمة فعلياً!)

إدارة الجلسة

الجزء الأول - مقدمة

١. إسألن المشاركات إلى أي مدى حواسيبهن قيمة بالنسبة لهن - مدى فائدتها وضرورتها في حياتهن الشخصية والمهنية؟ ما هي كمية المعلومات المخزنة في حواسيبهن؟
٢. والآن، إسألن المشاركات - كم من الوقت يخصص لصيانة أجهزتهن؟ غالباً ما يكون الفرق بين مدى تقدير الناس لأجهزتهم وكم الوقت الذي يخصصونه لصيانتها والإعتناء بها كبيراً جداً. إشرحن للمجموعة أن هذه الجلسة ستركز على الممارسات الأساسية الخاصة بحماية الأجهزة.

الجزء الثاني - المحيط المادي والصيانة

٣. أخبرن المجموعة أن عدداً لا بأس به من الممارسات المرتبطة بسلامة الجهاز هي في الحقيقة مرتبطة أكثر بالسلامة المادية أكثر مما هي مرتبطة بالأمن الرقمي (هذه طريقة مفيدة لتعزيز التركيز الشامل لهذا المنهاج). أحد الأمثلة المفيدة في هذا الصدد هو أهمية تنظيف الأجهزة، أي التخلص من الأوساخ أو الرواسب التي قد تتكدس داخل الجهاز، وإجراء عمليات تحقق دورية لتحديد ما إذا كان الجهاز قد تعرض لأي تعديلات

مادية أو محاولات تطفّل ماديّة. في هذا الصدد، يمكن التوصية باعتماد ممارسات رقمية أساسية - كإستخدام كلمة سرّ لإقفال الجهاز في حال لم يكن في حوزتك بعد إغلاقه - بالإضافة إلى أدوات الحماية المادية، كإستخدام حامي لوح المفاتيح (keyboard protector) أو سلك ضد سرقة لوحة المفاتيح (an anti-theft cable chain) لمنع أي سرقة أو إمكانية وصول غير مرغوبٍ بها. إحرصن على أن تُشرن هنا إلى أن أهم جانب من جوانب سلامة أجهزتهن المادية هو الوعي. لا بد من معرفة مكان وجود جهازٍ ما في أي لحظة - إما بحوزتهن وإما في غرفة أخرى وإما في مكان آمنٍ آخر.

٤. أطلبن من المشاركات إستدكار بعض التفاصيل عن مكان عملهن - ما هي المخاطر المادية المحتملة؟ هل حاسوبهن معرّض للسرقة؟ هل من أسلاك موضوعة بغير مكانها الصحيح؟ هل من الممكن أن يتعرض حاسوبهن للحرّ الشديد أو البرد أو الرطوبة؟ إلیکن بعض الجوانب المهمة الأخرى المرتبطة بالوعي - الوعي المادي لا يقتصر فقط على الحرص بالألا يصل أي خصم إلى أجهزتهن بل يتضمن أيضاً الضرر المحتمل الذي يتسبب به المكان الذي يتواجد فيه الجهاز.

الجزء الثالث - سلامة البرمجيات

٥. إشرحن للمشاركات مخاطر إستخدام برمجيات مقرصنة (من عيوب البرمجيات المقرصنة أنها تؤدي إلى إحتمالية أكبر لتحميل برمجيات خبيثة في أجهزتهن، ولا يمكن إجراء عمليات تحديث دورية بالطريقة ذاتها التي تعتمد عليها البرمجيات المرخصة... إلخ)؛ إلا أن البرمجيات المرخصة قد تكون باهظة الثمن في معظم الأحيان لذلك يمكن عندها مشاركة بعض الموارد مع المجموعة التي قد تساعد في معالجة هذه المشكلة مثل:

أوسلت° Osalt

إفتحن متصفحاً وإجثن عن "أوسلت" - هذا موقع إلكتروني يقدّم بدائل مجانية ومفتوحة المصدر لمعظم منصات البرمجيات المهمة المرخصة (مثلاً استخدام نظام

<http://www.osalt.com>°

أوبونتو Ubuntu بدل عن نظام ويندوز Windows؛ ليبر أوفيس LibreOffice بدل عن برنامج مايكروسوفت وورد Microsoft Office؛ إنكسكايب InkScape بدل عن أدوبي إيلستراتور (Adobe Illustrator).

تك سوب^٦ TechSoup

بواسطة "تك سوب"، يصبح المدافعون والمدافعات عن حقوق الإنسان ومنظماتهم مَحْوَلِينَ للحصول على نسخ مجانية أو خاضعة لتخفيضات هائلة من البرمجيات التجارية: قد يبحث المستخدمون عن موزعين رسميين من ضمن مقدمي خدمات تقنية المعلومات والإنترنت المحليين أو يطلبون حسومات على الترخيص للقطاع العام أو لمنظمة لا تهدف للربح. تدير تك سوب شبكة توزيع كبيرة للبرمجيات المتبرع بها - الرابط أعلاه يحتوي على قائمة بالشركاء والدول التي يعملون بها.

٥٦. إشرحن للمشاركات أهمية المحافظة على كافة برمجياتهن محدثة - لأن ذلك يحميها من نقاط الضعف الأمنية. يجب أن تقمن بتنزيل كل البرمجيات والتحديثات من مصادر موثوقٍ بها فقط؛ على سبيل المثال، عند تحديث برنامج أدوبي أكروبات ريدر Adobe Acrobat Reader، يجب أن تستخدم التحديثات المُنزلة مباشرة من أدوبي وليس من مواقع أخرى.

٥٧. بعد ذلك، إشرحن للمشاركات أهمية توفر برنامج مكافحة الفيروسات على حواسيبهن - وفرن بعض المعلومات التي قد تساعد في تفكيك بعض المعتقدات الشائعة الخاطئة المرتبطة ببرامج مكافحة الفيروسات، على شاكلة:

إستخدام برنامجين أو أكثر لمكافحة الفيروسات يوفر حماية إضافية. نظامي تشغيل ماك ولينوكس ليسا بحاجة لبرمجية مكافحة فيروسات لأنه لا يمكن أن تصاب بفيروسات. استخدام نسخة مقرصنة من برمجية مكافحة فيروسات آمن للغاية. برامج مكافحة الفيروسات المجانية غير آمنة أو موثوقة بها بالقدر ذاته كالبرامج المدفوعة.

٥٨. شاركن هذه الأفكار الشائعة، إلى جانب أي معتقدات أخرى قد تشاركها المشاركات معكن - ومن ثم ناقشن بعض الممارسات الآمنة الأساسية الخاصة باستخدام برمجيات

<http://www.techsoupglobal.org/network>^٦

مكافحة الفيروسات والحماية من البرمجيات (راجعن جلسة البرمجيات الخبيثة والفيروسات من هذه الوحدة). بعض الممارسات المفيدة التي يجب التركيز عليها هنا، في حال لم تتحدث عنها في جلسة البرمجيات الخبيثة والفيروسات في هذه الوحدة، هي:

إستخدام البرنامج المضاف على المتصفحات "يوبلوك" uBlock لتفادي النقر على إعلانات قد تؤدي إلى تنزيل ملفات برمجيات خبيثة على حاسوبهن. التنبه لمحاولات التصيد، وللروابط أو الملفات المرفقة المشبوهة الموجودة في رسائل بريد إلكتروني بشكل خاص، والتي تبدو أنها أرسلت من حسابات غير معروفة أو حسابات تبدو وكأنها مشابهة لجهات اتصال موثوق بها. هذه فرصة سانحة جيدة للأتيان على ذكر جدران الحماية Firewalls - حيث تقدم جدران الحماية طبقة تلقائية من الحماية على حواسيبهن. شاركن أدوات من قبيل "كومودو فايروول" Comodo Firewall و"زون الأرم" ZoneAlarm و"غلاسواير" e.Glasswir. نسخ أحدث (مرخصة) لنظامي التشغيل ويندوز وماك تتمتع بجدران حماية قوية مثبتة أصلاً.

الجزء الرابع - حماية البيانات والنسخ الاحتياطية

٩. إسألن المشاركات - كم مرة قن بإنشاء نسخ إحتياطية للمفاتهن؟ شاركن أمثلة عن أفضل الممارسات المرتبطة بإنشاء نسخ احتياطية للبيانات، على غرار الإحتفاظ بالنسخ الإحتياطية في مكان آمن منفصل عن حاسوبهن، وإنشاء نسخ إحتياطية لمعلوماتهن بشكل دوري ومعتاد - بحسب المعلومات التي أنشئت لها نسخ إحتياطية - والتفكير أيضاً في تشفير القرص الصلب أو وسيلة التخزين حيث ستُخزن البيانات.

١٠. شاركن مع المشاركات نموذج متابعة النسخ الإحتياطي الوارد أدناه، وأطلبن منهن البدء بملمته كل واحدة على حدة. فسرن للمجموعة أن هذه طريقة مفيدة لإنشاء سياسة شخصية لنسخ البيانات الاحتياطية - يمكنهن العودة إليه بعد التدريب، كورد مفيد لمعرفة مكان تخزين البيانات والموعد اللاحق الذي يجب فيه إنشاء نسخ احتياطية جديدة.

نموذج متابعة النسخ الاحتياطي

نوع المعلومات	الأهمية/ القيمة	ما وبيرة إنجاحها أو تغييرها؟	كم مره في الشهر/السنة بحث إنشاء نسخ احتياطية عنها؟

١١. فسّرنا بعد ذلك، أنه على الرغم من توفر أدوات تقوم بنسخ احتياطية بشكل تلقائي (على غرار Duplicati.com أو كوبيان Cobian)، ولكنه سهل علينا البدء بإنشاء نسخنا الاحتياطية يدوياً عبر وضع الملفات في وسيلة التخزين الاحتياطية. هذا يعتمد في النهاية على مدى تعقيد أو كمية البيانات التي يتوجب علينا التعامل معها - بالنسبة للمستخدم العادي غالباً ما تكون عملية إنشاء النسخ الاحتياطية يدوياً أكثر من كافية.
١٢. متابعة النسخ الاحتياطية المحمية للبيانات، راجعنا بإيجاز مفهوم تشفير وسائل التخزين. إشرحنا للمشاركات ما يعني القيام بذلك، ولماذا يعتبر تشفير أقراصنا الصلبة أو وسيلة التخزين مفيداً. تعتبر خدمتي "فيراكربت" VeraCrypt و"ماك كيبير" MacKeeper من الخدمات الشائعة نسبياً التي يستعان بها لتشفير الملفات أو الأقراص ويمكن ذكرها في هذا السياق كخيارات تستطيع المشاركات اعتمادها.

الجزء الخامس - حذف الملفات إستعادتها

١٣. إقرأنا بصوت عالٍ الجملة التالية:

من الناحية التقنية، لا وجود فعلي لخاصية حذف المعلومات على حاسوبك.

إسألنا المجموعة عن رأيها بتلك الجملة - هل هذه الجملة منطقية؟ كيف يمكن ألا تكون هذه الخاصية موجودة فعلاً؟ ذكرنا المشاركات أنهن قادرات على توصيل الملف إلى سلة المهملات على سطح مكتب حاسوبنا ومن ثم إفراغ السلة، ولكن هذه العملية تقتصر

فقط على إزالة رمز الملف وإزالة أسم الملف من الفهرس المختبأ الخالص بكل شيء على حاسوبين ومن ثم إخبار نظام التشغيل أنه يمكن استخدام هذه المساحة لغرض آخر.

١٤. إسألن المجموعة - برأيكن ماذا يحدث للبيانات التي تقمن "بحذفها"؟. إلى أن يستخدم نظام التشغيل هذه المساحة الفارغة الجديدة، ستبقى مملوءة بمحتويات مرتبطة بالمعلومات المحذوفة، تماماً تكزانة ملفات أزيلت فيها كل بطاقات التعريف ولكن بقيت فيها كل الملفات الأصلية.

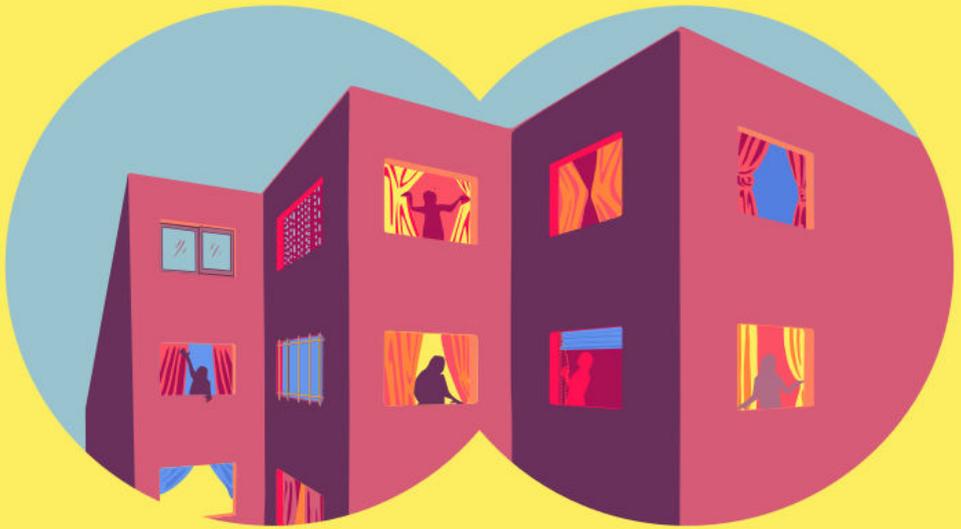
١٥. والآن إشرحن لهن أن ذلك يعود لكيفية إدارة الحاسوب لمساحة تخزين البيانات فيه، وفي حال توفرت لديهن البرمجية المناسبة وتصرفن بسرعة كافية، يمكنهن إستعادة المعلومات المحذوفة عن طريق الخطأ؛ لذلك تتوفر أيضاً أدوات يمكن إستخدامها لحذف الملفات بشكل دائم (وليس فقط إزالتها من فهرس الملفات إلى أن تُشغل المساحة الشاغرة). إغتمن هذه الفرصة لتقديم برمجية "سي كلينز" CCleaner، و/أو برمجية "إيرازر" Eraser، و/أو برمجية "بليتس بت" Bleachbit، كأدوات يمكن استخدامها لحذف الملفات وبرمجية "ريكوفا" Recuva تختيار يمكن اعتماده لإستعادة الملفات المحذوفة.

المراجع

- <https://seguridaddigital.github.io/segdig/>
- <https://securityinabox.org/en/guide/malware>
- <https://level-up.cc/curriculum/malware-protection/using-antivirus-tools>
- <https://securityinabox.org/es/guide/avast/windows>
- <https://securityinabox.org/en/guide/ccleaner/windows>
- <https://securityinabox.org/en/guide/backup>
- <https://securityinabox.org/en/guide/destroy-sensitive-information>
- <https://chayn.gitbooks.io/Avanzado-diy-Privacidad-for-every-woman/content/Avanzado-pclaptop-security.html>



النساء فى فضاء الإنترنت



الخصوصية

باب ١٦

إطرحي علي ما تريدينه من أسئلة!

- الأهداف: يعرف هذا التمرين المشاركات على مدى تغيير فهمنا للخصوصية حين تنقل إلى فضاءات الإنترنت.
- الطول: 15 دقيقة
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
 - الخصوصية^١
 - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟^٢
 - المواد اللازمة:
 - شرائح أو بطاقات عليها أسئلة ترد أدناه
- التوصيات: لا بد من مشاركة الإرشادات تدريجياً مع المشاركات مع التقدم في التمرين،

^١<https://vrr.im/819e>

^٢<https://vrr.im/47ba>

وبالترتيب الوارد أدناه - في حال قدمت الإرشادات كلها في آن واحد قبل إجراء التمرين الفعلي، لن تصلن إلى الغاية المنشودة.

تستند هذه الجلسة إلى الوحدة الموضوعية من قبل إليس مونروي Elis Monroy من مجموعة "سوبفرسيونس" Subversiones لمشروع "صوت النساء".

إدارة الجلسة

٠١ أطلبن من المشاركات إختيار شريكة من المجموعة ومن ثم أن يجدن مكاناً هادئاً للتحدث معها.

٠٢ بعد أن تجلس كل مشاركة مع شريكته، أطلبن منهن مشاركة الإجابات على الأسئلة التالية في ما بينهما:

ما هي الحادثة الأظرف أو الأكثر إحراجاً التي واجهتها في حياتك؟ أذكرني أمراً واحداً تكرهين القيام به.

هل تتمتعين بسماع موسيقى ليست مألوفة بالضرورة؟

هل كان لديك لقباً عندما كنت طفلة؟

كمدربات، يمكنكن إضافة أو تغيير هذه الأسئلة كما ترونه مناسباً - الهدف هو طرح أسئلة يرحح أن تثير معلومات أو قصص قد تكون محرجة أو مضحكة والتحدث عن الخصوصية مع المشاركات. يمكنكن أيضاً الإستعانة بأسئلة شخصية أكثر ولكن يجب أن تنتهين إلى خياراتكن بحسب البيئة التي تتواجدن فيها، إذ حتماً لا ترغبن في إشعار المشاركات بالإزعاج.

٠٣ بعد أن تنتهي المشاركات من تبادل الإجابات مع بعضهن البعض، أطلبن من كل شريكتهن الإضممام إلى شريكتهن جديديتين (يجب أن تتألف كل مجموعة الآن من أربع مشاركات)

٤. أطلبين من المشاركات ضمن المجموعات الجديدة التي شكلتها التعريف بالشركة التي عملن معها خلال الجولة الأولى، ومشاركة الإجابات على كل الأسئلة مع المشاركات في مجموعتهن الجديدة.

٥. بعد أن تنتهي المجموعات المؤلفة من أربع مشاركات من تعريف بعضهن البعض على قصص الأخرى، يمكنك الآن الطلب منهن الإنضمام إلى مجموعة أخرى (يجب أن تتألف كل مجموعة الآن من ثماني مشاركات) - ويجب أن يكررن العملية المذكورة في المرحلة الرابعة من جديد.

٦. إسألن المشاركات عما شعرن به خلال التمرين. بعض الأمثلة عن مشاكل قد يذكرنها المشاركات قد تشمل:

ربما شاركت إحدى المشاركات قصة ما لأنها تعرف الشخص الذي بدأت معه التمرين، أو لأنها شعرت بالإرتياح في تلك اللحظة - ولكنها لم تتوقع أن قواعد التمرين ستتغير هكذا. قد تجد إحدى المشاركات أن شريكتهما أخبرت إحدى قصصها بشكل غير صحيح.

٧. إختتمن التمرين بالتحدث عن الخصوصية، وكيف أن الناس توافق أحياناً على شروط الخدمة الخاصة بمنصة على الإنترنت من دون أن تكون واضحة بشأن ماهية "قواعد اللعبة" ومدى تغيرها عبر الزمن. تحدثن أيضاً عن الموافقة، وكيف أن شخصاً ما قد يوافق أحياناً (مثلاً) أن تلتقط صورة له، ولكن هذا لا يعني أنه وافق أيضاً أن تُشارك صورته على الإنترنت أو مع أشخاص آخرين.

إطرحي علي ما تريدينه من أسئلة!

باب ١٧

الخصوصية

- الأهداف: تعريف المشاركات بمفهوم الخصوصية والمعلومات المحددة لهويتنا المتوفرة على الإنترنت.
- الطول: 50 دقيقة
- الشكل: جلسة
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
 - حقوقك والتكنولوجيا الخاصة بكن^١
 - إطرحي علي ما تريدينه من أسئلة!^٢
 - الجمهور الشبكي^٣
 - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟^٤

^١ <https://vrr.im/1151>

^٢ <https://vrr.im/2b74>

^٣ <https://vrr.im/a184>

^٤ <https://vrr.im/47ba>

- المواد اللازمة:
 - الإستقصاء عن المعلومات الشخصية الخاصة بالمتصيد°
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
 - شرائح (عليها النقاط المفتاحية الواردة أدناه)
- التوصيات: بعض المشاركات قد يشعرون بالإنزعاج أو الاستياء من بعض المعلومات المتوفرة عنهن على الإنترنت خلال قسم "الاستقصاء عن الذات" في هذه الجلسة. في حال حدوث ذلك، إحرصن على تخصيص الوقت الكافي للجزء الأخير من هذه الجلسة الذي ستركز المشاركات فيه على وضع خطوات مستقبلية إستراتيجية للتعامل مع المعلومات التي قد يجدها، يجب أن يتوفر للمشاركات جهاز متصل بالإنترنت في الجزء العملي من هذه الجلسة.

تتضمن هذه الجلسة معلومات من قسم "الاستقصاء عن أنفسنا واستعادة السيطرة" من دليل مجموعة "تاكتيكال تكنولوجي" Tactical Technology "الهدوء وفن جعل التكنولوجيا تعمل لصالحك"

إدارة الجلسة

الجزء الأول - هل نتمتع فعلاً بالخصوصية؟

١. إبدأن النقاش بسؤال المشاركات عما إذا كنّ يعتقدن أن الخصوصية موجودة فعلاً أم لا. ومن بعد ذلك، إسألتهن عن مفهوم الخصوصية بالنسبة لهن - شاركن مفهومهن الخاص للخصوصية لتقديم مثال. ثم إنتقلن إلى الخطوات التالية عبر إخبار المجموعة أنهن في هذه الجلسة وخلال هذا التدريب، سيتمكنن جميعهن من إستعادة حقهن بالخصوصية!

٢. أطلبن من المشاركات مشاركة بعض الأمثلة عن عوامل قد تؤثر على قدرتهن على التحكم ببياناتهن ومعلوماتهن الشخصية وعناصر أخرى. قد تكون تلك العوامل ممارسات شخصية

أو منصات يضعن معلوماتهن بعهدتها أو المعرفة التي يتمتعن بها بشأن الأدوات والأجهزة التي يستخدمنها أو ما يقوم به الآخرون في شبكاتهم.

الجزء الثاني - "الاستقصاء عن الذات" Self Doxxing

٣. إشرح للمشاركات معنى الاستقصاء عن المعلومات الشخصية Doxxing- بشكل أساسي، هو القيام بجمع كميات كبيرة من المعلومات الشخصية عن شخص ما ومن ثم نشرها للعموم (عادةً على الإنترنت). يجب أن تفسرن أيضاً كيفية استخدام الاستقصاء هذا ضد بعض الأشخاص كتكتيك إنتقائي والذي غالباً ما يستخدم لتعريض الناشطين والمدافعين والناشطات والمدافعات عن حقوق الإنسان للخطر أو المضايقة أو التهديد.
٤. إخبرن المجموعة أنهن في هذا الجزء من الجلسة سيتدررن على عملية "الاستقصاء عن الذات" كطريقة لإكتشاف كم ونوع المعلومات التي يمكن إيجادها عن أنفسهن على الإنترنت. إشرحن لهن أن هذا تدير إستباقي مفيد لإتخاذ الخطوات اللازمة للتخفيف من كمية هذه المعلومات (إن أمكن ذلك).
٥. أطلبن من المشاركات فتح مستند فارغ على حواسيبهن، أو تجهيز ورقة بيضاء لتسجيل الملاحظات بشأن المعلومات التي يكتشفنها. ومن بعد ذلك، أطلبن من المشاركات إطلاق متصفح على ويندوز على حواسيبهن على أن يكون متصفحاً لا يستخدمه عادةً - وذلك لكي لا يسجل دخولهن تلقائياً إلى حساباتهن المختلفة.
٦. أطلبن من المشاركات، قبل أن يبدأن بذلك، وضع قائمة بكل الحسابات العامة وصفحات وسائل التواصل الاجتماعي الخاصة بهن؛ ومن ثم أطلبن منهن وضع لأحة بالكلمات أو الجمل الرئيسية التي قد تكون مرتبطة بهن، والتي قد تتضمن معلومات من قبيل: المدينة التي ولدن فيها المدينة التي يقطن فيها عنوان منزلهن المنظمة التي يعملن فيها (أو المنظمات التي يعملن لديها بشكلٍ دوري) القضايا التي يعملن عليها المشاريع والحملات الرئيسية التي يعملن فيها.

٧. قبل البدء بعملية الاستقصاء عن أنفسهن ، على المشاركات البدء أولاً بالبحث عن حساباتهن وصفحاتهن المتنوعة على الإنترنت (يفترض أن تظهر هذه كما تبدو للعموم بما أنهن لن يسجلن دخولهن)، وثانياً تسجيل ملاحظات بالمعلومات التي استطعن إيجادها عن أنفسهن فيها.

٨. بعد ذلك، على المشاركات البحث عن أسمائهن وعن كلمات رئيسية أخرى من القائمة التي وضعنها، بواسطة محرك غوغل وداك داك غو وفيسبوك وتويتر وأي منصات أخرى - إلا أن بعض الإقتراحات الإضافية لهذه المرحلة:
بالنسبة لغوغل وداك داك غو، عليهن البحث عن صور وفيديوهات إلى جانب عمليات البحث العادية.

في حال كنّ يعرفن قواعد بيانات معينة على الإنترنت - خاصة بمدن أو حكومات أو غير ذلك - حيث قد تُعرض معلومات عنهن، عليهن البحث فيها أيضاً. في حال كان لديهن موقعاً إلكترونياً خاصاً بهن، عليهن البحث عن عنوان المجال على <https://whois-search.com> للإطلاع على المعلومات الموجودة عنهن في سجل المجالات العامة.

الجزء الثالث - ماذا نفعل الآن؟

٩. إشرحن للمجموعة الآن أنه من خلال عملية الاستقصاء على الذات، بعضهن قد تجدن معلومات عن أنفسهن لم يكن يعرفن أنها متاحة للعموم، إلى جانب الحسابات التي لم يعدن يستخدمنها وربما قد نسين وجودها.

١٠. أطلبن من الجميع مراجعة كل الملاحظات التي سجلنها، ومن ثمّ تفكير في الخطوة التالية التي يجب أن يتخذنها للإمسك أكثر بزمام الأمور بشأن ما قد يجده الآخرون عنهن على الإنترنت. أطلبن منهن وضع لائحة بالخطوات التي يتوجب عليهن القيام بها، وقد تتضمن إقبال بعض الحسابات وتعديل بعض المعلومات و/أو إعدادات الخصوصية على صفحات وسائل التواصل الاجتماعي، وتشغيل خاصية حجب معلومات التسجيل على نطاق إستضافة موقعهن، إلخ.

١١. أثناء قيام المشاركات بوضع لوائح بالخطوات التي يتوجب عليهن إتخاذها، شاركنا معهن بعض الموارد المفيدة لهن أثناء تطبيق بعض تلك الخطوات - قد يجدن ما يساعدهن أيضاً في إيجاد خطوات لم يفكرن بها بعد:

أداة حجب عناوين الإنترنت بشكل مؤقت (**Temporary URL Blocking**) يمكن استخدامها لحجب نتائج البحث عن المواقع - لا تقوم فعلياً بإزالة المحتويات ولكنها تحجب المحتويات القديمة التي قد تكون حساسة من نتائج البحث إلى أن يُحدّث الموقع الإلكتروني:

<https://support.google.com/webmasters/answer/1663419?hl=en&lr=all&rd=2>

حذف حسابات فايسبوك يحتوي على إرشادات حول كيفية حذف أو تعطيل صفحات على فايسبوك:

<https://www.facebook.com/help/224562897555674>

قاتل الحسابات **AccountKiller** يحتوي على إرشادات حول كيفية إزالة حسابات أوصفات عامة على المواقع وخدمات التواصل الاجتماعي الأكثر شعبية:

<https://www.accountkiller.com>

“جست ديليت مي” **JustDelete Me** دليل بالروابط المباشرة لحذف حسابات من خدمات إنترنت وخدمات التواصل الاجتماعي:

<http://justdelete.me>

١٢. لإختتام الجلسة، ذكرنا المشاركات أن عمليات الاستقصاء عن المعلومات الشخصية قد تكشف فقط معلومات متاحة للعموم عنهن؛ ولكن منصات التواصل الاجتماعي وخدمات الإنترنت نفسها قادرة على الإطلاع على المزيد. شددنا للمجموعة على أن التمتع بمستوى خصوصية أفضل ممكن من خلال استخدام كلمات سر أقوى وممارسة عادات تصفح أكثر أماناً والاستفادة من التشفير لحماية المعلومات من الآخرين.

المراجع

<https://gendersec.tacticaltech.org/wiki/index.php/Self-dox> •

باب ١٨

الجمهور الشبكي

- الأهداف: تعرّف هذه الجلسة المشاركات بمفهوم “الجمهور الشبكي” من أجل فهم بشكلٍ أفضل المسائل الرئيسية وتداعيات الدور المتزايد للتكنولوجيا في المجتمع.
- الطول: 20 دقيقة
- الشكل: Session
- مستوى المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
 - إطرحي علي ما تريدينه من أسئلة!^١
 - الخصوصية^٢
 - ماذا يمكن لبياناتكن الوصفية (Metadata) أن تفصح عنكن؟^٣
 - الإستقصاء عن المعلومات الشخصية الخاصة بالمتصيد^٤

<https://vrr.im/2b74>^١

<https://vrr.im/819e>^٢

<https://vrr.im/1598>^٣

<https://vrr.im/7480>^٤

• المواد اللازمة:

- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
- شرائح (عليها النقاط المفتاحية الواردة أدناه)

تستند هذه الجلسة إلى بحث أجرته دانا بويد Danah Boyd.

إدارة الجلسة

١. إبدآن الجلسة بالشرح أنها ستتركز على فهم أوضح لما يحدث حين تصبح التكنولوجيا مكوناً حيوياً وأساسياً أكثر فأكثر في المجتمع وتأثير ذلك على الهوية والخصوصية.
٢. إشرحن أنه من أجل توضيح ذلك، ستتقرن لبعض المفاهيم الرئيسية الواردة في بحث دانا بويد، الذي يحمل عنوان: "إخراج المراهقين الأميركيين من سياق علاقاتهم الاجتماعية مع الجمهور الشبكي"

الجمهور الشبكي هو في ذات الوقت المكان الذي أنشأته التكنولوجيات المستندة إلى شبكات المجتمع المتصور الذي ينشأ نتيجة لتقاطع الأشخاص بالتكنولوجيا وممارساتهم.
محتوى الجمهور الشبكي:

محتوى الجمهور الشبكي يتكون أصلاً من ناقلات معلومات (بايتس). حيث ينتج عن كل من التعبير عن الذات والتفاعلات مع الأشخاص محتوى قائم على ناقلات المعلومات للجمهور الشبكي.
أربع خصائص للجمهور الشبكي:

تشكل ميزات ناقلات المعلومات الخصائص الأربع الأساسية للجمهور الشبكي:

الثبات: تُسجل وتُأرشف كل عمليات التعبير على الإنترنت بشكلٍ آلي،

إمكانية النسخ: من الممكن نسخ المحتوى المكوّن من ناقلات معلومات؛ المرونة وقابلية التوسّع: احتمالية ظهور المحتوى كبيرة؛ إمكانية البحث: المحتوى الموجود لدي الجمهور الشبكي يمكن الوصول إليه عبر البحث. هذه الخصائص الأربع تحدد بنية الجمهور الشبكي والتفاعلات التي تحدث فيه.

ديناميكيات الجمهور الشبكي: الجماهير الخفية: لا تظهر كل الجماهير حين يساهم شخص ما على الإنترنت بمحتوي ما. وليسوا بالضرورة موجودين في الوقت ذاته. انعدام السياقات: غياب الحدود المكانية والاجتماعية والزمنية تجعل من المحافظة على سياقات إجتماعية محددة أمرًا صعبًا. عدم وضوح الفرق بين العام والخاص: من دون القدرة على السيطرة على السياق، يصبح الفرق بين العام والخاص عديم المعنى. ويصبح من الممكن قياس هذه الثنائية بطرق جديدة ويصبح من الصعب المحافظة على فرق واضح بينهما.

٣. إشرحن وقدمن أمثلة عن كل خاصية من الخصائص الأربع بالإضافة إلى الديناميكيات. ومن المفيد أن ترفقن ذلك بصور مرتبطة بكل واحدةٍ منها لتسهيل عملية الفهم على المشاركات.

المراجع

• <http://www.danah.org/papers/TakenOutOfContext.pdf>

باب ١٩

التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟

- الأهداف: في هذه الجلسة، ستركز المشاركات على التطبيقات والمنصات على الإنترنت التي يستخدمها عادةً - سيساعدن ذلك في تحديد أنواع المعلومات المشاركة مع هذه المنصات وفي وضع تكتيكات لإستخدامها بشكل آمن في نشاطاتهن الشخصية وعملهن على الإنترنت.
- الطول: 120 دقيقة
- الشكل: جلسة
- مستوى المهارة: أساسي
- المعرفة المطلوبة:
- معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
- وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)
- كيف يعمل الإنترنت؟ (أسس الأمن الرقمي، الجولة الأولى)
- جلسات/تمارين ذات صلة:

- إطرحي علي ما تريدينه من أسئلة!^١
- الخصوصية^٢
- الجمهور الشبكي^٣
- الحملات الآمنة على الإنترنت^٤
- المواد اللازمة:
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
 - شرائح (عليها النقاط المفتاحية الواردة أدناه)
 - أوراق (بضعة أوراق لكل مشاركة)
 - أوراق صغيرة لاصقة (بألوان مختلفة)
- التوصيات: يجب أن يكون مع المشاركات هواتفهن المحمولة أو جهاز واحد متصل بالإنترنت من أجل القسم العملي من الجلسة. قدمن للمشاركات موارد إضافية موصى بها يمكنهن فيها تعلّم المزيد عن الخصوصية وعن الخطوات التي يمكنهن إتخاذها لحماية خصوصياتهن بشكل أفضل (راجعن قسم المراجع للإطلاع على الروابط).

إدارة الجلسة

الجزء الأول - أجهزتنا وبياناتنا

١. أطلبن من المشاركات مراجعة كل التطبيقات الموجودة على أجهزتهن والتحقق مما يلي:
 - الأذونات المعطاة على الجهاز لكل تطبيق؛
 - سياسات الخصوصية لدي التطبيقات، لمعرفة ما يمكن القيام به بالبيانات التي لدي التطبيق إمكانية الوصول إليها؛
 - هوية مطور كل تطبيق.

<https://vrr.im/2b74¹>

<https://vrr.im/819e²>

<https://vrr.im/a184³>

<https://vrr.im/8e6b⁴>

٠٢. إعطين المشاركات مهلة 15 دقيقة للقيام بما ورد أعلاه. بعد إنتهاء هذه المهلة، أطلبين من المشاركات مشاركة ما إكتشفنه بعد عملية البحث السريعة هذه. إحرصن على التحدّث عن مسائل من قبيل:

- أذونات التطبيقات التي لا علاقة واضحة لها مع وظيفتها الفعلية؛
- شروط خدمة غير واضحة أو مكتوبة بشكلٍ مبهم؛
- سياسات خصوصية تسمح للشركات ببيع بيانات المستخدمين للغير.

٠٣. شاركن أمثلة عن التطبيقات التي تتابع الدورة الشهرية علي سبيل المثال تطبيق My Calender والتطبيقات الأخرى الخاصة بمتابعة الصحة الشخصية مع المجموعة. فسرن لمن كيف يتم ذلك وأنه وفقاً للبحوث فقد تبين أن هذه التطبيقات قادرة على جمع كم لا بأس به من البيانات الشخصية من المستخدمين.
على سبيل المثال:

الاسم ورقم الهاتف والعنوان

تفاصيل عن الجسم كالألم الناتج عن الدورة الشهرية والوزن وعدد ساعات النوم؛
الحالات العاطفية كالإجهاد أو نقص التركيز أو القلق؛
تفاصيل عن الصحة الجنسية بما في ذلك وسائل منع الحمل؛
السلوك على الإنترنت كعدد النقرات ونوعها وأنواع الأجهزة المستخدمة؛
السلوك خارج الإنترنت بما في ذلك الأدوية المتناولة أو عادات الشرب أو التدخين.
هذا كم هائل من المعلومات، أليس كذلك؟

الجزء الثاني - من يتعقبنا أيضاً؟

٠٤. قسمن المشاركات إلى مجموعات من 3 إلى 4 مشاركات كحد أقصى وأطلبين من كل مجموعة وضع لأحة بما يعرفه عن فإيسبوك وغوغل - لتقديم مثال، يمكنكن الطلب

منهن البدء بالإجابة على هذه الأسئلة:

- هل هذين اليكانيين شركتين فعليتين؟
- ما هي أهداف أو رؤى هاتين الشركتين؟
- ما هي الخدمات التي تقدمانها؟
- هل هذه الخدمات مجانية أو مدفوعة؟
- ما هي قواعد/شروط استخدام تلك الخدمات؟

أهملن المشاركات 15 دقيقة للإنتهاء من وضع القائمة بكل المعلومات التي يعرفها.

٥. ما أن ينتهي الوقت المخصص، أطلبن من كل مجموعة وضع لائحة بما قد تعرفه شركتا فإيسوك وغوجل عنهن. في حال توفر للمشاركات إمكانية الوصول إلى الإنترنت من حواسيبهن أو هواتفهن المحمولة، ومن منهن لديها حساب على جي مايل Gmail يمكنها زيارة صفحة <https://www.google.com/maps/timeline> أيضاً للمساعدة في هذا الجزء من الجلسة. أهملن المشاركات من 20 إلى 25 دقيقة لوضع لوائحهن التي ستقوم كل مجموعة بعرضها على بقية المشاركات بشكلٍ موجز.

الجزء الثالث - الترويج لحقوق المرأة على شبكات التواصل الاجتماعي

٦. في هذا الجزء من الجلسة، حافظن على المجموعات بشكلها الحالي - ستعطين كل مجموعة سؤالاً لمناقشته وتحليله معاً (من الأسئلة الواردة في اللائحة أدناه):

ما هي الأدوات أو منصات الإنترنت التي نستخدمها لتنظيم وتبادل المعلومات عن حركاتنا الاجتماعية، تظاهراتنا وحملاتنا؟ ما هي الجوانب الإيجابية والسلبية لاستخدام هذه الأدوات لهذا الغرض؟ هل نعلم بأي أمثلة عن حملات محظورة أو صفحات أزالتها موقع فإيسوك أو فيديوهات محظورة على موقع يوتيوب أو أمثلة أخرى عن حسابات أغلقت على منصات التواصل الاجتماعي؟ شركات كشركة فإيسوك وغوجل تربطها علاقات وطيدة مع حكوماتنا ويعرف عنها أنها تبادل معلومات المستخدمين معها (<https://govtrequests.facebook.com>) ما تداعيات ذلك علينا؟ هل نعرف

بأي حالات عنف ضد النساء على الإنترنت بشكل عام؟ وبشكل خاص، أي حالات تلتقت فيها مدافعات عن حقوق الإنسان تهديدات على الإنترنت أو نشرت صور لهن وهن عاريات أو أنشأت حسابات على مواقع التواصل الاجتماعي للتشهير بهن أو "للترويح" لخدماتهن الجنسية؟ على أي منصات حصلت هذه الحوادث وكيف تعاملت المنصة مع ذلك؟

أطلبين من كل مجموعة التفكير في إجابات على هذه الأسئلة خلال 10 إلى 15 دقيقة؛ وما أن ينتهي الوقت المخصص لذلك، أطلبين من كل مجموعة مشاركة خلاصاتها مع بقية المشاركات.

٧. معاً كمجموعة، فكرن خلال 5 إلى 10 دقائق في كيفية استخدام هذه المنصات أيضاً كأماكن يجتمع فيها عدد كبير من المستخدمين/ات على الإنترنت - من هنا، تبدو هذه المنصات أماكن مثالية لتنفيذ جهود الحملات. في النهاية، خدمة فايسبوك والخدمات الأخرى المقدمة من غوغل توفر طرق مفيدة للتفاعل مع المتابعين وأفراد المجتمع؛ لذا على الرغم من المخاوف أو سلبيات هذه المنصات، يجب ألا ننسى أن المشاركات قد يرغبن بالإستمرار في إستخدامها للتواصل مع جماهيرهن.

الجزء الرابع - إستعادة الخصوصية

٨. ستقدن الآن المشاركات في الجزء الختامي من الجلسة. إشرحن لهن أنكن ستلقين نظرة الآن إلى الطرق التي يمكن من خلالها إستعادة الخصوصية على الإنترنت، عبر تعلّم كيفية الإستمرار في إستخدام التطبيقات والمنصات ومواقع التواصل الاجتماعي هذه للإستخدام الشخصي أو لجهود المناصرة ولكن بطريقة أكثر أماناً.

٩. مع إبقاء المشاركات في المجموعات ذاتها من التمارين السابقة، أطلبين منهن التركيز الآن على طرق إبداعية في التفكير بشكل جماعي لإستعادة خصوصيتهن. أعطين كل مجموعة رزمة أوراق صغيرة لاصقة بالإضافة إلى أقلام خطاطة وأقلام عادية. ومن ثمّ أطلبين منهن تقديم أكبر قدر ممكن من الأفكار خلال 10 إلى 15 دقيقة. يمكنكن تقديم

أمثلة عن بعض التكتيكات ليتمكن من البدء بالتفكير، عل سبيل المثال:

- إرباك الخوارزميات (algorithms) التي تستعين بها المنصات لأغراض الإعلان أو تحسين المحتوى؛
- مراجعة سياسات الخصوصية ومستجدات إعدادات الخصوصية بشكل دوري؛
- التنبه للأذونات المعطاة للتطبيقات على أجهزتهم، لا سيما تلك المرتبطة بإعدادات تحديد الموقع الجغرافي وتحديد الموقع الجغرافي للصور والمنشورات؛
- استخدام منصات بديلة ملتزمة إلى حد أكبر بالخصوصية والعمل في مجال حقوق الإنسان (رايز اب Riseup وتوتانوتا Tutanota وسيجنال Signal...إلخ).

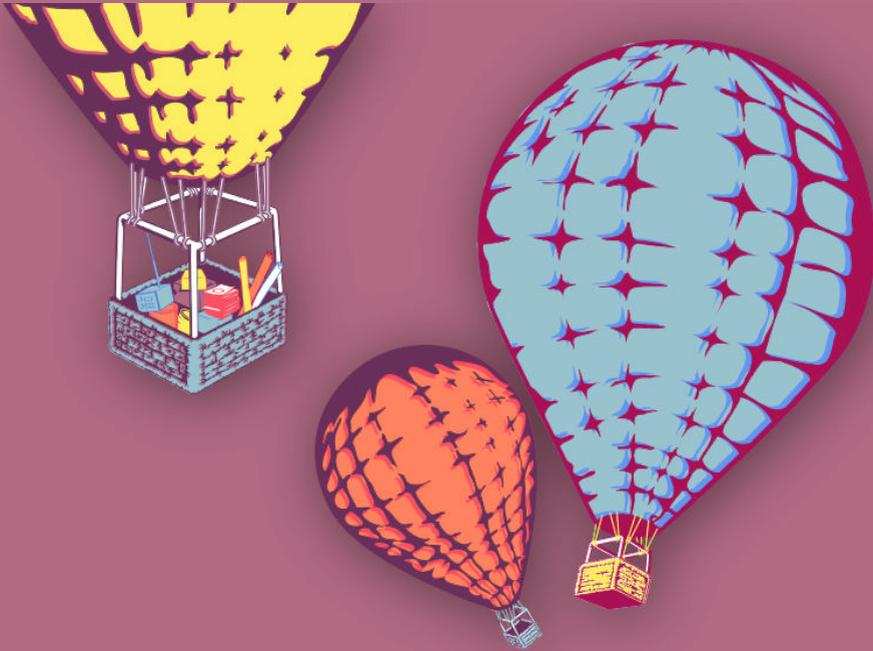
ما أن ينتهين من هذا الجزء الأخير من التمرين، أطلبن من كل مجموعة مشاركة بعض الأفكار التي توصلن إليها - يمكنكن عرض هذه الأفكار في مكان ظاهر في غرفة التدريب لكي تتمكن المشاركات من العودة إليها مع تقدمهن في التدريب. هذه الأفكار ستكون مفيدة لكن أيضاً عند تعديلكن محتوى تدريبيكن، لا سيما إذا أرادت المشاركات التركيز بشكل أكبر على تحسين مستوى إستخدامهن الآمن لشبكات التواصل الإجتماعي في عملهن.

المراجع

- <https://theglassroomnyc.org/data-detox/>
- <https://chayn.gitbooks.io/advanced-diy-privacy-for-every-woman/content/>
- <https://rankingdigitalrights.org/>
- <https://myshadow.org/>
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_man_ual



النساء فى فضاء الإنترنت



المناصرة الآمنة على
الإنترنت

باب ٢٠

مواقع إلكترونية أكثر أماناً

- الأهداف: في هذه الجلسة، ستساعدن المدافعات عن حقوق الإنسان في تحديد الممارسات الآمنة الواجب تطبيقها عند إدارة وحماية مواقعهن الإلكترونية - قد تكون المواقع هذه مواقعاً شخصية يستخدمنها في نشاطهن على الإنترنت أو مواقع إلكترونية خاصة بمنظماتهن/جماعاتهن/حركاتهن.
- الطول: 50 دقيقة
- الشكل: جلسة
- مستوي المهارة: متقدم
- المعرفة المطلوبة:
- معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
- معرفة سابقة بكيفية إدارة المواقع الإلكترونية
- بمن تثقن؟ (تمارين بناء الثقة)
- جلسات/تمارين ذات صلة:
- بمن تثقن؟¹

<https://vrr.im/bd0d1>

- التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟^٢
- الحملات الآمنة على الإنترنت^٣
- المواد اللازمة:
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
 - شرائح (عليها النقاط المفتاحية الواردة أدناه)
- التوصيات: هذه الجلسة تناسب مجموعات معينة أكثر من غيرها - ضمن هذه الجلسة على رأس سلم الأولويات لا سيما للناشطات أو الجماعات التي لديها موقع إلكتروني.
- من المفيد تحضير بعض الأمثلة قبل هذه الجلسة (من تقارير إخبارية أو منشوات على مدونات أو منشورات على وسائل التواصل الاجتماعي أو تجارب شخصية) عن الهجمات الإلكترونية ضد المدافعات عن حقوق الإنسان و/أو منظمات الدفاع عن حقوق الإنسان أو اختراقات المواقع الإلكترونية أو عمليات تدمير المواقع بشكل خاص.
- لا تنسين أنه في بعض الحالات، قد لا تقوم المنظمات بإدارة مواقعهن الخاصة. أو قد تعتمد قدرتها على إجراء التغييرات على مواقعها على قرارات المنظمات غير الحكومية الدولية الأكبر التي تدعمها. في كلا الحالتين، حتى لو لم تكن المشاركات قادرات على إدخال تغييرات مباشرة على عمليات إدارة مواقعهن، تقدم هذه الجلسة مع ذلك أساساً صلباً يمكن بواسطته البدء بالتفكير في التغييرات التي قد يقترحها (أو تولى سيطرة أكبر في مسألة إدارة مواقعهن).

إدارة الجلسة

الجزء الأول - ما الأشكال الممكنة للهجمات الإلكترونية؟

١. إبدأن الجلسة بمراجعة بعض الإجابات المقدمة خلال جلسة "بمن نثقن؟" (تمارين بناء الثقة) - وأذكرن بشكل خاص بعض الخوصوم المحتملين بحسب المشاركات أنفسهن.
- سيوفر لكن ذلك أساساً مفيداً لتناول مسألة سلامة المواقع الإلكترونية بشكل عام

^٢ <https://vrr.im/47ba>

^٣ <https://vrr.im/8e6b>

والمساحات الإلكترونية الخاصة بالناشطات بشكلٍ خاص.

٠٢. إسألن المشاركات - ما الذي يعتبره هجوماً على الإنترنت؟ ما هي حالات الهجوم الإلكتروني التي سمعن عنها؟ . وفي حال كان ذلك مناسباً، يمكنكن أن تسألن إن كانت أي عضوة من عضوات المجموعة تعرّضت لهجوم في السابق، إما على صعيد فردي أو ضمن نطاق منظمته/جماعتها. يمكنكن أيضاً تقديم بعض دراسات الحالات المعدّة مسبقاً من قبلكن في حال لا تتوفر لدى المشاركات أمثلة يمكنهن مشاركتها.
٠٣. إطرحن أسئلة متابعة بشأن الحالات التي تمت مشاركتها. هل سُئِر الهجوم ضمن سياق معين قبيل ملاحظة أو عرض تقرير ما أو نوع آخر من التجمعات العامة؟ ما كان شكل تعامل المدافعات عن حقوق الإنسان مع الهجوم؟ هل وُثِق الهجوم؟

الجزء الثاني - حماية المواقع الإلكترونية

٠٤. إستناداً إلى الأمثلة التي تمت مشاركتها، يمكنكن الآن البدء بمشاركة بعض التوصيات الأولية بشأن الممارسات لتحسين مستوى حماية مواقعهن الإلكترونية. بعض الأمثلة تتضمن ما يلي - بحسب المستويات المختلفة من المعرفة ضمن المجموعة، قد يتوجب عليكن تقديم شروحات أكثر تفصيلاً لكل واحدة منها:
- إختياري: حتى بالنسبة للمجموعات المزوّدة بحد أدنى من المعرفة أو المعلومات بشأن إدارة المواقع، قد يكون من المفيد شرح الطرق التي تدار المواقع بواسطتها قبل الإنتقال إلى التوصيات الواردة أدناه. قد تتضمن بعض مواضيع الأمثلة أنواع النطاقات ونظام أسماء النطاقات (Domain Name System DNS) و استضافة المواقع ونُظْم إدارة المحتويات (Content management system CMS).

حماية موقعك

- استخدم كلمات سر قوية لإدارة الموقع لتفادي تعرض الموقع للاختراق - إستغلال
الخصوم كلمات السر الضعيفة للوصول إلى الجهة الخلفية لأحد المواقع يعتبر من الطرق
الشائعة التي تُعرض بها المواقع للاختراق. في حال كان ذلك ممكناً، فعلن خاصية
التحقق بخطوتين في حساب الموقع وخدمة الإستضافة وأي بوابات وصول أخرى.
- عند تسجيل اسم مجال ما، غالباً ما يتطلب الأمر من الشخص الذي يقوم بالتسجيل
تقديم معلومات من قبيل اسمه/ها وعنوانه/ها وبريده/ها الإلكتروني. تحقق لمعرفة
ماهية المعلومات المتوفرة في ملف تسجيل مجال معين وفكرن في تغييره إلى ملف تسجيل
مجال خاص (استخدام <http://whois.net> طريقة سهلة للتحقق من ذلك).
- ما هو الموقع الجغرافي الذي تم فيه إستضافة نطاق الموقع؟ لا بد من أخذ عوامل متعددة
بعين الإعتبار في هذا الصدد، لا سيما:
 - في أي دولة (أو حتى مدينة) تتواجد خوادم المضيف؟ هل يمكن الوثوق
بحكومة تلك الدولة بشأن بياناتك، والسؤال الأهم، هل يمكن الوثوق بأن
خدمة الإستضافة لن تسلّم بياناتك بناءً على طلب الحكومة؟ هل قد تحاول
حكومة تلك الدولة التدخل بموقعك أو تحاول تدميره؟
 - فكرن في مدى فائدة شراء خدمات الإستضافة من خلال بائع ثاني، ففي بعض
الهيئات قد تحتجن لفريق دعم جيد قادر على مساعدتك، لذا إحرصن على
القيام بالخيارات الصائبة. إحرصن على التأكد من ذلك، لأن بعض خيارات
الإستضافة تعرف بأن الدعم الفني لديها سيء.
- تحققن من البرامج المضافة التي يستعين بها موقع ما حالياً - هذا النوع من البرامج شائع
بشكل خاص على المواقع التي تستعين بمنصات كورد برس Wordpress كنظام إدارة
معلومات. إحرصن على استخدام البرامج المضافة الضرورية فقط، وتحققن من أن أي
برنامج إضافي مستخدم حالياً مصنوع من مصدر موثوق به.

- فكرن في تثبيت برامج خدمات من قبيل برنامج "جت باك" Jetpack من شركة أوتوماتيك Automatic على منصة وورد برس لا سيما للخدمات مثل العناصر التفاعلية (wid-gets) الخاصة بالتواصل الاجتماعي والتعليقات ونماذج الاتصال. تتوفر أيضاً برامج مضافة خاصة بأمن المواقع الأساسي من قبيل "بيتر دلبوي سيكيوريتي" Better WP Security، بالإضافة البرامج المضافة الخاصة بالنسخ الاحتياطية الآلية للبيانات من قبيل "فولت برس" VaultPress أو "باك أب بودي" Backup Buddy.
- إحرص على إجراء تحديثات على الخوادم المستضيفة للموقع بشكلٍ دوريّ (في حال لم تكن هذه التحديثات مدارة تلقائياً من قبل خدمة الإستضافة)، بالإضافة إلى أي تحديثات مدخلة على نظام إدارة المعلومات أو البرامج المضافة أو أي منصة أخرى مستخدمة للإدارة والتسيير.

حماية زوار مواقعك

- يوصى بشكلٍ كبير أن تقدم المواقع للمستخدمين والمستخدمات صلات مزودة ببروتوكول نقل النص الفائق الأمان (HTTPS) بشكلٍ تلقائيّ (وليس فقط اختيار) - خدمة "ليتس إنكريبت" Let's Encrypt من مؤسسة إلكترونيك فرونتير Electronic Frontier Foundation هي خدمة تتولى دور هيئة الشهادات وتقدّم شهادات ببروتوكول نقل النص الفائق الأمان مجاناً.
- تعمل جماعات كثيرة حول العالم على دعم جهود الناشطين في مجال التكنولوجيا وتخصص في العمل مع منظمات الناشطين مثل: "فروتلاين ديفنדרز" Frontline Defenders، "إلكترونيك فرونتيرز فاوندايشن" EFF، لجنة حماية الصحفيين CPJ، "أيفكس" ifex، "منظمة تكتيكل تكنولوجي كوليكثيف Tactical Technology Collective، منظمة تبادل الإعلام الاجتماعي SMEX، "آي ركس" IREX، و"إنترنيوز" Internews.
- سبق أن تعرضت منظمات أو مواقع إلكترونية لهجمات حجب الخدمة الموزعة في الماضي، فكرن في الإستعانة بخدمات الحماية من هذه الهجمات المقدمة من مبادرات

كثيرة منها “ديفلكت” Deflect أو “بروجكت شيلد” Project Shield. مبادرة “ديفلكت” التي تديرها منظمة “إيكواليتي. إي إي” Equalit.ie من مونتريال، كندا، هي عبارة عن خدمة مجانية بالكامل وموثوق بها بشكل كبير في مجتمع الأمن الرقمي. إختياري: فكن في مشاركة الموارد بشأن التعامل مع هجمات حجب الخدمة الموزعة، مثل::

<https://github.com/OpenInternet/MyWebsiteIsDown/blob/dev/MyWebsiteIsDown.md>

المراجع

- <https://onlinesafety.feministfrequency.com/en/>
- <https://www.apc.org/>
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_man_ual/en

باب ٢١

الحملات الآمنة على الإنترنت

- الأهداف: تهدف هذه الجلسة إلى مشاركة توصيات الأمن الرقمي للمدافعات عن حقوق الإنسان اللواتي يعملن على حملات على الإنترنت.
- الطول: 50 دقيقة
- الشكل: جلسة
- مستوى المهارة: متوسط
- المعرفة المطلوبة:
- بمن نثقن؟ (تمارين بناء الثقة)
- جلسات/تمارين ذات صلة:
- بمن نثقن؟^١
- بناء كلمات سرّ قوية^٢
- البرمجيات الخبيثة والفيروسات^٣
- كيفية حماية حاسوبك^٤
- الخصوصية^٥

<https://vrr.im/bd0d>^١

<https://vrr.im/f794>^٢

<https://vrr.im/47e5>^٣

<https://vrr.im/ac95>^٤

<https://vrr.im/819e>^٥

- التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟^٦
 - مواقع إلكترونية أكثر أماناً^٧
 - نموذج المخاطر القائمة على النوع الاجتماعي^٨
 - المواد اللازمة:
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
 - شراخ (عليها النقاط المفتاحية الواردة أدناه)
 - التوصيات: الهدف من هذه الجلسة هو جعل المشاركات قادرات على تحديد حلول في مجال الأمن الرقمي، يستطعن تنفيذها من أجل نشاطات حملات على الإنترنت أكثر أماناً؛ ولكن الهدف النهائي ليس أن يطبقن هذه الحلول خلال الجلسة، بل أن يبدأن عملية إستكشاف لتحديد تلك الحلول المناسبة لبيئتهن الفردية.
- تستند هذه الجلسة إلى دليل إرشادي موضوع من قبل إنديرا كورنيлио Indira Cornelio لصالح "سوشل تي آي سي" SocialTIC

إدارة الجلسة

الجزء الأول - المقدمة والتخطيط الوقائي

١. إشرحن للمشاركات أن هدف الجلسة هو تحديد الحلول في مجال الأمن الرقمي، التي يمكن تطبيقها من أجل نشاطات حملات على الإنترنت أكثر أماناً. لن يتوجب عليهن تطبيقها مباشرة خلال الجلسة. ولكن الهدف هو أن يبدأن بعملية إستكشاف من أجل تحديد تلك الحلول المناسبة لبيئتهن الفردية وحملتهن.
٢. أطلبن من المشاركات مشاركة بعض الأمثلة عن الحملات على الإنترنت التي يعرفن عنها - هل يمكنهن تحديد أي أنماط معينة في كيفية تنفيذ هذه الحملات؟

^٦ <https://vrr.im/47ba>

^٧ <https://vrr.im/bdeb>

^٨ <https://vrr.im/c0c3>

٣. ذكّن المشاركات أنه حين يتعلق الأمر بتنظيم حملاتهن الخاصة على الإنترنت وجهود المناصرة، يجب ألا ينسين المعلومات والخصوم الذين تم تحديدهم خلال تمرين بمن تثقن؟. بما أن الحملات بطبيعتها، جهود عامة جداً، لا بد لمن من التنبه جيداً لمن قد يراقبهن أو من قد يشكل تهديداً لهن.

٤. في سياق عملهن، إقترحن على المشاركات أنه عندما يحين وقت البدء بمرحلة التخطيط لجهود الحملات على الإنترنت، سيتوجب عليهن مع فرق عملهن على الإجابة على الأسئلة التالية:

- ما هو موضوع الحملة؟
- ما هو الجمهور المستهدف الرئيسي؟ ما رأيهن بالموضوع أو المسألة؟ هل هن معه أم ضده؟
- من سيشعر بأنه مستهدف أو مكشوف من قبل هذه الحملة؟
- ما هي الحجج المحتملة التي يمكن استخدامها ضد هذه الحملة؟
- ما هي النتائج الأفضل والأسوأ لهذه الحملة؟

٥. الإجابة على هذه الأسئلة قد تساعدهن في التخطيط لتدابير إحترازية ضد التهديدات الممكنة بشكل إستراتيجي أكثر - التأكيد على المجموعة أنه يمكنهن حتى إعداد رسائل مسبقاً رداً على السيناريوهات الممكنة الناتجة عن الردود على هذه الأسئلة. إضافة إلى ذلك، ذكّن المشاركات أن وضع تصور لأفضل سيناريو ممكن للحملة قد يساعدهن في التخطيط للتدابير الإحترازية - على سبيل المثال، كيف يمكن أن يحضرن لإحتمال ألا يتمكن موقعهن من تحمّل الإرتفاع المفاجئ لعدد زوار الموقع وأن ينهار على أثر ذلك، في حال لاقت الحملة نجاحاً ورواجاً كبيراً؟

٦. والآن، إشرحن للمجموعة أنه خلال الأجزاء التالية من هذه الجلسة، ستقمن بتوفير التوجيهات والتوصيات بشأن ممارسات الأمن الرقمي المفيدة في جهود الحملات على الإنترنت (إن أمكن، بحسب الوقت المتوفر للعمل على ذلك، إسمحن للمشاركات زيارة مواقع الأدوات الموصى بها).

الجزء الثاني - حماية الأجهزة

٧. إسألن المشاركات إذا كنَّ يستخدمن أجهزتهن الشخصية لتنفيذ الحملة (مقابل جهاز "العمل") - ما كمية المعلومات المرتبطة بالحملة التي تخزن على هذه الأجهزة؟ هل هي متصلة أيضاً بعنوان البريد الإلكتروني وحسابات مواقع التواصل الإجتماعي؟

٨. إلیکن بعض الممارسات الأساسية الواجب التوصية بها للمجموعة في مسألة حماية الأجهزة:

حماية حواسيبهن وهواتفهن المحمولة بواسطة كلمة سرّ؛
ثبيت برمجيات مكافحة للفيروسات على كل من حواسيبهن وهواتفهن المحمولة؛
إجراء عمليات نسخ إحتياطية بشكلٍ دوريٍّ للبيانات المهمة أو الحساسة (تسجيلات الفيديو أو الصوت، ملاحظات المقابلات، التقارير...إلخ).
تفعيل تشفير القرص الكامل على أجهزتهن:

في الهواتف المحمولة التي تعمل بواسطة نظام أندرويد و ماك آي أو إس، يمكن تفعيل ذلك عبر إعدادات الهاتف؛

في الحواسيب المحمولة، تعتبر برمجية "ماك أو إس إكس فايل فولت" (Mac OS X FileVault) وبرمجية "ويندوز بيتلوكر" (Windows BitLocker) من أكثر الخيارات الشائعة المتاحة لتشفير الأقراص تشفيراً شاملاً؛

ملاحظة: برمجية "فايل فولت" Filevault مقدمة مجاناً مع نظام "ماك أو إس أكس"؛ ولكن، برمجية "بت لوكر" لا تقدم مجاناً إلا مع نسخ "برو" Pro و"إنتربرايز" Enterprise و"إيديوكاشن" Education من ويندوز.

<https://en.wikipedia.org/wiki/FileVault>^٩
<https://en.wikipedia.org/wiki/BitLocker>^{١٠}

الجزء الثالث - إدارة إمكانية الوصول في الحسابات

٩. غالباً ما يتطلب الحملات على الإنترنت أن يعمل عليها مستخدمون ومستخدمات عديدين من أجل التمكن من الوصول إلى الحسابات ذاتها (أو الأجهزة، في بعض الحالات). تؤدي إمكانية الوصول إلى جهاز أو حساب من قبل عدة مستخدمين أو مستخدمات بواسطة بيانات الدخول ذاتها إلى إرتفاع حاد للخطر؛ ولكن، من خلال إتخاذ بعض التدابير الإحترازية، تستطيع المشاركات تقليص إحتمالية أن تتحول هذه المخاطر إلى تهديدات مباشرة بشكل ملحوظ. علي سبيل المثال يمكن عمل الآتي:

بالنسبة لكل الحسابات على الإنترنت والأجهزة المشتركة، يعتبر تحديد لأحة بأقل عدد ممكن من الأشخاص المخولين بالوصول من التدابير الأولى الأهم الواجب تطبيقها؛ ومن التدابير الأخرى، الحرص على الإلتزام بروتوكولات أو إجراءات معينة بشكل منتظم (لا سيما في ما يخص التوصيات التالية) : بالنسبة للنصتات على الإنترنت بشكل خاص، يجب أن تحرص كل عضوات الفريق اللواتي مُنح إمكانية الوصول على التحقق بشكل دوري من سجل الاستخدام والنشاط على الحسابات المشتركة - على سبيل المثال، يمكنهن على حسابات "جي مايل"/"غوغل"، التحقق من سجل عمليات تسجيل الدخول الحديثة (وإعداد إنذارات للنشاطات المشبوهة) ضمن "نشاط الحساب الأخير" (Last Account Activity)؛ وعلى نحو مماثل، في فايسبوك يمكنهن الدخول إلى سجل النشاطات على الحساب المشترك للتحقق من النشاط المستجد؛

تطبيق ممارسات كلمات السرّ القوية الأساسية لكل الأجهزة والحسابات التي ستستخدم في أي حملة. تسمح برامج إدارة تخزين كلمات السرّ الآمنة من قبيل "كي باس" -Keep- ass"/"كي باس إكس" KeePassX¹¹ بإنشاء ملفات قواعد بيانات فردية لكلمات سرّ الحسابات، التي تكون محمية بدورها بواسطة كلمة سرّ رئيسية؛ على نحو مماثل، بالنسبة للحسابات على غوغل وفايسبوك وتويتر يوصى بتفعيل خاصية التحقق بخطوتين التي توفر مستوى إضافي من القدرة على التحكم؛ في حال كان لا بد من مشاركة كلمة سرّ ما مع

¹¹ <http://keepass.info/>

أعضاء الفريق، وفي حال لم يكن القيام بذلك وجهاً لوجه ممكناً، يعتبر خيار إرسال كلمات السر عبر البريد الإلكتروني المشفّر - بواسطة برمجية جي بي جي GPG أو بواسطة خدمة مثل خدمة توتانوتا^{١٢} Tutanota أو عبر الرسائل المشفّرة (بواسطة تطبيق سيجنال على هاتف محمول) من الخيارات الأكثر أماناً - في حال استخدام تطبيق سيجنال، إحرصن على تحديد بروتوكول مع أعضاء الفريق حول عملية حذف الرسائل المزوّدة بكلمات السرّ من أجهزتهن ما إن تصلهن.

الجزء الرابع - اختيار التطبيقات للحملة

١٠. عند تنفيذ وتنظيم حملة على الإنترنت، من الشائع استخدام تطبيقات وأدوات معيّنة للتمكن من متابعة أرقام وسائل التواصل الاجتماعي/الموقع الإلكتروني، أو لتحديد جدول زمني للمنشورات على وسائل التواصل الاجتماعي. وعند إتخاذ القرارات بشأن مثل هذه التطبيقات واختيار تلك التي ستستخدم، لا بد أن تأخذ المشاركات بعين الاعتبار بعض المسائل التي قد تساعدن بشكلٍ أساسي على تفادي مشاركة معلوماتهن بواسطة بعض الأدوات غير الآمنة أو الأدوات التي لم تعد مدعومة من المطورين:

هل ما زال التطبيق فاعلاً، أي هل يتابع المطورون/ات توفير تحديثات على الأمان والخصائص بشكلٍ دوري؟

هل للتطبيق حسابات على مواقع التواصل الاجتماعي يمكننا متابعتها والتفاعل معها؟ ماذا يقول المستخدمون الآخرون عن التطبيق على الإنترنت على قنوات التواصل الاجتماعي الخاصة بهم؟

هل تتوفر أي منشورات على مدونات عن التطبيق مؤخراً؟

^{١٢} <https://tutanota.com/>

الجزء الخامس - بناء المجتمعات من خلال فإيسبوك

١١. غالباً ما يستخدم فإيسبوك في الحملات على الإنترنت من أجل تنظيم المجتمعات ونشر الرسائل المهمة وأي إتصالات أخرى بسرعة. ولكن لا بد تسليط الضوء على بعض نقاط الضعف المحتملة عند إستخدام هذه المنصات كجزء من البنية التنظيمية الأساسية للحملة:

يجب أن تدرك المشاركات أن لإستخدام فإيسبوك (أو أي منصة تواصل إجتماعي كبيرة أخرى) تداعيات محتملة على هوياتهن الشخصية على الإنترنت - للتخفيف من مدى تعرضهن، يمكنهن إنشاء صفحات مخصصة لإدارة صفحات الحملة عوضاً عن إستخدام صفحاتهن الشخصية؛ تجدر الإشارة هنا أنه من الممكن الآن تلقي إشعارات من فإيسبوك تكون مشفرة بواسطة مفتاح جي بي جي العام مرتبط بحساب بريد إلكتروني - قد يكون ذلك مفيداً للدفاعات عن حقوق الإنسان اللواتي يرغبن في إتخاذ تدابير إضافية لفصل عملهن عن هوياتهن الشخصية على الإنترنت أثناء إدارة الحملات؛ يجب أن تخطط المسؤولات عن إدارة الحملات على الإنترنت بشكلٍ مدروس لأنواع المعلومات والإتصالات التي يشاركنها على منصات إلكترونية كمنصة فإيسبوك - فالأمثلة السابقة كثيرة عن إختراق صفحات حملات على فإيسبوك من قبل الخصوم، وهذا ما فرض على مديري الصفحات إغلاقها (أو أدى ذلك إلى تدمير الصفحة بالقوة من قبل المنصة بسبب تبليغ الخصوم عنها) قد يشكّل ذلك تراجعاً ملحوظاً بالنسبة للحملة وعملية تقدّم بناء المجتمع، لذا شدّدن للمشاركات على أهمية توفر قنوات إتصال وتنظيم بديلة - قد تتضمن هذه القنوات:

تطوير مجتمعات فاعلة على منصات أخرى في الوقت ذاته، لكي تتوفر منصة إحتياطية يمكن الاعتماد عليها على الدوام؛

تستطيع المستخدمات أيضاً تنزيل المعلومات الموجودة على صفحة الفإيسبوك لإنشاء نسخ إحتياطية خارج الإنترنت، وهذه إستراتيجية جيدة؛

إستخدام خدمة تكلمة قوائم "رايز أب" ^{١٣} Riseup لإنشاء مجموعات بريد إلكتروني

^{١٣} <https://www.lists.riseup.net>

لإرسال نشرات إخبارية أو أي رسائل أخرى؛

تنظيم إجتماعات وجهًا لوجه إن أمكن؛ ولكن، بالنسبة للحملة التي تتناول قضايا معينة ودول معينة، لا بد من الانتباه إلى أن ذلك قد يشكل خطراً كبيراً لذا يوصى بعدم عقد مثل هذه اللقاءات؛

الجزء السادس - الموافقة عن دراية

١٢. ناقش أهمية الموافقة عن دراية مع المجموعة - لا بد من ذلك بشكلٍ عام في حملات التوعية بشأن قضايا حقوق الإنسان، ولا سيما عند الإستعانة بـ صور أو شهادات حية للضحايا والناجين وشاهدي العيان للأعمال الوحشية أو الانتهاكات الأخرى في مواد الحملة: قبل تسجيل الصور أو الفيديو لهؤلاء الأفراد، أو توثيق قصصهم، يجب أن يوافقوا بشكلٍ صريحٍ وواضحٍ على ذلك مسبقاً؛ وعلى نحوٍ مماثل، يجب أن يوافقوا أيضاً بشكلٍ صريحٍ وواضحٍ أن تُشارك أي مادة من هذه المواد مع عموم الناس - يجب أن تُشرح لهم بشكلٍ واضحٍ الغرض ومكان مشاركة هذه المواد والتداعيات المحتملة لذلك عليهم.

المراجع

- <http://seguridadigital.org/post/156287966318/consejos-de-seguridad-digital-para-gestionar-redes>
- <https://archive.informationactivism.org/en/index.html>

باب ٢٢

ماذا يمكن لبياناتك الوصفية (Metadata) أن تفصح عنك؟

- الأهداف: في هذه الجلسة، ستقدّم من مفهوم البيانات الوصفية وأهمية التنبيه للبيانات الوصفية الموجودة في أنواع مختلفة من المحتويات - لا سيما عند إجراء عمل حساس مرتبط بحقوق الإنسان.
- الطول: 90 دقيقة
- الشكل: جلسة
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- الجمهور الشبكي^١
- الحملات الآمنة على الإنترنت^٢

^١<https://vrr.im/a184>

^٢<https://vrr.im/8e6b>

- المواد اللازمة:
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
 - شرائح (عليها النقاط المفتاحية الواردة أدناه)
 - أمثلة عن أدوات لتحليل البيانات الوصفية وإزالتها
- التوصيات: مع أن ذلك ليس ضرورياً، إلا أن هذه الجلسة سوف تكون أفضل بشكلٍ كبير في حال حصلت المشاركات من قبل على جلسة الجمهور الشبكي . غالباً ما يعتبر موضوع البيانات الوصفية من الموضوعات المعقدة التي يمكن تقديمها في العملية التدريبية - إحرص على تخصيص الوقت الكافي لتقديم هذه الجلسة بالتفصيل، فهي مهمة جداً لبيئات عمل المدافعات عن حقوق الإنسان والناشطات الحقوقيات

إدارة الجلسة

الجزء الأول - ما هي البيانات الوصفية؟ Metadata

١. إبدأن الجلسة بمشاركة بعض النقاط الرئيسية مع المشاركات - أهمها يتضمن ما يلي:
 - إشرح ماهية البيانات الوصفية، وبعض الأماكن الشائعة التي قد تجدها فيها المشاركات (ملفات الصور، مستندات وورد Word/إكسيل Excel... إلخ.) شاركن بعض الأمثلة الشائعة عن البيانات الوصفية (تاريخ وتوقيت الإنشاء، مكان الإنشاء، أسم الكاتب/ة أو إسم المستخدم/ة، نوع الجهاز) - قد تطلبن من المشاركات إيجاد صورة أو ملف مشابه آخر على حواسيبهن لكي يتمكن من تحديد مكان البيانات الوصفية الخاصة بهن عليه، أو يمكنن مشاركة بعض الأمثلة عبر لقطات الشاشة عن بيانات وصفية كما تظهر في أنواع الملفات الشائعة. شرح الطرق المختلفة التي يتم من خلالها إنشاء بيانات وصفية، وكيفية تغييرها أو إزالتها بالكامل.
- غالباً ما يعتبر موضوع البيانات الوصفية من الموضوعات المعقدة التي يمكن تقديمها في العملية التدريبية، لذا إحرص على سؤال المشاركات إن كان المفهوم واضحاً بالنسبة لهن

- في حال لم يكن كذلك، خصصن الوقت اللازم للإجابة عن أسئلتهن بشكلٍ مفصّل
إستناداً إلى خبرتكن.

الجزء الثاني - تداعيات البيانات الوصفية في بيئة العمل على حقوق الإنسان

٢. عند العمل مع المدافعات عن حقوق الإنسان، لا بد من شرح إيجابيات وسلبيات
البيانات الوصفية - يمكنكن شرح ذلك بإيجاز للمشاركات من خلال فكرتين رئيسيتين:

١. تكشف البيانات الوصفية معلومات كثيرة عنكن أظهن من المشاركات إتقاط
صورة بهواتفهن والتحقق من كل البيانات التعريفية التي يحتويها ملف الصورة -
سيتوجب عليكن تزويدهن بأداة من قبيل "كاميرا في" CameraV للقيام بذلك،
أو يمكنكن مشاركة أداة على الإنترنت على غرار <http://metapicz.com>
في حال كان التدريب مخصصاً لمجموعة من المبتدئات. والآن، أظهن من
المشاركات إعادة التمرين ولكن هذه المرة مع تعطيل خدمات تحديد الموقع
الجغرافي على هواتفهن. قسمن المشاركات إلى مجموعات من 3 إلى 4 مشاركات
كحد أقصى لمناقشة أفكارهن حول مدى فائدة البيانات الوصفية وكيف برأيهن
قد تؤدي إلى تعريض أمنهن للنظر عند القيام بعمل في مجال حقوق الإنسان.
خلال نقاشهن، لا بد من المحافظة على التركيز على العمل في مجال حقوق الإنسان،
ولا بد للمشاركات أيضاً من تحديد ظروف إيجاد البيانات الوصفية في المستندات
أو الفيديوهات أو الصور التي قد تساعد في إعتبار هكذا محتوى دليلاً على توثيق
للعمل في مجال حقوق الإنسان. شاركن معهن بعض الممارسات - من قبيل
حفظ الملفات الأصلية على جهاز مشفر وإنشاء نسخ منفصلة لغايات التنقيح
والتعديل أو التخزين على حواسيبهن.

٢. تنشأ البيانات الوصفية ولكن من الممكن إزالتها أيضاً. أظهن المشاركات
على بعض الخيارات المتاحة، من قبيل "أوبسكورا كام" ObscuraCam أو
"ميتانول" Metanull، المخصصة لمسح البيانات التعريفية من الفيديوهات
والصور. في حال توفر الوقت الكافي للجلسة، قد تفكرن أيضاً بإضافة خيار مسح

البيانات التعريفية من المستندات بواسطة "ليبر أوفيس" LibreOffice.

المراجع

- <https://ssd.eff.org/en/module/why-metadata-matters>
- <https://guardianproject.info/apps/obscuracam/>
- <https://archiving.witness.org/archive-guide/create/how-capture-metadata/>
- <https://securityinabox.org/en/lgbti-mena/remove-metadata/>



النساء فى فضاء الإنترنت



هواتف محمولة أكثر أمانًا

باب ٢٣

ماركو بولو

- الأهداف: هذا التمرين البسيط مثاليّ لشرح كيفية عمل الهواتف المحمولة للمشاركة وكيفية تلقينا للرسائل النصية القصيرة والاتصالات الهاتفية وبيانات الاتصال بالإنترنت على أجهزتنا.
- الطول: 15 دقيقة
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- الخصوصية^١
- الجمهور الشبكي^٢
- المواد اللازمة:
- الإبداع!

يستند هذا التمرين إلى تمرين "ماركوبولو" الذي أنشأته مؤسسة كاريزما

^١<https://vrr.im/819e1>

^٢<https://vrr.im/a184>

إدارة الجلسة

٠١. اخترن إحدى المشاركات في المجموعة للعب دور "الهاتف المحمول" - من بعد تحديد المتطوعة، أطلبن منها مغادرة الغرفة.
٠٢. في المساحة المتوفرة لديكن في مكان التدريب، قسمن بقية المجموعة إلى "مبانٍ" و"هوائيات لاسلكية" وزعهن في كافة أرجاء الغرفة. إحرصن أن تتوزع الهوائيات بشكلٍ متساوٍ، بحيث تستطيع كل واحدة تحديد "نطاق" خاص بها في الغرفة. يمكن لكل مشاركة وضع دائرة على الأرض لتحديد نطاقها الخاص إذا كانت مساحة التدريب تسمح بذلك.
٠٣. أطلبن من الهاتف المحمول العودة إلى الغرفة، وإغماض عينيها. فسرن لها أنه سيتوجب عليها تحديد مواقع كل الهوائيات في الغرفة من خلال منادة كلمة "ماركو" - وستجيب الهوائيات بكلمة "بولو" ولكن فقط إذا مرّ الهاتف المحمول في جولتهن بالنطاق الخاص بكل هوائي. في هذا الأثناء يجب على المباني أن تبقى صامتة.
٠٤. أطلبن من الهاتف المحمول أن يحاول تحديد مواقع كل الهوائيات في الغرفة من خلال منادة كلمة "ماركو" - ما أن تنجح في تحديد مواقع كل الهوائيات، يمكنكن الآن شرح الوظائف الأساسية لشبكة الهواتف المحمولة:
تشغل شركات الاتصالات هوائيات في مناطق مختلفة، توفر كل واحدة منها التغطية لمنطقة (أو نطاق) معين؛
تتلقي الهواتف المحمولة التغطية عبر إرسال طلبات إلى الهوائيات الجديدة التي تلتقي بها ("ماركو") أثناء تنقلها من مكان لآخر، وترد الهوائيات بـ ("بولو") على الطلبات عبر تقديم التغطية.

باب ٢٤

الهواتف المحمولة، الجزء الأول

- الأهداف: تقدم هذه الجلسة للمشاركات لمحة عامة تعريفية حول كيفية عمل الهواتف المحمولة من خلال شبكات الإتصالات الهاتفية.
- الطول: 60 دقيقة
- الشكل: جلسة
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
 - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟^١
 - ماركو بولو^٢
 - المواد اللازمة:
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
 - أوراق
 - شرائح (عليها النقاط المفتاحية الواردة أدناه)

^١ <https://vrr.im/47ba>

^٢ <https://vrr.im/4450>

• التوصيات: هذه الجلسة لها فعالية قصوى في حال قُدمت مباشرة من بعد تمرين ماركو بولو من هذه الوحدة، ولكن يمكن تقديمها وحدها أيضاً.

هذه الجلسة نسخة معدلة من نشاط "كيف تعمل الهواتف المحمولة؟" التي وضعتها أليكس دون Alix Dunn (من منظمة "ذا أنجن روم" The Engine Room) لصالح منظمة "ليفل أب" LevelUp

إدارة الجلسة

إبدأ الجلسة بشرح المكونات الرئيسية للهواتف المحمولة للمشاركين. يمكنك عرض صور لكل مكون منها أثناء الشرح.

الجزء الأول - ما هي مكونات الهاتف؟

١. على الرغم من أن بعض الهواتف، لا سيما الهواتف الذكية منها، تتمتع بقدرات متطورة، تشارك كل الهواتف مكونات أساسية عدة منها الآتي:

الهوائي

الهوائيات اللاسلكية، التي تسمح بالتواصل بين الهاتف المحمول والشبكات الخارجية، قد تكون ظاهرة في الأجهزة الأقدم - حيث في بعض الأجهزة القديمة جداً كان من الضروري إخراجها يدوياً للتمكن من استخدامها. معظم الهواتف الحديثة العهد مزودة بهوائيات ضمن الجهاز مباشرة، لذا لم تعد "ظاهرة". عدا عن الهوائي المسؤول عن التواصل مع شبكة الهواتف، قد تكون هذه الهواتف الحديثة مزودة بهوائيات للاتصال بشبكة الإنترنت اللاسلكي؛ بعض المصنعين يجمعون هاتين الوظيفتين في هوائي واحد للجهاز.

البطارية

البطارية هي ما يخزّن الطاقة اللازمة لتشغيل الهاتف المحمول، في معظم الهواتف من السهل إزالة البطارية. وفي بعض الهواتف الذكية الأحدث (لا سيما هواتف الآي فون ولاحقاً هواتف سامسونغ غالاكسي إس)، لم تُصمّم البطاريات بشكل يمكن المستخدم من إزالتها وقد يصعب الوصول إليها حتى. البطاريات القابلة للإزالة مفضّلة للمستخدمين الذين يعتمدون تكتيكات لرفع مستوى أمنهم.

المعالج المصغّر للنطاق الأساسي Baseband Microprocessor

يتولى هذا المكوّن إدارة إتصالات الهاتف، بما في ذلك الإتصالات والأوامر التي يصدرها المستخدم للهاتف، ومن الهاتف من وإلى شبكة الهواتف. يعتبر النطاق الأساسي في أي هاتف عادةً "ملكية" مهمة من قبل المصنّعين وقد يعتبر "الصندوق الأسود" (لا يمكن الوصول إليه ويصعب التلاعب به) من حيث بروتوكولات إتصالاته وكيفية التحكم بها والوظائف الأخرى الخاصة بالشبكة/الجهاز. قدرة شبكات الهواتف على تشغيل الهاتف وتحديد موقعه والإستماع عبر المايكروفون وتنزيل البيانات من الجهاز كلها مرتبطة بالنطاق الأساسي للجهاز.

شريحة الهاتف ومكان وضعها

هذا هو مكان تخزين شريحة الهاتف في الجهاز المحمول. قدرة تخزين البيانات على شريحة هاتفك محدودة، ويمكن لبعض المستخدمين إتخاذ القرار بشأن حفظ بيانات معينة على شريحة هاتفهم أو في الذاكرة الداخلية للهاتف أو على وسائط قابلة للإزالة من عدمه. لا تنسين ذكر أن بعض الهواتف مصممة لتحمل أكثر من شريحة واحدة؛ الهواتف الأخرى التي لا تعمل على شبكات غير شبكات النظام العالمي للاتصالات المتنقلة (GSM) عادةً شبكات الوصول المتعدد باستخدام الشفرة المقسمة (CDMA) غير مزوّدة بشريحة.

الوسائط القابلة للإزالة

الوسائط القابلة للإزالة تشمل أي نوع من وسائط تخزين الذاكرة الخارجية التي يمكن إدخالها وإزالتها من أي جهازٍ محمول؛ غالباً ما تكون هذه الوسائط شرائح الذاكرة أو شرائح

الذاكرة المصغرة. بعض الهواتف مزودة أيضاً بمنافذ أشعة تحت الحمراء (infrared) لنقل البيانات عبر الأشعة من هاتف لآخر، بالإضافة إلى خاصية البلوتوث (Bluetooth) آلات التصوير

معظم الهواتف اليوم مزودة بآلات تصوير قادرة على إلتقاط الصور و/أو الفيديو، لا سيما الهواتف الذكية. وعدد لا بأس به منها مزوداً أيضاً بآلات تصوير في كل من الجهة الأمامية والجهة الخلفية من الجهاز، وغالباً ما تستخدم آلي التصوير هذه في تطبيقات إتصالات الفيديو من قبيل فإيسبوك مسنجر أو سكايب.

الجزء الثاني - الممارسة التطبيقية

٢. أطلبين من المشاركات العمل ضمن مجموعات من شخصين ووضع لائحة بالمخاطر أو التهديدات المرتبطة بالهواتف المحمولة؛ ومن ثمّ، أطلبين منهن وضع لائحة أخرى ببعض الممارسات الموصى بها التي يعتقدن أنها قادرة على حماية أجهزتهن، في ما يتعلق بكل مكون من المكونات المذكورة في الجزء الأول أعلاه.

٣. ما إن تنتهي كل مجموعة من العمل، أطلبين منها عرض حلولهن على بقية المجموعة. إنصتن لما يذكر من الممارسات والأدوات التالية في عروضهن - في حال لم يتم ذكر أحدها، إحرصن على ذكر شرح موجز عنها بعد أن تنتهي كل المجموعات من العرض: برامج مكافحة الفيروسات على الهواتف المحمولة الشبكات الافتراضية الخاصة التحقق من إعدادات ضبط التطبيقات كلمات سر قوية النسخ الاحتياطية للبيانات عدم شحن هواتفكن بواسطة منفذ اليوأس بي على أجهزة حاسوب عامة

المراجع

• <https://securityinabox.org/en/guide/mobile-phones>

<https://level-up.cc/curriculum/mobile-safety/how-mobile-networks-work/input/how-do-mobile-devices-work/> •

باب ٢٥

الهواتف المحمولة، الجزء الثاني

- الأهداف: تعرّف هذه الجلسة المشاركات ذوات المعرفة المتوسطة بالأدوات والتوصيات اللازمة لتحسين مستوى أمن هواتفهن المحمولة.
 - الطول: 50 دقيقة
 - الشكل: جلسة
 - مستوى المهارة: متوسط
 - المعرفة المطلوبة:
- ماركو بولو (هواتف محمولة أكثر أماناً)
 - الهواتف المحمولة، الجزء الأول (هواتف محمولة أكثر أماناً)
 - تعريف بمسألة التشفير (التشفير)
 - كيفية حماية حاسوبك (أسس الأمن الرقمي، الجولة الأولى)
 - جلسات/تمارين ذات صلة:
 - كيفية حماية حاسوبك^١
 - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟^٢

^١<https://vrr.im/ac95>

^٢<https://vrr.im/47ba>

- ماركو بولو^٣
- الهواتف المحمولة، الجزء الأول^٤
- المواد اللازمة:
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
 - شرائح (عليها النقاط المفتاحية الواردة أدناه)
- التوصيات: إن أمكن ذلك، حاولن معرفة أنواع الهواتف التي تستخدمها المشاركات قبل التدريب - على سبيل المثال، قد يرد سؤال عن ذلك ضمن عملية مسح تقييمية قبل التدريب. سيساعدكن ذلك في تعديل محتوى جلستكن ليتناسب وخصائص الأجهزة/أنظمة التشغيل التي تستخدمها المشاركات أصلاً. قبل البدء بالجلسة، ذكرن المشاركات ببعض ممارسات الأمن الرقمي الأساسية التي يمكن تطبيقها في الهواتف المحمولة من قبيل: تحميل برمجيات مكافحة الفيروسات على الهواتف المحمولة، والشبكات الإقترابية الخاصة للهواتف المحمولة، والتحقق من إعدادات التطبيقات وأذوناتها. أطلبن من المشاركات إجراء عملية نسخ احتياطي للملفات الموجودة على أجهزتهن قبل البدء بهذه الجلسة! بما أنهن سيستخدمن أجهزتهن الخاصة في هذه الجلسة، لا بد أن يقمن بعملية نسخ احتياطي لبياناتهن من باب الاحتياط.

إدارة الجلسة

الجزء الأول - التشفير في الهواتف المحمولة

١. ذكرن المشاركات بالجلسات السابقة التي تناولت مفهوم التشفير، لا سيما جلسة التعريف بمسألة التشفير - ولعلكن أيضاً ناقشتن سابقاً التشفير من حيث تشفير الأقراص بشكلٍ شامل خلال جلسة كيفية حماية حاسوبكن. أذكرن للمشاركات أن النسخ الأحدث من أنظمة آي أو أس وأندرويد (أيار/مايو 2017) مزودة بتشفير مفعّل تلقائياً.

^٣<https://vrr.im/4450>

^٤<https://vrr.im/7c02>

الجزء الثاني - استخدام برمجية جي بي جي على الهواتف المحمولة

٢. في حال كانت المشاركات تعرفن التشفير بواسطة برمجية جي بي جي GPG، قد من لمن خدمة البريد الإلكتروني "كاي 9" وبرنامج "آي بي جي" APG. ناقشن إيجابيات وسلبيات استخدام تشفير جي بي جي على هاتف محمول (لا سيما خطر تخزين مفتاح جي بي جي خاص على هاتف محمول في مواجهة نقاط الضعف الخاصة بالهواتف المحمولة) - المقصود هنا هو التشديد على أن هذه القرارات قد تختلف من بيئة لأخرى؛ سيتوجب على المشاركات الاختيار بأنفسهن إن كانت إيجابيات استخدام جي بي جي على هاتف محمول أكبر وأهم من السلبيات.

إختياري: إمنحن المشاركات الوقت الكافي لتثبيت والتدرّب على استخدام "كاي 9" و"آي بي جي" خلال الجلسة - قد يرغبن بتجربة المفتاحين الجديدين اللذين قمن بإنشائهما للتعرف على الأداة.

الجزء الثالث - هل يقوم هاتفك بتعقبك؟

٣. إسألن المشاركات - ما كمية المعلومات التي تعرفها هواتفنا عنّا؟ الهواتف هي وسيلة نستخدمها لإجراء عدد لا بأس به من أحاديثنا وبالتالي، هي قادرة على الوصول إلى معظم محتوياتها إن لم تكن كلها؛ وعلى نحو مماثل، لا تقوم الهواتف أيضاً بتعقب المحتوى فحسب بل تتعقب جهات الاتصال الخاصة بنا - فكل حديث مرتبط بفرد معين.

٤. قد ترغبن أيضاً في مناقشة كيف يمكن أن يعتبر نوع التعقب الذي يجريه الهاتف نوعاً من أنواع المراقبة، وكيف أن المراقبة قادرة على الحدوث من خلال طرق كثيرة أخرى غير الطرق الاعتيادية المتوقعة. إسألن المجموعة عن أنواع المخاطر أو التهديدات التي يشعرن أنها محددة بهواتفهن المحمولة، لا سيما في بيئة عملهن كمدافعات عن حقوق الإنسان.

المراجع

- <https://securityinabox.org/en/guide/mobile-phones>
- <http://www.zeit.de/datenschutz/malte-spitz-data-retention>



النساء فى فضاء الإنترنت



المحافظة على سرية
الهوية

باب ٢٦

الصديقة السرية

- الأهداف: في هذه الجلسة، ستشرح مفهوم المحافظة على سرية الهوية وستوجهن المشاركات في عملية ممارسة تطبيقية ستشعرهن بأهميته.
- الطول: 30 دقيقة
- الشكل: تمرين
- مستوى المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
 - المحافظة على سرية الهوية^١
 - المزيد من الهويات الإلكترونية!^٢
 - المواد اللازمة:
 - أقلام وأوراق لكتابة الرسائل ومغلقات
 - كراسي

^١<https://vrr.im/70ff>

^٢<https://vrr.im/e9f7>

- وعاء أو إناء
 - قصاصات صغيرة من الورق الأبيض
 - عصبة للعينين أو أي شيء آخر لتغطية العينين
- التوصيات: يوصى بإعلام المشاركات بهذا التمرين قبل مواعده وبما قد يترتب عنه. ولأن الوقت المتاح للتدريب محدود، من الممكن الحصول على أفضل النتائج من هذا التمرين إذا توفر للمشاركات بعض الوقت للتفكير بشأن الهويات التي سينشأها وبالتالي يمكنهن المجيء جاهزات وقد فُكّرُن في كل هذه التفاصيل.

إدارة الجلسة

الجزء الأول - المقدمة

١. خلال هذا التمرين، ستشارك كل مشاركة هوية جديدة بالكامل لها. يفترض أن تحضر المشاركات هذه الهوية مسبقاً، ويجب ألا تستند على شخص فعلي وأن تكون من نسج الخيال.
٢. إشرحن لهن أنه عند بناء هذه الهوية الجديدة، يمكنهن التمتع بالحرية الكاملة، أي يمكنهن أن يكن نساءً أو رجالاً، أو حتى مكاناً، أو أي شيء يخطر في بالهن. الفكرة الأساسية من هذا التمرين هي أن يُختلقن هوية جديدة لهن بكل ما للكلمة من معنى - وهذا يعني إختلاق اسم جديد لهن ومكان سكن جديد ومكان عمل جديد وعائلة جديدة وحتى هويات جديدة.

الجزء الثاني - حان وقت اللعب!

٣. من بعد التعريف بالتمرين، إبدأن المرحلة التالية بالتعريف بشكل موجز بمفهوم المحافظة على سرية الهوية. إسألن المشاركات لماذا يعتبرن مسألة المحافظة على سرية الهوية مسألةً لا بد منها في عملهن وفي حياتهن الشخصية وعلاقتهن على حدٍ سواء.

من بعد أن قمتن بالتعريف بمفهوم المحافظة على سرية الهوية وبتقديم لمحة عامة عنه، يجب أن تسيّر التمرين نفسه من خلال إتباع الخطوات التالية:

٥٤. يجب أن تجهز كل مشاركة قبل المجيء إلى التمرين مفهوماً واضحاً لهويتها الجديدة - على أن يشمل ذلك اسمها ومكان ولادتها ومكان عملها وعائلتها وحتى هواياتها،... إلخ. قبل البدء بالتمرين، أطلبين من كل مشاركة الإفصاح عن أسم هويتها الجديد معكن وليس للمجموعة لكي تتمكني كدربات من المتابعة (هذا عنصر مهم من التمرين).

٥٥. يجب أن يكتب الجميع على قصاصة ورق الاسم الذي اختارته لهويتها الجديدة. إجمعن كل القصاصات وضعنها كلها في وعاء.

٥٦. تجولن في الغرفة وإسمحن لكل مشاركة بسحب اسم واحد من الوعاء - في حال سحبت المشاركات هوياتهن الخاصة، عليهن إعادة القصاصة وسحب أخرى. الاسم المسحوب من قبل كل مشاركة سيصبح اسم صديقتها السرية.

٥٧. والآن يجب أن تقوم المشاركات بكتابة رسالة لصديقاتهن الجديديات يصفن فيها (من منظور الهوية التي أنشأتهن لنفسها) من هنّ ومن أين هنّ وما هي هواياتهن أو ما هو عملهن، إلخ.

٥٨. بعد أن ينتهين من كتابة هذه الرسائل، سيضعنها داخل مغلف. يجب أن يكتبن اسم صديقتهن السرية على المغلف من الخارج. إحرصن ألا ترى المشاركات ما تكتبته الأخريات لتفادي إنكشاف أي تفاصيل.

٥٩. تجولن في الغرفة وإجمعن كل المغلفات. إستناداً إلى لاأحتكن التي تحدد الهوية الجديدة المرتبطة بكل مشاركة، وزعن الرسائل على المتلقيات المقصودات (هذه المرة أيضاً، إحرصن ألا ترى المشاركات الأسماء المكتوبة على المغلفات، بإستثناء تلك المخصصة لهن).

٥١٠. واحدة تلو الأخرى، أطلبين من كل مشاركة التقدّم إلى مقدمة الغرفة والجلوس على كرسي ووضع عصبة على أعينهن. سيقمن حينها بمشاركة تفاصيل الرسالة التي تلقينها،

بما في ذلك اسم صديقتهن السرية.

١١. أثناء وصف كل مشاركة لمحتوى رسالتها، يجب على صديقتها السرية الجلوس في كرسي آخر وضع إلى جانب المتطوعة.

١٢. بعد أن تنتهي كل مشاركة من وصف رسالتها، أطلبن منها محاولة تخمين من من المشاركات الأخريات هي صديقتها السرية. وبعد أن تحاول ذلك، أزلن العصابة عن عينها وأطلبن منها أن تنظر إلى الشخص الجالس إلى جانبها لمعرفة ما إذا كان تخمينها صحيحاً.

١٣. تابعن التمرين، عبر تكرار العملية المذكورة أعلاه إلى أن تتكشف كل الهويات.

الجزء الثالث - الحلقة الختامية

١٤. بعد الإنهاء من التمرين، إسألن المجموعة - هل كانت تخميناتهن صحيحة بشأن هوية صديقاتهن السريات؟ كيف تمكن من معرفتها، أو ما هي العملية الذهنية التي إستعن بها في تخميناتهن؟ ما كان مدى صعوبة ذلك عليهن؟

١٥. إختتمن التمرين بالتفكير في أهمية المحافظة على سرية الهوية والتمكن من حماية هوية شخص ما بالكامل، ومن ناحية أخرى مدى سهولة إخفاء الآخرين لهوياتهم الحقيقية أحياناً (ولياتهم أيضاً).

باب ٢٧

المحافظة على سرية الهوية

- الأهداف: في هذه الجلسة، ستقدم للشاركات مفهوم المحافظة على سرية الهوية على الإنترنت، بالإضافة إلى الأدوات والممارسات المرتبطة بهذا المفهوم، والتي قد تساعد في حماية الهوية وعدم الكشف عنها.
- الطول: 40 دقيقة
- الشكل: جلسة
- مستوي المهارة: متوسط
- المعرفة المطلوبة:
- معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
- جلسات/تمارين ذات صلة:
- التصفح الآمن^١
- ماذا يمكن لبياناتك الوصفية (Metadata) أن تفصح عنك؟^٢
- الصديقة السرية^٣

<https://vrr.im/aee7>^١

<https://vrr.im/1598>^٢

<https://vrr.im/873b>^٣

- المزيد من الهويات الإلكترونية!٤
- المواد اللازمة:
- شراخ (فيها النقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض

إدارة الجلسة

الجزء الأول - تعريف بالمحافظة على سرية الهوية على الإنترنت

١. إبدأن الجلسة بسؤال المشاركات عن ما يعنيه لهن مفهوم المحافظة على سرية الهوية؟ بعد أن تستمعن لبعض الإجابات، قدمن للمجموعة مفهوم المحافظة على سرية الهوية بشكلٍ مفصل أكثر شارحاتٍ ما يلي:

- إشرحن فوائد معرفة المزيد عن ماهية المحافظة على سرية الهوية وأهميتها في العمل في مجال حقوق الإنسان؛
- قدمن أمثلة للمشاركات عن آثار البيانات على الإنترنت التي قد تساعد في تحديد هوية شخص ما - قد تتضمن بيانات مثل اسم المستخدم، منشورات على مواقع التواصل الاجتماعي، الأجهزة المستخدمة والمواقع الجغرافية وأنواع أخرى من البيانات الوصفية؛
- تحدثن عن كيفية تطبيق مفهوم المحافظة على سرية الهوية على مستويات أو طبقات مختلفة، شارحات للمشاركات أنهن قادرات على المحافظة على سرية الهوية في نشاط معين أو اتصال معين أو صفحة بأكملها أو جلسة استخدام

<https://vrr.im/e9f7٤>

الجزء الثاني - البيانات المحددة للهوية والمحافظة على سرية الهوية

٢. في الجزء السابق من هذه الجلسة، ناقشتن الأنواع المختلفة من آثار البيانات على الإنترنت التي قد تساهم في تحديد هوية شخصٍ ما. والآن، ستسلطن الضوء على إحداها لأنها مهمة لعنصر معين على الإنترنت - عنوان بروتوكول الإنترنت:

• ما هو عنوان بروتوكول الإنترنت؟ إشرحن للمشاركات ماهية هذا العنوان والغرض منه وكيف يمكن أن يكون هذا العنوان معلومة مهمة جداً في بيئة الإنترنت (لا سيما عند محاولة تصفّح المساحات الإقتراضية من دون الكشف عن الهوية)؛

• بغية تبيان بعض تداعيات عناوين بروتوكول الإنترنت على المحافظة على سرية الهوية للمجموعة، أطلبن منهن استخدام موقع إلكتروني من قبيل <https://whatismyipaddress.com/> للتعرف على عنوان بروتوكول الإنترنت الخاص بهن كأفراد، وكيف أنها تكشف عن أنواع أخرى من المعلومات التي قد تكون حساسة أو قادرة على تحديد هوية شخصٍ ما.

٣. والآن، ستقدمن الأدوات التالية للمشاركات وستشرحن أهمية كل واحدة منها في المحافظة على سرية الهوية على الإنترنت - أشرن إلى أن كل واحدة منها تقدّم إمكانية المحافظة على سرية الهوية بطرقٍ مختلفة أو بمستويات مختلفة:

- متصفح تور
 - الشبكات الإقتراضية الخاصة (Virtual Private Networks VPN's)
 - نظام "نايلز" (The Amnesiac Incognito Live System)
 - برنامج "إيتش تي بي إس إفري وير" HTTPS Everywhere
- لا بد من شرح بعض الممارسات الرئيسية التي يجب أخذها بعين الإعتبار عند استخدام الأدوات المذكورة أعلاه بشكلٍ آمن وتخصيص الوقت الكافي لقيام المشاركات بتثبيتها والتدرب على استخدامها.

الجزء الثالث - بعض التطبيق العملي

٤. أطلبين من المشاركات التحقق من جديد من عناوين بروتوكول الإنترنت الخاصة بهن على موقع <https://whatismyipaddress.com/> - يجب أن يقمن بذلك مرة أثناء استخدام شبكة افتراضية خاصة ومرة ثانية أثناء استخدام متصفح تور. هل سيلاحظن فرقاً في عناوين بروتوكول الإنترنت أو في أمرٍ آخر؟
٥. هذه فرصة جيدة لتناول نقطة أخرى تترك المستخدمين/ات: التصفح المتخفي (Incognito Mode). ففي معظم الأحيان، يظنّ المستخدمون أنهم يتصفحون الإنترنت من دون الكشف عن هويتهم أثناء استخدام التصفح المتخفي فقط (أو ما يعادله، بحسب المتصفح المستخدم). ما الذي تلاحظينه بشأن عنوان بروتوكول الإنترنت الخاص بهن الآن؟

باب ٢٨

المزيد من الهويات الإلكترونية!

- الأهداف: الإستماع إلى أمثلة عن حالات وأدوات وممارسات سليمة خاصة بإنشاء الهويات الإلكترونية.
- الطول: 120 دقيقة
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
- المحافظة على سرية الهوية (المحافظة على سرية الهوية)
- ماذا يمكن لبياناتك الوصفية أن تفصح عنك؟ (المناصرة الآمنة على الإنترنت)
- التصفح الآمن (أسس الأمن الرقمي، الجولة الأولى)
- جلسات/تمارين ذات صلة:
- التصفح الآمن^١
- ماذا يمكن لبياناتك الوصفية (Metadata) أن تفصح عنك؟^٢

^١<https://vrr.im/ae7>

^٢<https://vrr.im/1598>

- الصديقة السرية^٣
- المحافظة على سرية الهوية^٤
- المواد اللازمة:
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
 - لوح ورقي (ورقة أو ورقتين لكل مشاركة)
 - أقلام خطاطة أو أقلام

تستند هذه الجلسة إلى الدليل المعنون "إنشاء الهويات الإلكترونية وإدارتها" من دليل جماعة "تاكايكل كنولوجي كوليكثيف" المعنون "الهدوء وفن جعل التكنولوجيا تعمل لصالحك"

إدارة الجلسة

الجزء الأول - الهويات الإلكترونية المتصلة

١. إبدآن التمرين بالطلب من المشاركات وضع لائحة بأي من الهويات الإلكترونية التي يمتلكنها، يمكن أيضاً سؤالهن بكل بساطة عما إذا كانت إحدهن تستخدم أكثر من هوية إلكترونية واحدة. وأي مشاركة تشير إلى استخدامها لأكثر من هوية إلكترونية واحدة، عليكن سؤالها إذا كان بإمكانها مشاركة أسباب ذلك مع بقية المجموعة والغرض من استخدامها لها.
٢. إستناداً إلى أي أمثلة شاركتها المجموعة، إشرحن لهن أن استخدام هويات إلكترونية متعددة ممارسة شائعة بين المدافعات عن حقوق الإنسان - وقدمن بعض الأمثلة عن السيناريوهات:
 - المدافعات اللواتي يستخدمن فايسبوك لإدارة الحملات على الإنترنت، إلا أنهن لا يرغبن في استخدام صفحاتهن الشخصية أو هويتين لإدارة صفحة الحملة؛ المدافعات اللواتي يجرين عمليات بحث حساسة على الإنترنت، ويرغبن في ترك أقل قدر ممكن من الآثار

^٣ <https://vrr.im/873b>

^٤ <https://vrr.im/70ff>

الرقمية التي تسمح بتعقب أثرهن؛

الدفاعات اللواتي كنّ يوثق حالات إنتهاك الحكومات لحقوق الإنسان، واللواتي يخططن لفضح هذه المعلومات عبر نشر تقرير مهم أو بيان عام.

٣. والآن أطلب من المشاركات تشكيل مجموعات من شخصين وتحديد الظروف الأخرى التي يفضل أن ينشئ فيها هوية جديدة غير مرتبطة بهويتين الشخصية. أطلب منهن التفكير في مدى مزجهن لهوياتهن الشخصية وعملهن ككاشطات:

هل يدجن حساباتهن مع بعضها البعض؟ هل يدجن هوياتهن بعضها ببعض؟

ما مدى إرتباط حياتهن الرقمية الشخصية بحياتهن ككاشطات؟

ما هي الأنشطة التي قد تعرّضهن للخطر في حال إستخدامن فيها هوياتهن الحقيقية؟ أمثلة عن ذلك تشمل:

طلب معلومات من وكالات حكومية؛

زيارة المواقع الإلكترونية الحكومية لجمع معلومات سينشرها على الإنترنت؛ إدارة حسابات مواقع التواصل الإجتماعي الخاصة بمنظمتن أو جماعتن)؛

الجزء الثاني - فصل الهويات الإلكترونية عن بعضها البعض وإدارتها

٤. إستناداً إلى عملية التفكير التي قامت بها المجموعة في المرحلة السابقة، إشرحن للمجموعة ثلاث خيارات خاصة بإدارة هوياتهن الإلكترونية: إنشاء هوية إلكترونية مزيفة وجديدة بالكامل؛ فصل الصفحات الشخصية عن الصفحات المهنية؛ ترك هوياتهن كما هي الآن (عدم تغيير أي شيء)؛

٥. قدمن لكل خيار من الخيارات الواردة أعلاه، مثال حيّ واحد على الأقلّ وإشرحن للمشاركات تداعيات كل خيار منها، على سبيل المثال:

إنشاء هوية إلكترونية مزيفة وجديدة بالكامل: يتطلب ذلك على الأرجح أن تكون هذه الهوية منفصلة بالكامل عن أي عنصر قد يربطها بهويتكن الحقيقية لكي تكون هذه

الخطوة فعّالة. وهذا يعني إنشاء عناوين بريد إلكتروني جديدة وصفحات جديدة على مواقع التواصل الاجتماعي، وضرورة تسجيل الدخول والخروج من هذه الحسابات بشكلٍ مستمر لضمان عدم تلاقي الهويتين، ويفترض ذلك أيضاً البدء بعدد صفر متابعين/ات على صفحات التواصل الاجتماعي؛

فصل الصفحات الشخصية عن الصفحات المهنية: يتطلب ذلك فقط من المستخدمين تغيير إعدادات الخصوصية الخاصة بحساباتهم، إما من أجل الحد من المعلومات المتوفرة للعموم وإما لإدارة مستوى المعلومات المتاحة لأصدقاء ومتابعين وجهات اتصال معينين؛ ولكن في حالات أخرى، فصل هاتين الهويتين قد يفرض الحاجة إلى المحافظة على مجموعتين منفصلتين من الصفحات والحسابات لكل منهما (أي سيتوجب إنشاء مجموعة جديدة إما لهويتين الشخصية أو المهنية) ترك هوياتهن كما هي الآن: يتطلب ذلك على الأرجح من المستخدمين تغيير إعدادات الخصوصية الخاصة بحساباتهم، إما من أجل الحد من كمية المعلومات المتوفرة للعموم وإما لإدارة مستوى المعلومات المتاحة لأصدقاء ومتابعين/ات وجهات اتصال معينة.

٥. والآن، أطلب من المشاركات مناقشة ضمن المجموعات ذاتها في المرحلة الثالثة، بعض إيجابيات وسلبيات كل خيار من هذه الخيارات، إما بالمعنى العام أو خصيصاً بالنسبة لمن وليئة عملهن. ومن ضمن المشاكل التي قد تنشأ خلال هذه النقاشات، هي المشاكل المرتبطة بالجانب العملي والمصدقية - كنّ جاهزات للتحدث عن هذه المسائل تحديداً حين تقمن المشاركات بمشاركة بعض خلاصات نقاشهن مع المجموعة.

الجزء الثالث - الممارسة التطبيقية والتوصيات

٥. إشرحن للمشاركات أنه يمكنهن الإختيار أي من الخيارات الثلاثة المقدمة للجزء التالي من التمرين (ستستعين المراحل الواردة أدناه بخيار إنشاء هوية جديدة بالكامل).
٦. إعطين كل مشارك ورقة أوورقتين من اللوح الورقي وبعض الأقلام الخطاطة، وأطلبن منهن البدء بوضع مسودة بخصائص هويتهم الجديدة - تتضمن بعض الإعتبارات المحددة التي يتوجب عليهن التفكير فيها ما يلي:

ما هو الاسم الذي قد يستخدمه؟ (إنتبهن إلى أن بعض منصات التواصل الاجتماعي، لا سيما فايسبوك وغوغل، قادرة على تحديد وتدمير الحسابات صاحبة الأسماء المزيّفة، لذا يجب أن تفكرن المشاركات بطريقة إبداعية)؛ ما هي هوياتهن وإهتماماتهن المحتملة؟ أين ولدن وأي عشن؟ ما هي الصور أو الرسوم الذي قد يستخدمنها؟ هل من الممكن استخدام هذه التفاصيل لإقتفاء أثر هوياتهن الحقيقية؟

٧. بعد أن تنتهي المشاركات من وضع مسودة بتفاصيل صفحاتهن وهوياتهن الجديدة، شاركن معهن بعض توصيات الأمن الرقمي التي من شأنها أن تساعدن في تفادي إنكشاف هوياتهن الحقيقية. إذكرن أن بعض تلك التوصيات سبق أو وردت في جلسات سابقة (المحافظة على سرية الهوية، ماذا يمكن لبياناتكن الوصفية أن تفصح عنكن؟، التصفح الآمن)، وأنها ستكون بمثابة مراجعة لها:

يساعد استخدام هاتف يستخدم لمرة واحدة للحسابات والصفحات الجديدة - يستوجب غوغل تزويده برقم هاتف لإرسال رموز التحقق خلال عملية الإعداد للحساب، كما تستوجب عملية إعداد خاصية التحقق بخطوتين إدخال رقم الهاتف على عدد من المنصات (يوصى باستخدام خاصية التحقق بخطوتين لحماية هذه الحسابات) - يجب على المستخدمين إدخال رقم ليس رقمهم الأساسي في هذه الحالات. استخدام آلات أو أجهزة مختلفة لكل هوية - كما ورد أعلاه، هذا يساعد في فصل هوياتهن المختلفة وفصل الأنشطة، مما يساعد المستخدمين على تفادي الأخطاء التي تعرض هويتهم الجديدة لخطر الإنكشاف. تستطيع المشاركات القيام بذلك عبر استخدام أجهزة حاسوب أو هواتف منفصلة، وإعداد آلة إقتراضية منفصلة على حاسوبهن، أو عبر استخدام نظام تشغيلي بديل كنظام تايلز (راجعن جلسة لنعد إلى خانة الصفراء! للزيد من المعلومات)؛ عند إعداد صفحة جديدة، يفضل أن تفكرن المشاركات عند تسجيل الدخول في الحسابات المرتبطة في استخدام متصفح منفصل مختلف عن الذي يستخدمه بشكل رئيسي للوصول إلى صفحاتهن الحالية - سيساعدن ذلك في تفادي ربطها بالحسابات، أو تسجيل دخولهن إلى إحداها في المتصفح الآخر عن طريق الخطأ ومشاركة المعلومات التي قد تفضح الفصل بين هوياتهن؛ راجعن عادات

التصفح الآمن العامة مع المشاركات - يمكنك استخدام هذه المراجعة كأساس للتحدث عن مفهوم "بصمات" المتصفح، وأثر ذلك المحتمل على الفصل بين هوياتهن <https://panopticlick.eff.org/static/browser-uniqueness.pdf>؛ إضافة إلى ذلك، يمكنك مراجعة كيفية تعميم عناوين بروتوكول الإنترنت التي قد تفضح تفاصيل موقعك الجغرافي؛

يجب ألا تتبع المشاركات أي أصدقاء أو أعضاء من عوائلهن أو منظماتهن بواسطة هوياتهن الجديدة - فقد يسمح ذلك بسرعة لأي شخص يبحث بدقة علي إكتشاف الرابط بين الهوية تلك والهوية الحقيقية؛

ذكرن المشاركات أن يتبنهن للبيانات الوصفية وكيف يمكن لها أن تكشف عن معلومات خاصة بهن. راجعن كيفية نشوء البيانات الوصفية وكيفية حذفها من ملفاتهن قبل نشر الصور أو الفيديوهات أو قبل إرسال الملفات من حسابات هوياتهن الجديدة.

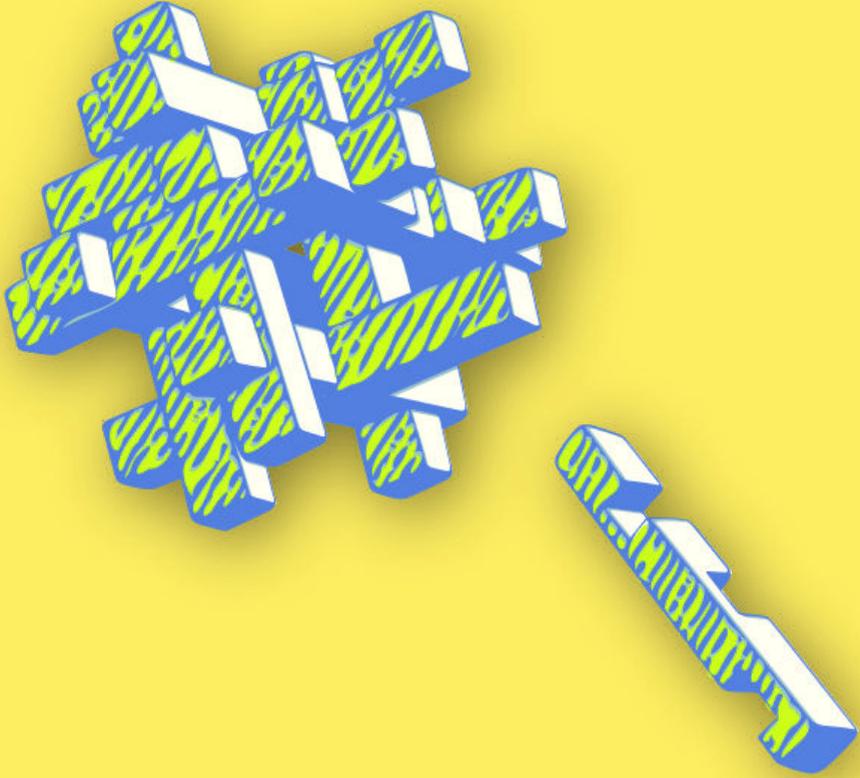
٨. والآن، يمكن للمشاركات البدء بإنشاء صفحات وحسابات هوياتهن الإلكترونية الجديدة!

المراجع

https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual#Creating_and_managing_identities_online



النساء فى فضاء الإنترنت



التشفير

باب ٢٩

تعريف بمسألة التشفير

- الأهداف: هذه الجلسة التعريفية ستشرح للمشاركات مفهوم التشفير، بالإضافة إلى لمحة عامة موجزة عن الأنواع المختلفة للتشفير المتوفر للمستخدمين/ات.
- الطول: 50 دقيقة
- الشكل: جلسة
- مستوى المهارة: متوسط
- المعرفة المطلوبة:
- معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
- جلسات/تمارين ذات صلة:
- الخصوصية^١
- الحملات الآمنة على الإنترنت^٢
- الاتصالات المشفرة^٣
- التخزين والتشفير^٤
- المواد اللازمة:

<https://vrr.im/819e1>

<https://vrr.im/8e6b2>

<https://vrr.im/27253>

<https://vrr.im/0ccc4>

- شراخ (فيها النقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
- أمثلة عن تقنيات التشفير (مطبوعة)

إدارة الجلسة

الجزء الأول - هل سبق لكن أن إستخدمتن التشفير؟

- ٠١ إشرح لمن أن هذه الجلسة جلسة ستعرفهن على التشفير كمفهوم، لذا لن نتمعن كثيراً في شرح أي من أدوات التشفير التي يحتمل أن تكون المشاركات قد سمعت عنها في السابق (لاسيما جي بي جي/GPG/بي جي بي PGP)
- ٠٢ قسمن المشاركات إلى مجموعات من شخصين ومن ثمَّ إبدأن الجلسة عبر عرض بعض الأمثلة عن تقنيات التشفير. إلكن بعض الأمثلة التي يمكنن تحضيرها مسبقاً لمشاركتها مع المجموعة:

شيفرة كلمة "بلوريننس" BLUEPRINTS

كل حرف من كلمة "BLUEPRINTS" يربط برقم.

S T N I R P E U L B
9 8 7 6 5 4 3 2 1 0

هذا مثال محدد إستعين بكلمة محددة، ولكن يمكن تطبيقه بشكلٍ عام على أي تسلسل أرقام وأحرف - على سبيل المثال، في حال إستخدمتن النظام المذكور أعلاه نفسه، تسلسل الأرقام 82579 يعني كلمة TURNS حين "يفك التشفير".

يمكنن أيضاً قلب ترتيب الأرقام بحيث يصبح التسلسل الآن كما يلي

S T N I R P E U L B
0 1 2 3 4 5 6 7 8 9

في هذه الحالة، تسلسل الأرقام 82579 سيدل على تسلسل الأحرف التالي LN PUB (وهذه ليست كلمة) حين "يُفك التشفير"؛ ولكن مثلا يمكننا الآن "فكّ تشفير" التسلسل 43206 للتوصل إلى كلمة RINSE.

الرسائل القصيرة القديمة الطراز

إستخدمن صورة لوح مفاتيح هاتف من الطراز القديم (كما يرد أدناه) لعرض نوع آخر من أنواع "التشفير" التي قد تعرفها المشاركات



الرسائل النصية القديمة الطراز

إسألن المشاركات عن كيفية إستخدامهن اللوح المفاتيح هذا لكّابة كلمات متنوعة - أحد الأمثلة على ذلك التي يمكننا الاستعانة بها قد تكون الطلب من كل مشاركة شرح كيفية استخدامها للوح المفاتيح لكّابة اسمها. على سبيل المثال، لكّابة اسم إحدى المشاركات: لينا

Lina، نكتب تسلسل الأرقام التالي 66 2 444 555.

٣. عد أن تنتهين من عرض الأمثلة المذكورة أعلاه، سألن المشاركات إذا ما سبق لهن أن إستخدمن أي نوع من أنواع التشفير - إما نوع شبيه بالأمثلة المذكورة أعلاه وإما أي أمثلة أخرى قد تخطر في بالهن (على سبيل المثال طريقة تشفير شائعة إستخدما الكثير من الناس في حياتهم اليومية هي "إيتش تي بي إس" (HTTPS)).

٤. إختتمن هذا الجزء من الجلسة عبر طرح سؤال آخر: ما هي العناصر الشائعة التي يمكنهن تحديدها من أمثلة التشفير الأخرى هذه؟

الجزء الثاني - شرح ماهية التشفير

٥. إستناداً إلى العناصر الشائعة من عناصر التشفير التي حددنها المشاركات في الجزء الأول، عليكن الآن التوسع وشرح المزيد من الأسس والممارسات للمجموعة:

طرق التشفير: خصصن الوقت الكافي لشرح كيفية عمل التشفير إستناداً إلى الأمثلة من الجزء الأول بالإضافة إلى عرض بعض الأمثلة عن صور ملتقطة عن شاشات لشكل البريد الإلكتروني المشفر بواسطة "جي بي جي". شددن على بعض حالات تنفيذ التشفير الشائعة - وبشكل خاص، خصصن الوقت الكافي لمراجعة تقنية "إيتش تي بي إس" والتشفير الكامل وتقنية جي بي جي/بي جي بي.

المفاتيح والمفاتيح الثنائية: إشرحن كيفية عمل مفاتيح التشفير الثنائية والعلاقة الخوارزمية بين المفاتيح العام والخاص. إستعدن الأمثلة عن التطبيقات المذكورة آنفاً (إيتش تي بي إس، التشفير الكامل و جي بي جي/بي جي بي) وإشرحن أنه لكل واحدة من هذه التطبيقات مفاتيح خاصة مخزنة و/أو ظاهرة للمستخدم.

ممارسات التشفير: ألتين الضوء على أهم الممارسات الفضلى المرتبطة بالتطبيقات الشائعة للتشفير، كتقنية التحقق من البصمة والتوقيع الرقمي على المفاتيح لعرض ذلك، أطلبن من المشاركات تحديد المكان في تطبيق سيجنال الذي يمكن للمستخدم فيه التحقق من

بصمة مستخدم آخر؛ وعلى نحو مماثل، في حال كانت المشاركات تمتلكن مفاتيح جي بي جي/بي جي بي، يمكن مناقشة فوائد ومساوئ توقيع وتوزيع المفاتيح المتاحة للعموم. والوقت مناسب أيضاً لمناقشة المراسلات المشفرة تشفيراً كاملاً في تطبيقات المحادثة كتطبيق سيجنال وواتساب وتليغرام- ذكّن المشاركات أن التشفير الكامل ليس دائماً مفعلاً بشكلٍ تلقائي على بعض هذه الخدمات.

النسخ الإحتياطية المشفرة: إستناداً إلى مثال التشفير بواسطة جي بي جي/بي جي بي المذكور أعلاه، إسألن المشاركات إذا كنّ يعتقدن أن القيام بنسخة إحتياطية لمفتاح جي بي جي الخاص بهن فكرة جيّدة، وإن كان كذلك، ما هي الخطوات التي يمكنهن إتباعها؟

المراجع

• <https://www.gnupg.org/gph/en/manual/book1.html>

باب ٣٠

الإتصالات المشفرة

- الأهداف: تستند هذه الجلسة إلى محتويات التدريب السابقة المرتبطة بالتشفير، ناقلهً إلى المشاركات أهمية تشفير الإتصالات وفائدتها وتقديم الأدوات المهمة لذلك
- الطول: 50 دقيقة
- الشكل: جلسة
- مستوي المهارة: متوسط
- المعرفة المطلوبة:
- معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
- تعريف بمسألة التشفير (التشفير)
- جلسات/تمارين ذات صلة:
- الخصوصية^١
- الحملات الآمنة على الإنترنت^٢
- تعريف بمسألة التشفير^٣
- المواد اللازمة:

<https://vrr.im/819e¹>

<https://vrr.im/8e6b²>

<https://vrr.im/f5d4³>

- شراخ (فيها النقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض

إدارة الجلسة

- ٠١ إبدآن الجلسة بمشاركة بعض الأمثلة المهمة عن حالات يكون فيها تشفير الإتصالات مفيداً، وخصصن الوقت اللازم لشرح كيفية عمل التشفير. أعرضن بواسطة بعض أمثلة عن صور لشاشات بريدًا إلكترونيًا مشفّرًا بواسطة جي بي جي لإظهار كيف تبدو الرسائل ورسائل البريد الإلكتروني حين تكون مشفّرة وسلطن الضوء على التطبيقات الشائعة للتشفير - لا سيما تقنية إيتش بي بي إس والتشفير الكامل وتشفير جي بي جي/بي جي بي.
- ٠٢ إحصرن النقاش الآن بالتحديد على الأدوات التي تسمح بتشفير الإتصالات: تطبيق سيجنال للإتصالات والرسائل، وتطبيق "ميت.جيتسي" <https://meet.jitsi> لإتصالات الفيديو وتوتانوتا أو جي بي جي و"ثندر بيرد" Thunderbird لرسائل البريد الإلكتروني. كلها أمثلة مفيدة لأبد من مشاركتها.
- ٠٣ إشرحن الفوائد الأمنية لهذه الأدوات للمجموعة، وبشكلٍ أساسي كيف تمكّن المستخدمين من الحد من إمكانية وصول الآخرين إلى اتصالاتهم؛ ومن ثمّ ناقشن الحالات التي قد يتعرض فيها أمن بيانات المستخدم لخطر الإنكشاف، حتى مع إستخدام الإتصالات المشفّرة. إسألن المشاركات - كيف يمكن أن نتعرض لمحتويات بريد إلكتروني مشفّر بواسطة جي بي جي لخطر الإنكشاف بسبب تسجيل المفاتيح (keylogging) أو برمجيات الخبيثة لإلتقاط صور الشاشة (screen-capturing) (malware)؟ ما الذي قد يحدث في حال تمكّن أحد الخصوم من الوصول إلى مفتاح جي بي جي خاص بمستخدم/ة - كيف يمكن للخصوم استخدامه للوصول إلى بياناتهم؟
- ٠٤ في حال كان الوقت المتوفر يسمح بذلك، لأبد من توفير فرصة الممارسة التطبيقية للمشاركات على الأقلّ على واحدة من الأدوات المذكورة آنفًا في المرحلة الثانية. ومع

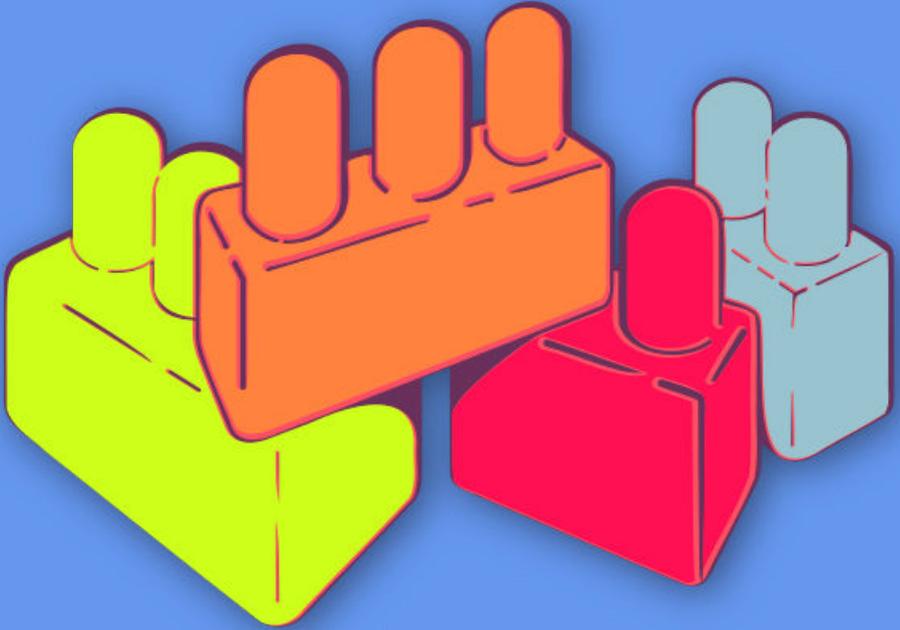
أن الوقت قد لا يكون متاحاً لتعليم المجموعة كيفية إعداد تقنية جي بي جي/بي جي بي للبريد الإلكتروني، يمكنكن اختيار عرض إتصال فيديو محمي بتقنية إيتش تي تي بي إس عبر تطبيق “ميت.جيتسي”، أو أطلبين من المشاركات تثبيت تطبيق سيجنال على هواتفهن للتدرّب على إرسال الرسائل المشفّرة إلى بعضهن البعض، أو تبادل الاتصالات الهاتفية المشفّرة.

المراجع

- <https://ssd.eff.org/en/module/how-use-signal-android>
- <https://ssd.eff.org/en/module/how-use-signal-ios>



النساء فى فضاء الإنترنت



أسس الأمن الرقمي | الجولة
الثانية

باب ٣١

التخزين والتشفير

- الأهداف: في هذه الجلسة، ستشددن على أهمية القيام بنسخ احتياطية للبيانات بشكلٍ دوري، وستناقشن كيفية منع التلاعب أو الوصول غير المسموح به لمعلومات المشاركين.
- الطول: 90 دقيقة
- المعرفة المطلوبة:
 - معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
 - تعريف بمسألة التشفير (التشفير)
 - كيفية حماية حاسوبك (أسس الأمن الرقمي، الجولة الأولى)
- جلسات/تمارين ذات صلة:
 - كيفية حماية حاسوبك^١
 - الخصوصية^٢
 - الحملات الآمنة على الإنترنت^٣

<https://vrr.im/ac95>^١

<https://vrr.im/819e>^٢

<https://vrr.im/8e6b>^٣

- تعريف بمسألة التشفير^٤
- المواد اللازمة:
 - شرائح (فيها النقاط المفتاحية الواردة أدناه)
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
 - نسخ مطبوعة عن نموذج النسخ الاحتياطي (أدناه)
 - مفاتيح يو إس بي أو نوع آخر من وسائط التخزين (لكل مشاركة)
- التوصيات: المشاركات في هذه الجلسة ستستخدم إما برمجية "فيراكريت" veracrypt أو "ماك كبير" mackeeper (بحسب النظام التشغيلي الخاص بهن) للتدريب على تشفير النسخ الاحتياطية للبيانات ووسائط التخزين - لتوفير الوقت، فكون في الطلب من المشاركات تنزيل أي من هذه البرمجيات مسبقاً بشكل عام، ولا سيما للبتدئات، لا ينصح بإجراء المشاركات لعملية تشفير شاملة للقرص الصلب على حاسوبهن الآن - عوضاً عن ذلك، يتوجب عليهن اختبار برمجيتي "فيراكريت" أو "ماك كبير" على وسيط تخزين خارجي (من قبيل مفتاح يو إس بي) باستخدام ملفات مزيفة حضرها خصيصاً لهذه الجلسة. إذ حتماً لا ترغبن في التعرض لخطر فقدان إحدى المشاركات لإمكانية الوصول إلى أي بيانات خلال التدريب عن طريق الخطأ!

إدارة الجلسة

الجزء الأول - نسخ البيانات الاحتياطية والتخطيط

١. إسألن المشاركات - كم مرّة في السنة يقمن بنسخ احتياطية لملفاتهن؟ شاركن أمثلة عن الممارسات الفضلى في مجال إنشاء نسخ احتياطية للبيانات، من قبيل الإحتفاظ بالنسخة الاحتياطية في مكان آمن منفصل عن حاسوبهن، وإنشاء نسخ احتياطية لمعلوماتهن بشكلٍ دوري ومتكرر، بحسب للمعلومات التي يُنشأ لها نسخ احتياطية، والتفكير أيضاً في تشفير القرص الصلب أو وسيط التخزين حيث سيقمن بتخزين البيانات.

<https://vrr.im/f5d4>^٤

٢. شاركن مع المشاركات نموذج تنظيم النسخ الاحتياطي الوارد أدناه، وأطلبن منهن البدء بملمته بشكلٍ فرديّ. إشرحن للمجموعة أن الإستعانة به طريقة مفيدة لوضع سياسة شخصية خاصة بإنشاء نسخ احتياطية للبيانات - يمكنهن الإستعانة بهذا النموذج بعد التدريب، كمورد مفيد في متابعة مكان تخزين البيانات وعدد المرات التي يجب فيها إنشاء نسخ احتياطية للبيانات.

نموذج تنظيم النسخ الاحتياطي

- نوع المعلومات
- الأهمية/القيمة
- ما وتيرة إنتاجها أو تغييرها؟
- كم عدد المرات التي يجب فيها إنشاء نسخ احتياطية لها؟

الجزء الثاني - تشفير التخزين والنسخ الاحتياطية

٣. بعد أن تنتهي المشاركات من ملء نموذج تنظيم النسخ الاحتياطية، أطلبن منهن مراجعة أنواع المعلومات (إلى جانب أهميتها وقيمتها) الموجودة على لائحتن مجدداً - أثناء قيامهن بذلك، أطلبن منهن التفكير في ما قد يحدث في حال وصلت هذه المعلومات إلى أحد خصومهن، أو في حال فقدان هذه المعلومات كلها. ما أثر ذلك عليهن شخصياً وعلى منظمتهن؟

٤. والآن، قدمن مفهوم التشفير للمجموعة - إشرحن لهن أنهن على الأرجح يجدن التشفير مرات عدة في حياتهن اليومية، فهو مستخدم بطرق مختلفة في أدوات ومنصات مختلفة. على سبيل المثال، يمكنكن الإشارة إلى أن "إيتش تي تي بي إس" هو نفسه شكل من أشكال تشفير البيانات "المتنقلة" (البيانات المتنقلة من النقطة "أ" إلى النقطة "ب") في حين أنهن في هذه الجلسة، ستناقشن تشفير البيانات "الثابتة" (أي البيانات المخزنة في مكان واحد).

٥. ذكرن المشاركات بأنه طلب منهن تنزيل إما برمجية "فيراكربت" أو برمجية "ماك كبير" على حواسيبهن. لمنحن المشاركات الوقت اللازم لتثبيت هذه الأدوات واختبارها،

بواسطة وسيط تخزين خارجي (من قبيل مفاتيح يو إس بي) وملفات مزيفة حضرناها خصيصاً لهذه الجلسة. لا ينصح بإجراء عملية تشفير شاملة لقرص الحاسوب الصلب الآن، لا سيما للمشاركات المبتدئات - إذ حتماً لا ترغبين في التعرّض لخطر فقدان إحدى المشاركات لإمكانية الوصول إلى أي بيانات خلال التدريب عن طريق الخطأ!

المراجع

- <https://securityinabox.org/en/guide/veracrypt/windows/>
- <https://securityinabox.org/en/guide/veracrypt/mac>
- <https://securityinabox.org/en/guide/veracrypt/linux>

باب ٣٢

لنعد إلى خانة الصفر (إعادة الضبط)!

- الأهداف: تعزز هذه الجلسة فكرة أنه "ليس للأدوات والتكنولوجيا سطوة سحرية خارقة علينا!" ستقدن المشاركات هنا في عملية سترفع من مستوى قدراتهن هي عملية "البدء من خانة الصفر" عبر إعادة ضبط أجهزتهن من أجل البدء باستخدامها وكأنها جديدة.
- الطول: 90 دقيقة
- الشكل: جلسة
- مستوى المهارة: متوسط
- المعرفة المطلوبة:
- معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
- تعريف بمسألة التشفير (التشفير)
- التخزين والتشفير (أسس الأمن الرقمي، الجولة الثانية)
- جلسات/تمارين ذات صلة:
- وجهات النظر الشخصية حيال الأمن^١
- البرمجيات الخبيثة والفيروسات^٢

^١ <https://vrr.im/9339>

^٢ <https://vrr.im/47e5>

- الخصوصية^٣
- المزيد من الهويات الإلكترونية!^٤
- التخزين والتشفير^٥
- المواد اللازمة:
 - شرائح (فيها النقاط المفتاحية الواردة أدناه)
 - مفاتيح يو إس بي مجهزة بنظامي تايلز وأوبونتو Ubuntu القابلين لإعادة التشغيل.
- التوصيات: فكون في جلب مفاتيح يو إس بي مجهزة بنظام تشغيل لكل مشاركة على أن يحتفظن بها؛ والأجهزة حاسوباً لتتدرب المشاركات عليه (أو إثيين في حال عرضتن نظامي تايلز وأوبونتو التشغيليين) - وحتى لو كان الهدف من النشاط تشغيل نظامي تايلز أو أوبونتو من مفتاح يو إس بي مجهزة بنظام تشغيل، عوضاً عن تثبيتته، قد لا تشعر بعض المشاركات بالإرتياح لإستعمال حاسوبهن الخاص لإختباره. من الممكن أيضاً تغيير ذلك بحيث يسهل إدخاله إلى أي جلسة مخصصة لانشاطات لا يخنن من شيء في ورشتكن التدريبية، يرغن في تغيير الأنظمة التشغيلية بالكامل من ماك أو ويندوز إلى نظام كنظام أوبونتو من شركة لينوكس linux.

إدارة الجلسة

الجزء الأول - تبديد الخرافات

الجزء الأول - تبديد الخرافات

١. إبدأن الجلسة بشرح الهدف من هذه الجلسة: إعادة تأكيد قدرة الإنسان على التحكم بالتكنولوجيا، وتبديد فكرة أن الأجهزة الرقمية لها "قوى خارقة" تسيطر من خلالها على مستخدميه. في حال قدمتن جلسة وجهات النظر الشخصية حيال الأمن للمشاركات، يمكنكن تذكيرهن بما يلي من التأكيدات الختامية:

<https://vrr.im/819e٣>

<https://vrr.im/e9f7٤>

<https://vrr.im/0ccc٥>

ليس للأدوات والتكنولوجيا سطوة سحرية خارقة علينا! نحن من يقرر ما يمكنها الوصول إليه، وفي حال طرأ أي حادث، يمكننا دوماً إعادة ضبطها!

الجزء الثاني - ما الذي نعينه فعلياً بإعادة الضبط؟

٢. كررنا للمجموعة هذا التأكيد من المرحلة السابقة، وشددنا على الجملة الأخيرة منه "يمكننا دوماً إعادة ضبطها" - ماذا يعني ذلك؟ إشرح لنا ذلك عبر تقديم السيناريو التالي: لعلك في إحدى محطات مسيرتك مع الأمن الرقمي، شعرت أنك تقمّن بكل شيء بالطريقة الخاطئة.

تنظرون إلى حاسوبك - هو مليء بالبرمجيات المقرصنة والأفلام والبرامج التلفزيونية المنزلة عبر منصة "تورينت" والملفات الأخرى المبعثرة التي لا تتذكرن حتى أنك نزلتها. استخدمت مفاتيح اليو إس بي من دون تمييز - على حاسوبك المحمول، وعلى حواسيب وآلات طباعة في مقاهي إنترنت، وربما لا تقمّن دائماً بإخراجها بالطريقة الصحيحة حين تنتهي من استخدامها.

ربما انفصلت مؤخرًا عن شخص ما تعرفن جيداً أنه/ها كان يفتح حاسوبك في غيابك - وربما قام/ت بتخمين كلمة السرّ أو حتى أعطيتنه/ها إياها بأنفسكن.

والآن، تشعرن بأنك فقدت السيطرة - من يعرف ما نوع الفيروسات الموجودة على قرصك الصلب، أو من ياترى له القدرة على الوصول إلى معلوماتك؟ ولكن على فكرة، ذلك ليس مشكلة كبيرة! لم يفت الأوان بعد لفتح صفحة جديدة. هل ترغبن في فتح صفحة جديدة؟ هذه الجلسة معدة خصيصاً لكنّ إذا!

٣. والآن، بعد أن قرأت السيناريو الوارد أعلاه لتحديد السياق، يمكنك شرح ما يعني مصطلح إعادة الضبط في هذا السياق: أي البدء من خانة الصفر عبر إعادة ضبط جهازك أو حاسوبك إلى حالته وإعداداته الأصلية، وبالتالي منح أنفسكن "صفحة بيضاء" لمسيرة الأمن الرقمي الخاصة بكن.

لا تسين تذكير المشاركات أن هذه الجلسة ستفسّر لهن كيفية إجراء عملية إعادة ضبط - لن يتوجب عليهن إجراء عملية إعادة ضبط خلال الجلسة، أو حتى خلال التمرين. فقد تترتب نتائج سيئة جداً عن عملية إعادة الضبط في حال لم تكن المشاركات جاهزات لها، أو في حال لم يقمن بإجراء نسخ احتياطية لبياناتهن مؤخراً - وقد يحتجن لحواسيبهن المحمولة بما أنهن يرغبن حالياً بالمحافظة على قدرتهن على الوصول إلى بياناتهن إلى أن يصبحن جاهزات أكثر لإجراء عملية إعادة الضبط. ولكن، خلال هذه الجلسة ستتاح للمشاركات فرصة التدرّب بواسطة أنظمة تشغيل بديلة على حواسيبهن، وهذا ما يشكل محطة تحضيرية مهمة في حال قررن إجراء عملية إعادة ضبط لاحقاً.

الجزء الثالث - التحقق: هل تحتجن لإنشاء نسخ احتياطية؟

٤. يفصّل أن تكنّ قد قدمتن قبل الآن جلسة التخزين والتشفير للمشاركات بما أنها تناولن نقاطاً مهمة في مجال إنشاء نسخ احتياطية للبيانات. بكل الأحوال، قبل أن تبدأن بالجزء الخاص بالممارسة التطبيقية من هذه الجلسة، قمن بعملية تحقق سريعة مع المجموعة حول إنشاء نسخ احتياطية لبياناتهن.

إختياري: كتذكير سريع بجلسة التخزين والتشفير، إسألن المشاركات - كم مرّة في السنة يقمن بنسخ احتياطي لملفاتهن؟ شاركن أمثلة عن الممارسات الفضلى في مجال إنشاء نسخ احتياطية للبيانات، من قبيل الإحتفاظ بالنسخة الإحتياطية في مكان آمن منفصل عن حاسوبهن، وإنشاء نسخ احتياطية لمعلوماتهن بشكل دوري ومتكرر، بحسب المعلومات التي ينشأ لها نسخ احتياطية، والتفكير أيضاً في تشفير القرص الصلب أو وسيط التخزين حيث سيقمن بتخزين البيانات.

الجزء الرابع - إعادة الضبط وإعادة التشغيل Resetting & Rebooting

٥. قبل البدء بالجزء الخاص بالممارسة التطبيقية من هذه الجلسة، لا بد من تناول مسألة مهمة هي العلاقة بين إعادة التشغيل وإعادة الضبط فرمما إستخدم هذان المصطلحان من

دون تمييز بينهما طوال هذه الجلسة:

يدلّ هذان المصطلحان إلى عمليتين تشبه بعضهما إلى حد كبير بالمعنى العام، ولكن ذكرن المشاركات أن كلمة "إعادة الضبط" تستخدم هنا للدلالة على مفهوم "فتح صفحة جديدة" في سياق هذه الجلسة. عملية إعادة التشغيل هي عملية تقنية تجريها حواسيبهن خلال عملية إعادة فتحها؛ هي عملية مهمة أيضاً يجب فهمها من أجل الممارسة التطبيقية لأنظمة التشغيل البديلة التي ستجرى في الجزء التالي من الجلسة.

٠٦. لمزيد من التوضيح للفكرة الواردة أعلاه، قدمنا أنظمة تشغيل تايلز وأوبونتو إلى جانب تقديم بعض المعلومات التقنية القيّمة للمشاركات التي ستكون مفيدة في الجزء التالي من الجلسة. إشرحن ما الذي يجعل من تايلز وأوبونتو نظامين بديلين عن أنظمة التشغيل الأخرى مثل ماك أو إس وويندوز - في هذه الجلسة، سيركز الجزء الخاص بالممارسة التطبيقية على تشغيل هذين النظامين التشغيليين من مفتاح يو إس بي.

الجزء الخامس - الأنظمة التشغيلية الحية

٠٧. قد يطرح عليكم سؤالاً من قبيل: كيف يمكننا استخدام النظام التشغيلي الجديد على حواسيبنا المحمولة من دون التخلّص من الذي نستخدمه الآن؟ ماذا سيحدث لبياناتنا؟ عليكم الآن إغتنام هذه الفرصة لشرح بعض المصطلحات للمشاركات قد تساعدهن على فهم كيفية عمل تايلز وأوبونتو في سياق هذه الجلسة بشكلٍ أوضح:

النظام الحي Live System

النظام الحيّ هو نظام تشغيلي يمكن تشغيله مباشرة من وسيط تخزين خارجي مثل مفتاح يو إس بي أو شريحة ذاكرة. نظام تايلز التشغيلي هو مثال عن الأنظمة الحية؛ ومن الممكن إعداد أوبونتو للعمل كنظام حيّ، وهو "نسخة" أخرى عن النظام التشغيلي المستند إلى نظام لينوكس الذي يستعين به نظام تايلز.

لينوكس Linux

لينوكس نظام تشغيلي شبيه بنظامي ويندوز وماك، إلا أن الفرق الرئيسي بينه وبينهما هو أنه موزع كبرمجية مجانية ومفتوحة المصدر. ولذلك، تتوفر نسخ مختلفة كثيرة مستندة إلى نظام لينوكس - نظام دبيان Debian، هو إحدى النسخ الأكثر شعبية وهو يشكل أساس نظام تايلز.

الجهاز القابل للتشغيل Bootable Device

أجهزة التشغيل (أو القابلة للتشغيل) هو جهاز أو قرص يمكن للحاسوب تحميل ملفات منه للتمكن من العمل. على سبيل المثال، على معظم الحواسيب يعتبر القرص الصلب جهاز التشغيل الذي يتم من خلاله تحميل نظام التشغيل (مثل ويندوز) عند تشغيل الحاسوب. بالإضافة إلى الأقراص الصلبة، تعتبر الوسائط كالأقراص المدمجة CD وأقراص دي دي DVD وشرائح الذاكرة ومفاتيح اليو إس بي من الأجهزة القابلة للتشغيل.

نظام الإدخال والإخراج الأساسي (Basic Input/Output System Bios)

نظام الإدخال والإخراج الأساسي BIOS هو البرمجية الأولى التي تشغيلها معظم الحواسيب حيث يتم تشغيلها. يستخدم هذا النظام لإجراء عمليات إختبار ذاتية على الأنظمة والأجهزة لضمان عملها بشكل سليم، ومن أجل تفعيل تسلسل التحميل للبرمجيات (كالأنظمة التشغيلية) الموجودة على الأجهزة القابلة للتشغيل المتوفرة. يتمتع نظام الإدخال والإخراج بواجهة تفاعلية، ولكن لا يمكن للمستخدمين الوصول إليها إلا إذا قاموا بخطوة محددة خلال إقلاع الجهاز للوصول إليه مباشرة.

تسلسل التشغيل

تسلسل التشغيل، الذي يمكن الوصول إليه من خلال نظام الإدخال والإخراج (أو واجهة البرنامج الثابت الممتد UEFI) أثناء إقلاع حاسوبٍ ما، هو لائحة بالأجهزة القابلة للتشغيل على حاسوبٍ ما - يستخدم لتحديد التسلسل الذي يحاول الحاسوب وقته تحميل المعلومات من هذه الأجهزة. عادةً القرص الصلب في الحاسوب هو الجهاز الأول في تسلسل التشغيل، ومنه يتم تحميل نظام التشغيل. ولكن من الممكن تغيير تسلسل التشغيل ليحمل معلومات من أجهزة خارجية قابلة للإزالة أولاً كأقراص دي في دي أو مفاتيح اليو إس بي.

الجزء السادس - الممارسة التطبيقية

٨. للبدء بالجزء المخصص للممارسة التطبيقية من هذه الجلسة، قسمن المشاركون إلى مجموعتين على الأقل. قدمن لكل مجموعة حاسوباً ليجرين عليه تشغيل نظام أوبونتو أو تايلز من مفتاح يو إس بي معدّ مسبقاً؛ أو، في حال توفر لديكن العدد الكافي من مفاتيح اليو إس بي المعدّة مسبقاً لكل المشاركين، عندها سيتمكن من التدرّب كل واحدة على حدة (في هذه الحالة، ستقمن بجعل الجميع يتدربن على استخدام إما نظام تايلز وإما نظام أوبونتو)

٩. على حاسوبكن المحمول، وبواسطة جهاز عرض، وجهن المشاركون عند إجرائهن لعملية إعادة تشغيل حواسيبهن وإطلاق نظام تايلز/أوبونتو خلال تسلسل تشغيل نظام الإدخال والإخراج. وأثناء قيامكن بذلك، إحرصن على شرح الفوارق بين نظامي تايلز وأوبونتو لكي تفهمن المجموعة بشكلٍ أفضل كيفية استخدامها في عملية "إعادة الضبط" الخاصة بهن.

١٠. إختتمن الجلسة بمناقشة كيف يمكن أن تكون عملية إعادة الضبط بواسطة تايلز أو أوبونتو خياراً لفتح "صفحة جديدة" على حواسيب المشاركين في حال التعرّض لهجوم برمجيات خبيثة أو أي فقدان آخر للسيطرة، ولكن إحرصن أيضاً على ذكر أنواع أخرى

من الهجمات التي لا ينفع فيها هذا الحلّ بشكلٍ فعال، كالعنف على الإنترنت.

المراجع

- <https://tails.boum.org/>
- <http://www.ubuntu.com>



النساء فى فضاء الإنترنت



العنف على الإنترنت ضد
النساء

باب ٣٣

طيف الآراء

- الأهداف: يوفر هذا التمرين طريقة مفيدة للمشاركة للتعرف على أفكار بعضهم البعض بشأن مسائل محددة، عبر إنشاء "طيف من الآراء" في مكان التدريب.
- الطول: 90 دقيقة
- الشكل: تمرين
- مستوى المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
- جلسات/تمارين ذات صلة:
 - إنترنت نسوي¹
- المواد اللازمة:
 - غرفة كبيرة أو مساحة في الهواء الطلق
 - أنفسكن!

محتوى هذا التمرين وضعته ماريليل غارسيا Mariel Garcia من منظمة سوشل تي آي سي SocialTIC وسبيروس موناستيرويوتيس Spyros Monastiriotis من منظمة تاكتيكل

¹ <https://vrr.im/d7d1>

إدارة التمرين

- ٠١ إبدآن الجلسة بإرشاد المجموعة إلى مكان طرفي الطيف - في حال إستخدام مكان داخلي، يمكن استخدام الجهتين المعاكستين من الغرفة لهذا الغرض؛ أما بالنسبة للمساحات في الهواء الطلق، يمكن الإستعانة بشجرتين أو حائطين أو أي معالم أخرى.
- ٠٢ إشرحن لهن أن كل طرفٍ منهما يدلّ على رأي عام - حددن أن إحدى الجهتين ستمثّل الرأي "الموافق جدًّا" والجهة الأخرى ستمثّل الرأي "المعارض بشدّة".
- ٠٣ والآن، إشرحن لهن سير التمرين - ستقرآن عبارات بصوتٍ عالٍ (لا بد من تسميتها بالعبارات وليس بالأسئلة)، ومن ثمّ تكرارها؛ ومن بعدها، تقمن المشاركات بترتيب مواقعهن وفقًا لطيف الآراء من "موافق جدًّا" إلى "معارض بشدّة" بحيث تعبرن عن مدى أهمية العبارة الذي تمت قراءتها.
- ٠٤ ذكرن المشاركات أنهن لسن مضطرات لإختيار الجهة القصوى المعينة من طيف الآراء أو الجهة الثانية؛ يمكنهن أيضًا الوقوف في منتصف المساحة في حال لم يكونّ رأياً في موضوع ما، أو يمكنهن الوقوف في أي موقع آخر يشير إلى مدى موافقتهن أو رفضهن للعبارة
- ٠٥ ي طيف الآراء هذا، ستقرآن بصوتٍ عالٍ عبارات عدّة مرتبطة بالأمن الرقمي وتجارب النساء على الإنترنت - إليكن في ما يلي بعض الأمثلة على العبارات التي يمكنكّن إستخدامها:
 - لا يوجد سبب وجيه لمشاركة أي شخص لكلمة سرّ بريده الإلكتروني/حساب وسائل التواصل الإجتماعي.
 - أحيانًا، لا بد لنا كنساء أن نتفادى مشاركة بعض الآراء على الإنترنت .

-
- النشاطات والناشطون يواجهون نوع العنف ذاته الذي يؤدي إلى نوع من أنواع العنف والتهديدات على الإنترنت.
 - يصبح عملياً مستحيلاً في حال عدم توفر إمكانية وصول آمنة إلى المساحات الإلكترونية.

٠٦. بعد أن تنتهي المشاركات من ترتيب تمركزهن من بعد الإدلاء بعبارة ما، أطلبن من مجموعات من إثنين إلى ثلاث مشاركات عن سبب إختيارهن لمكان وقوفهن فقد يحول ذلك النقاشات إلى نقاشات مثيرة للاهتمام.

٠٧. يمكنكن أيضاً إطلاع المشاركات أنه في حال، من بعد الإستماع إلى شرح إحداهن ، قررن تغيير رأيهن، يمكنهن الإنتقال إلى مكان آخر على الطيف في حال أردن ذلك - إحرصن على السؤال عن سبب تغيير المكان!

باب ٣٤

إنترنت نسوي

- الأهداف: هذه الجلسة التعريفية العامة عن وحدة العنف ضد المرأة على الإنترنت هدفها توفير فرصة لزيادة نسبة الوعي لدى المشاركات تجاه التحديات التي تواجه النساء في المساحات على الإنترنت.
- الطول: 40 دقيقة
- الشكل: جلسة
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
 - قصتها مع التكنولوجيا^١
 - العنف الرمزي^٢
- المواد اللازمة:
 - أوراق لوح ورقي
 - أقلام خطاطة ملونة

^١ <https://vrr.im/c865١>

^٢ <https://vrr.im/075e٢>

- نسخ عن مستند مبادئ الإنترنت النسوي للمشاركة

إدارة التمرين

الجزء الأول - التوعية

١. إبدآن الجلسة بسؤال المشاركات - ما هي الرسائل أو الأفكار المتداولة التي سمعنها عن النساء والتكنولوجيا؟ ما هي الآراء المسيطرة تجاه النساء والتكنولوجيا في بلدانهم؟
٢. أطلبن من المشاركات التفكير معاً ببعض العوائق التي تواجهها النساء في أغلب الأحيان حين يحاولن الوصول إلى التكنولوجيا وإستخدامها، أو المشاركة بشكلٍ فاعل في مساحات الإنترنت. يمكنهن القيام بذلك ضمن مجموعة واحدة أو ضمن مجموعات صغيرة - انخيار يعود لكن. سيجلن العوائق التي تذكرها المجموعة على ورقة كبيرة من أوراق اللوح الورقي.
٣. من بعد الإنهاء من عملية التفكير والمناقشة، شاركن بعض الإحصائيات العالمية التالية مع المشاركات - وإن أمكن، حاولن أيضاً ذكر إحصائيات خاصة ببلد معين أو منطقة معينة مرتبطة ببيئة المشاركات:

- نسب الإستخدم والوصول إلى الإنترنت أعلى لدى الرجال من لدى النساء في كل مناطق العالم - الفجوة الجندرية العالمية في استخدام الإنترنت بين الجنسين هو 12 في المئة.
- 60 في المئة من حالات العنف ضد النساء المرتبطة بالتكنولوجيا لم تحقق بها السلطات.
- من بين كل محرري موقع ويكيبيديا على الإنترنت في العالم، تتراوح نسبة الذكور منهم بين 84 و 91 في المئة.
- تشغل النساء 27 في المئة من وظائف الإدارة العليا في الشركات الإعلامية و 35 في المئة من اليد العاملة في غرف التحرير.
- تحصل النساء العاملات في مجال التكنولوجيا على رواتب أدنى مما لا يقل عن 28 في المئة من الرواتب التي يحصل عليها الرجال من المستوى العلي ذاته وعدد

سنوات الخبرة ذاته والعمر ذاته.

٤. قسمن المشاركات إلى مجموعات صغيرة وأطلبن منهن التفكير في البيانات المشاركة - ما هي تداعيات هذه الإحصائيات على حياة النساء وعلى شكل الإنترنت كمساحة مشتركة ومتاحة مجاناً لاستخدام الجميع؟

الجزء الثاني - المبادئ النسوية للإنترنت

٥. والآن قدم من المبادئ النسوية للإنترنت التي وضعتها الجمعية التقدمية للاتصالات APC، كتمرين للتفكير في ما يلزم لبناء:

... إنترنت نسوي يعمل على تمكين النساء وغيرهن من الفئات المهمشة مثل الأقليات الجنسية والجنسانية والتمتع بحقوقهن والتمتع والمرح والقضاء على الذكورية.

٦. زودن كل مجموعة من المجموعة بقسمٍ من المبادئ النسوية للإنترنت - قد تكون هذه المبادئ هي المستند نفسه (بعد تنزيله من الموقع الإلكتروني) أو نص المبادئ المقسمة إلى فئات هي:

- إمكانية الوصول
- الحركات والمشاركة العامة
- الإقتصاد
- التعبير
- القدرة على الاختيار

٧. أطلبن من كل مجموعة مناقشة كيف يمكن تطبيق كل مجموعة من المبادئ في بيئتهن ووضع لائحة بالطرق التي يمكن فيها لكل مشاركة المساهمة في تغيير واقع النساء والتكنولوجيا.

٨. أطلبن في الختام من كل مجموعة عرض المبادئ بالإضافة إلى إستنتاجاتهن التي فكرن فيها.

المراجع

- <http://feministinternet.net> •
- https://en.wikipedia.org/wiki/Gender_bias_on_Wikipedia •
- http://cdn.agilitycms.com/who-makes-the-news/Imported/report_s_2015/global/gmmp_global_report_en.pdf •

باب ٣٥

العنف الرمزي

- الأهداف: يعرض هذا التمرين للمشاركات كيفية تحديد حالات العنف الرمزي وكيفية الربط بين العنف الرمزي والعنف القائم على الجندر على الإنترنت.
- الطول: 30-45 دقيقة
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
- جلسات/تمارين ذات صلة:
 - طيف الآراء^١
 - إنترنت نسوي^٢
- المواد اللازمة:
 - شريط لاصق
 - ألواح ورقية
 - أقلام أو أقلام رصاص

^١<https://vrr.im/5e60>

^٢<https://vrr.im/d7d1>

- أوراق ملونة
- قصاصات لاصقة

إدارة التمرين

الجزء الأول - ما هو العنف الرمزي؟

١. إبدآن بشرح ما المقصود بمصطلح "العنف الرمزي":

العنف الرمزي ينتج عن فرض الأعراف والسلوكيات الثقافية المرتبطة بالجنس. فالنساء يتعلمن من صغرهن أن "أمرًا ما" قد يحدث لهن إذا قررن المشي وحدهن في الليل أو اعتماد طريقة لبس معينة أو التصرف بلا مبالاة، عندها يصبح الخوف لدي النساء حالة ذهنية طبيعية ومقبولة.

وهذا يعني أننا كنساء نُحمّل مسؤولية أي عنف نواجهه، فيولد بدوره الخوف أو حتى الملح - ينتج هذا الخوف أو الملح "خارطة ذهنية بالأماكن المنوعة" علينا، مما يولد ردود فعل مشروطة من قبيل:

الشعور بالحاجة إلى العودة إلى المنزل في الليل في سيارة أجرة أو مع مرافق، المشي بسرعة أكبر أو حتى الركض في حال سمعنا صوت خطي ورائنا، ممارسة الرقابة الذاتية لا شعورياً على وسائل التواصل الاجتماعي والمنصات الإلكترونية الأخرى؛ اختيار عدم الخروج أو اللبس بطريقة معينة خشية ما قد يحدث لنا؛

إضافة إلى ذلك، مع أن النساء يجبرن على تحمّل مسؤولية العنف الذي نعيشه، لم تقدم أبداً في الوقت عينه إستراتيجيات وموارد لمعالجة ذلك العنف (عدا ردود الفعل المشروطة المذكورة أعلاه)، ولا إستراتيجيات وموارد للتمتع والسيطرة على المساحات المتاحة أو للتحرك والتعبير عن أنفسنا وعن جسدنا وجنسائيتنا بجرية، إلخ.

ينتج عن العنف الرمزي مساحات وحالات ممنوعة على النساء، مما يمنعنا عن حقنا الأساسي في الأمن والتحرك بحرية؛ وما يزيد من الطين بلة هو الحصانة المعطاة غالباً للمعتدين، ففي أغلب الأحيان، لا يخضعون للتحقيق أو المساءلة بل يصنفون "كجانيين" أو كغير قادرين على التحكم أو تتحمل مسؤولية أفعالهم.

وقد يتوجب علينا هنا مناقشة صور عن حالات عنف ضد النساء (إن كان رمزياً أو غير ذلك) توزع وتطبع من خلال وسائل الإعلام، ولا سيما في المساحات المتاحة على الإنترنت.

الجزء الثاني - تحديد حالات العنف الرمزي التي إختبرناها

٢. وزعن على كل مشاركة رزمة صغيرة من القصاصات اللاصقة، عليها سيتوجب عليهن تحديد وتدوين أمثلة عن أنشطة توقفن عن القيام بها، أو سلوكيات عدلنها بسبب العنف الرمزي الذي يختبرنه كنساء في مساحات الواقع والقضاء الرقمي على حد سواء. من بعد الإنتهاء من ذلك، إجمعن القصاصات اللاصقة وإقرأن بعض الأمثلة المدونة بصوت عالٍ - ناقشنها معاً كجموعة، وعلقن على المحفزات المحتملة لتغيير هذه السلوكيات والخاوف المحسوسة.

٣. مباشرة من بعد النقاش الجماعي، إشرحن أن ثلاثة عوامل رئيسية تؤدي إلى نشوء الخوف والهلع وإنتشارهما كرد فعل على العنف الرمزي:

- السيطرة على جسد المرأة: ما زال ينظر إلى جسد المرأة على أنه أداة لمتعة الرجل، وينتج عن ذلك انعدام الإحساس بالأمن أو الثقة في موارد الجسد وقدراته.
- الشعور بالذنب والعار: يعتبر هذين الشعورين دائمين وعنصرين ثابتين يسهلان النظر إلى حالات العنف المرتكبة القائمة على النوع الاجتماعي كنتيجة مستحقة وأومقبولة إلى حد ما.
- "العجز الملقن": هذه عبارة عن حالة نفسية تنشأ في أغلب الأحيان حين ينظر

إلى الأحداث الجارية كأحداث خارجة عن السيطرة - حين يعتبر أنه لا يمكن القيام بأي شي لتغيير نتيجة ما حصل، بتكيف الحالة النفسية مع ذلك، مضحية بالتالي بقدرتها على التحكم بتلك النتيجة (فتقبله وتعتبره طبيعياً عوضاً عن ذلك).

٤. من بعد شرح هذه العوامل الثلاثة، إسألن المشاركات عن الإستراتيجيات التي تخطر على بالهن من أجل تحويل تلك العوامل إلى مقاربات لمعالجة العنف الرمزي! أطلبن منهن كتابتها على القصاصات الورقية اللاصقة. نعرض أدناه بعض الإستراتيجيات المحتملة التي يمكن طرحها:

- إستعادة السيطرة على الخطاب المرتبط بأجسادنا والتعريف بها والتأكيد على أنها مساحة خاصة بالمتعة والصمود في الوقت عينه.
- الإقرار وعدم إنكار أن هناك ضرر لحق بأجسادنا (على المستوى الجسدي أو النفسي)، وتخطي أي نظرة إلى الذات بأننا ضحايا ومحاولة بناء قدرة الناجيات على الصمود.
- بناء شبكات دعم والمحافظة عليها لكن وللأخريات على الإنترنت وفي عالم الواقع. لن نكون وحدنا أبداً في هذا النضال

المراجع

- https://en.wikipedia.org/wiki/Learned_helplessness
- <http://www.autodefensafeminista.com/attachments/article/277/>
- MANUAL%20Autodefensa%20Feminista.pdf

باب ٣٦

التبليغ عن الإساءات على منصات التواصل الاجتماعي

- الأهداف: في هذه الجلسة، ستقدم للمشاركات بعض النصائح حول العنف على الإنترنت في منصات التواصل الاجتماعي مثل فايسبوك وتويتر.
- الطول: 40 دقيقة
- الشكل: جلسة
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟^١
- الحملات الآمنة على الإنترنت^٢
- التبليغ عن الإساءات على منصات التواصل الاجتماعي^٣

<https://vrr.im/47ba>^١

<https://vrr.im/8e6b>^٢

<https://vrr.im/01ad>^٣

- لنبدأ بتوثيق الحالات!؛
- المواد اللازمة:
 - جهاز عرض وشرائح عرض
 - قصاصات ورقية لاصقة
 - حاسوب لكل مشاركيتين (إن أمكن)
- التوصيات: يوصى بهذه الجلسة لمجموعات النساء اللواتي تعرّضن للتحرش على الإنترنت أو المشاركات في حملات على الإنترنت.

إدارة الجلسة

١. إبدآن الجلسة بطرح الأسئلة التالية على المشاركات:
 - هل يعرفن بأي جماعات نسائية أو ناشطات تعرّضن للتحرش على الإنترنت؟
 - في حال كنّ يعرفن أيّاً منها، على أي منصات حصلت حالات التحرش؟
- أطلبين منهن تقديم أمثلة عن تكتيكات شهدن على إستخدامها، من قبل تلك المجموعات أو الأفراد لمعالجة أو مكافحة التحرش على الإنترنت، أو التكتيكات التي إستعنّ بها هنّ. أطلبين من المشاركات كتابة هذه التفاصيل على القصاصات الورقية اللاصقة.
٢. شاركن بعض التوصيات بشأن الممارسات الأساسية للتبليغ عن العنف ضد النساء على الإنترنت المستعان بها عادةً، بالإضافة إلى أي منظمات غير حكومية أو جماعات تقدم المساعدة في التعامل مع حالات التحرش:
 - يوصي موقع فليسبوك بالإشارة إلى التعليق أو المنشور المحدد (The exact comment or post)، وتقديم أكبر قدر ممكن من معلومات السياق في عملية التبليغ. يمكن للمشاركات الإطلاع على التحديثات على هذه العملية على الرابط التالي:
<https://www.facebook.com/report>

<https://vrr.im/899f4>

- حجب المتحرشين سيمنعهم من إرسال طلبات الصداقة أو المتابعة، ومن بدء الأحاديث أو إرسال الرسائل والإطلاع على المستجندات المنشورة على حائط المستخدم/ة. لا يُبلغ المستخدمين بحجبهم، ولكن يمكنهم أن يلاحظوا حصول ذلك، في حال لم يعودوا قادرين فجأة على التواصل مع ضيقتهم. إن التقطن صور للشاشة قبل حجب المتحرشين على المنصات للحصول على أدلة توثق التحرش - فما إن يتم حجبهم، يصبح من الصعب جداً جمع الأدلة الداعمة، التي يُطلب من المستخدمين عادةً تقديمها خلال التحقيق في الحادث (قد يتوجب عليكم تعليم المشاركات كيفية إتقاط صور الشاشات على حواسيبهن في حال كنّ لا يعرفن ذلك).
- يوصي موقع تويتر المستخدمين المستهدفين من قبل المتحرشين على الإنترنت، التبليغ عن الحادث والإحتفاظ برقم الحالة من أجل الإطلاع على أي إجراء متابعة متخذ ضد المتحرش. ومن الممكن على تويتر التبليغ عن تعريده واحدة أو صفحة شخصية كاملة.

يوصى أيضاً بتفادي نقر أي روابط قد يتم تلقيها في رسائل أو إتصالات أخرى مرسلة من قبل المتحرشين، فقد تؤدي إلى تثبيت برمجيات خبيثة على جهاز المستخدم/ة..

- ٣. خلال هذا الجزء من الجلسة، يتوجب عليكم أيضاً تعليم المشاركات كيفية حجب المستخدمين والتبليغ عن الصفحات الشخصية أو المنشورات على فايسبوك وتويتر، إلى جانب أي منصة تواصل إجتماعي أخرى يستخدمونها كثيراً. إحرصن على البحث عن هذه التفاصيل قبل التدريب من أجل أن تعرفن المستجندات، فليسوء الحظ نتغير هذه الإجراءات كثيراً (تماماً كإعدادات الخصوصية الخاصة بالحسابات).

- ٤. في حال أردتن منح المشاركات فرصة القيام ببعض الممارسة التطبيقية، يمكن تقسيمهن إلى مجموعات صغيرة وإبحثن عن صفحات قد تُستهدف من قبل المتحرشين أو المزعجين - على سبيل المثال، عليهن محاولة توثيق أي منشورات أو صفحات شخصية على فايسبوك، تُرتكب من خلالها حالات التحرش ومن ثم تقديم التقارير عبر الآلية المحددة.

المراجع

<https://karisma.org.co/descargar/manualeseguridadtw> •

باب ٣٧

لنبدأ بتوثيق الحالات!

- الأهداف: تعرّف هذه الجلسة المشاركات بالمزيد من التفاصيل حول الممارسات المرتبطة بالتبليغ عن الإساءات على الإنترنت، لا سيما توثيق الحوادث.
- الطول: 45 دقيقة
- الشكل: جلسة
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
- التبليغ عن الإساءات على منصات التواصل الاجتماعي^١
- الإستقصاء عن المعلومات الشخصية الخاصة بالمتصيد^٢
- المواد اللازمة:
 - شرائح (فيها النقاط المفتاحية الواردة أدناه)
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
 - نسخ مطبوعة عن نماذج سجل التوثيق (أدناه)

^١<https://vrr.im/01ad>

^٢<https://vrr.im/7480>

- التوصيات: يوصى بهذه الجلسة عند العمل مع مجموعات نتعامل مع حالات التحرش على الإنترنت، ومع اللواتي تلقين تهديدات على الإنترنت وفي الواقع، أو اللواتي يعملن على مشاريع أو حملات قد تزيد من خطر تعرضهن للتحرش.

إدارة الجلسة

الجزء الأول - ما أهمية التوثيق؟

١. في الجزء الأول من هذه الجلسة، ستبدأن بشرح ما يلي للمشاركات:

ما هو التوثيق؟ التوثيق في هذا السياق يشير إلى مقارنة منظمة وممنهجة لمتابعة حالات الإساءة أو التحرش التي نشهدها في سياق عملنا - والهدف الأساسي منها هو أرشفة الأدلة.

ما هو الحادث؟ الحادث هو أي تطوّر يطرأ إما على الإنترنت أو في الواقع قد يشكل إساءة أو تحرشاً - تصنيف التطوّر على أنه حادث أم لا، يعتمد كثيراً على البيئة والظروف التي طرأ فيها وشدة أثره بهذه العوامل. على سبيل المثال، في حال تلقيتين بريداً إلكترونياً يبدو وكأنه محاولة تصيد - وأنتن معتادتات على تلقيها غالباً - قد لا يكون ذلك مهماً بما فيه الكفاية لإعتبره حادثاً؛ ولكن في حال كانت منظمتهن تستعد لإطلاق حملة مهمة وبدأتن بتلقي أعداداً كبيرة جداً غير معتادة منها، قد يشكل ذلك حادثاً ولا بد من توثيقه. مثال آخر على ذلك، في حال كانت منظمتهن تستعد لإطلاق حملة مهمة وبدأتن بتلقي عدد هائل من طلبات الصداقة على فإيسبوك من غرباء.

ما هو سجل التوثيق؟ سجل التوثيق هو المكان الذي يمكنكن فيه الاحتفاظ بسجل بكل الحوادث التي تطرأ، بطريقة منظمة ستساعدكن على الاحتفاظ بمعلومات وأدلة مهمة عن كل حادث يمكن استخدامها لاحقاً أو اعتمادها كمراجع.

ما الذي يجعل عملية التوثيق بهذه الأهمية؟ التوثيق مفيد كمرجع يستخدم لاحقاً حين

تحاولن فهم الوضع بأكمله وربط حوادث مختلفة ببعضها البعض طرأت خلال إطار زمني محدد أو طالت عدداً من الأشخاص من المنظمة نفسها.

قد يكشف التوثيق أنماطاً معينة من الإساءة أو الهجمات الأخرى على الإنترنت، ربما لم تكن لتلاحظها لولاها، وعبر تقديم مجموعة من الأدلة المترابطة، إكتشاف هذه الأنماط يساعدنا في تحديد هوية الخسوم، أو في فهم مجريات الأمور والعلاقة بين أنواع معينة من الحوادث، وأنواع معينة من الأعمال التي تقمن بها أنتن أو منظمتهن. وعند التبليغ عن حوادث الإساءة على منصات التواصل الإجتماعي، على سبيل المثال، قد تُطلب أدلة كصور ملتقطة للشاشات أو أسماء الصفحات الشخصية خلال عملية التحقيق.

الجزء الثاني - كيفية توثيق الحوادث؟

٢. بعد الإنتهاء من مراجعة الفقرات الواردة أعلاه عن التوثيق ومعرفة أسباب التوثيق وأهميته، يمكنك توزيع نسخ مطبوعة من نماذج سجل التوثيق أدناه على المشاركات.
٣. أذكرن للمشاركات أن هذه النماذج توفر مثلاً واحداً فقط عن أنواع المعلومات المهمة التي لا بد من جمعها في عملية توثيق الحوادث. وهن الحرية في إضافة أو إزالة أي خانة وفقاً لتقديرهن حين يقمن بوضع نماذج خاصة ببيئة عملهن في المستقبل. 4. في ما يلي نموذجان، الأول مخصص لتوثيق الحوادث على الإنترنت، والثاني مخصص للحوادث في الواقع خارج الإنترنت:

نموذج سجل التوثيق (على الإنترنت)

ملاحظات	إجراءات المتابعة	مستوى الخطر	توصيف محتوى صورة الشاشة	صورة الشاشة (اسم الملف أو نسخ/لصق)	الرابط (URL)	المنصة	ملد ص مجرات الحاد ت	التوقيت	التاريخ

نموذج سجل التوثيق (في الواقع)

ملاحظات	إجراءات المتابعة	مستوى الخطر	الأشخاص المعنيين/ات	ملخص مجرات الحاد	المكان	التوقيت	التاريخ

٤. معظم الخانات في هذين النموذجين واضحة الوظيفة؛ ولكن، سيتوجب عليك مع ذلك شرح العملية لكل أفراد المجموعة، عبر وصف موجز لكل واحدة منها (أي ما يجب أن نتابعه المشاركات للمء كل واحدة منها).

٥. إحرص على التركيز على خانة مستوى الخطر، فهذه الخانة ذاتية بإمتمياز وأقل وضوحاً من الخانات الأخرى. وكيفية تعريف المشاركات و/أو المنظمات لمستويات الخطر مرتبط إلى حد كبير ببيئته الخاصة - من المفيد هنا التوقف عن الشرح والطلب من المشاركات تقديم أمثلة عن حوادث يصنفن خطرها كخطر ذو مستوى منخفض، أو متوسط أو مرتفع (على سبيل المثال). شددن للمشاركات أنه سيتوجب عليهن التفكير في الأثر المحتمل للحادث (إما على المستوى الشخصي وإما على مستوى المنظمة، وإما الإثنين معاً) عند التعريف بالخطر في هذه البيئة.

إختياري: إما قبل أو مباشرة بعد هذه الجلسة، فمن يتمرّن نماذج المخاطر القائمة على النوع الإجتماعي مع المشاركات. خلال ذلك التمرّن، ستستنى فرصة أفضل للمجموعة للتعريف بمستويات الخطر في بيئتهن الخاصة - ويمكنهن تطبيق هذه التعريفات للمخاطر في سجلات التوثيق الخاصة بهن.

٦. وختاماً، لا بد من التشديد أيضاً على خاتمة إجراءات المتابعة خلال هذا الجزء من الجلسة. فإجراءات المتابعة في هي فعلياً الخطوة التالية المتخذة لمعالجة الحادث الحالي (مثلاً تقديم تقرير تبليغ على فيليبسوك)، أو إجراء سينفذ لمنع أي حادث مماثل في المستقبل أو التقليل من أثره.

إختياري: إما قبل أو مباشرة بعد هذه الجلسة، فمن بجلسة الخطط والبروتوكولات الأمنية الخاصة بالمنظمة مع المشاركات. خلال هذا التمرّن، ستستنى فرصة أفضل للمجموعة لتحديد الخطط والبروتوكولات الأمنية الخاصة بالتعامل مع مخاطر معروفة أو محتملة معيّنة - لا بد من خطوات مشابهة عند التخطيط لإجراءات متابعة الحوادث.

الجزء الثالث - وضع سجلات التوثيق

٧. أطلبين من المشاركات البدء بملاء نماذج سجلهن بشكلٍ فرديّ - بمنحنهن من 10 إلى 15 دقائق لملاء أكبر قدر ممكن من الخانات. يمكنهن ملء الخانات بمعلومات مفصلة عن الحوادث الفعلية التي تعرضن لها في حال رغبن في ذلك، ويمكنهن أيضاً استخدام أمثلة إقتراضية للتدرّب على ملء النماذج.

٨. من بعد أن ينتهين من وضع المسودة الأولى للسجل، أطلبين منهن تشكيل مجموعات من شخصين ومشاركة الحوادث التي سجلنها مع شريكاتهن - في هذه المرحلة، يفضل جمع مشاركتين من المنظمة ذاتها (إن أمكن). على كل ثنائي تبادل طرح الأسئلة حول مستوى التفاصيل أو دقتها في تقارير الحوادث الخاصة بهما - في بعض الحالات، قد يساعد ذلك المشاركات على تذكر بعض التفاصيل المحددة لم يتذكرنها قبل ذلك. تجدر الإشارة إلى أن بعض المشاركات قد لا يرتحن لمشاركة سجلهن مع الأخريات، لذا أُنحن

لهن إمكانية العمل وحدهن إن أردن ذلك.

الجزء الرابع - ممارسات ونصائح عن كيفية الحفاظ على سجلات التوثيق

٩. ذكّر المشاركات، أنه من أجل المحافظة على سجلات التوثيق ومتابعتها بشكلٍ دوري، سيتوجب عليهن إيجاد طرق لدمج عملية تحديث في الإجراءات الروتينية الموجودة داخل كل منظمة. إن كنّ يعملن في منظمة، على المشاركات التفكير في ما إذا ستוכל مهمة جمع المعلومات للسجل إلى شخص محدد؛ أو قد يكون من الأسهل أو الأفضل تناوب الأفراد أو الفرق على إجراء المهمة. عليكن أيضًا التذكير أنه في حال تعرّض شخص ضمن المنظمة لحادث، قد يكون من المفيد تولى شخص آخر مهمة توثيق الحادث.
١٠. شجّعن المشاركات على إختبار سبل عمل مختلفة لجعل عملية تحديث سجلات التوثيق الخاصة بهن أكثر كفاءة وفعالية - قد تتوفر طرق لجعل بعض الإجراءات تتم بشكل أوتوماتيكي، أو قد يجدن أن بعض خانات النموذجين الواردين أعلاه غير مهمة في بيئتهن (وهذا ما سيوفر عليهن أي عمل غير ضروري).
١١. إختتمن الجلسة بسؤال المشاركات، بعد منحهن الوقت اللازم للتفكير في أهمية توثيق الحوادث في بيئاتهن، إن كنّ أستقين أي عبر أساسية من النقاش أو أفكار، بشأن كيفية المحافظة على السجل وجعل عملية تحديثه أكثر سهولة.

باب ٣٨

الإستقصاء عن المعلومات الشخصية الخاصة بالمتصيد

- الأهداف: عرّفن المشاركات على مجموعة من الأدوات والأنشطة الخاصة بجمع المعلومات حول المتصيدين والمتحرشين بهن على الإنترنت. يمكن إستخدام هذه المعلومات لمساعدتهن في إتخاذ القرارات بشأن الخصوصية والأمن على الإنترنت.
- الطول: 180 دقيقة
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
- ماذا يمكن لبياناتكن الوصفية أن تفصح عنكن؟ (المناصرة الآمنة على الإنترنت)
- التصفح الآمن (أسس الأمن الرقمي، الجولة الأولى)
- جلسات/تمارين ذات صلة:
- التصفح الآمن¹

¹<https://vrr.im/aee7>

- ماذا يمكن لبياناتك الوصفية (Metadata) أن تفتح عنك؟^٢
- لنبدأ بتوثيق الحالات!^٣
- المواد اللازمة:
 - شرائح (فيها النقاط المفتاحية الواردة أدناه)
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
 - نسخ مطبوعة عن نموذج سجل التوثيق (على الإنترنت)
- التوصيات: يوصى بهذا التمرين لمجموعات المدافعات عن حقوق الإنسان اللواتي يتعرضن حالياً لحالات تحرش/ تهديد على الإنترنت، أو اللواتي تعرضن مؤخراً لها. مع أن هذا ليس مطلوباً، ولكن يفضل إجراء هذا التمرين من بعد جلسة "لنبدأ بتوثيق الحالات!"^٤ يفضل إجراء هذا التمرين والمشاركات معهن أجهزتهن الخاصة أو حواسيبهن. قد يتوجب عليكن تقسيم هذا التمرين إلى جزئين، فهو تمرين طويل ومكثف. كما يمكنكن تنفيذه من دون تقسيمه ولكن مع تخصيص إستراحة أطول من العادة عند منتصفه.

هذا التمرين مستقى من نشاط وضعه كل من إنديرا كورنيوليو Indira Cornelio (من سوشل تي آي سي SocialTIC) وفي ريكويم Phi Requiem (#سيغوري دادديجيتال Seguri-dadigital) بالتعاون مع مشروع "تايبك باك ذا تيك" (لنسترد التكنولوجيا) للجمعية التقدمية للاتصالات

إدارة التمرين

الجزء الأول - ما هو الإستقصاء؟

١. إشرحن للمشاركات ماهية الإستقصاء - هي القيام بجمع كمية مهمة من المعلومات الشخصية عن شخصٍ ما ومن ثمّ نشرها للعموم (على الإنترنت عادةً). عليكن أن تشرحن أن هذا النوع من الإستقصاء يستخدم أحياناً ضد أشخاص للائتيقار منهم،

<https://vrr.im/1598٢>

<https://vrr.im/899٣>

وغالباً ما يستخدم المضايقة وتهديد وتعريض الناشطين/ات والمدافعين/ات عن حقوق الإنسان للخطر.

٢. شددن على أهمية ما يلي للمشاركات قبل متابعة هذا التمرين:

الهدف من هذا التمرين هو عدم التوصية بعملية الإستقصاء كممارسة فضلى (أو عدم التوصية بإستخدام وسائل غير قانونية أو مريبة للقيام بذلك) - الإستقصاء هذا يعنى نشر معلومات شخصية للعلن، لذا لا بد من التشديد على أن "نشر" هوية أو معلومات شخص ما غير ضروري. هدف هذا التمرين هو تعلم المشاركات كيفية جمع هذا النوع من المعلومات لمساعدتهن على إتخاذ قرارات بشأن كيفية التعامل مع حالات الإساءة أو التحرش.

٣. ختاماً، إشرح أيضاً أنه لا بد للمشاركات من تذكّر ما يعرفه عن ممارسات التصفّح الآمن حيث يتخلل جزء من هذا التمرين زيارة صفحات ومساحات المتحرّشين على الإنترنت

الجزء الثاني - تحديد هوية المتحرشين

٤. إحرصن على العمل مع المشاركات على تحديد توقعاتهن لهذا التمرين، وإسألنهن - ما الذي يردن معرفته عن المتحرشين بهن؟ أذكرن عدداً من الدوافع الممكنة قبل أن تبدأ المشاركات بالتمرين:

- هل ذلك لمعرفة هويتهم الحقيقية؟
- لفهم دوافع تحرشهم بهن؟
- لمعرفة إن كانوا يتحشون بمدافعات أخريات عن حقوق الإنسان أيضاً؟
- لمعرفة إن كان وراء التحرش شخص واحد أو عدة أشخاص يتصرفون وكأنهم شخص واحد؟

٥. قد تجدن أن بعض المشاركات سبق لهن أن سمعن بطرق للحصول على هذا النوع من المعلومات عن المتحرشين بهن، ولكن وضح لهن أن الأدوات والتكتيكات التي

ستشاركهن إياها لا تكفي وحدها. في حال سبق أن خضعت المجموعة لجلسة "لنبدأ بتوثيق الحالات!"، ذكرنهن بأهمية المحافظة على مجموعة من الأدلة - فهي ضرورية للتمكن من تحديد أنماط الإساءة والتبليغ عن التحرش. في حال لم تخضع المجموعة بعد للجلسة المذكورة آنفاً، إشرحن لهن أنكن ستطلعن خلال هذا التمرين على طريقة لمتابعة حوادث التحرش.

الجزء الثالث - أنواع مختلفة من الأشخاص ودوافع مختلفة

٠٦. شاركن بعض قصص وتجارب ناشطات أو صحفيات مع التحرش على الإنترنت. حاولن إيجاد حالات ذات صلة ببيئة المشاركات وتظهر أنواع مختلفة من المتحرشين ودوافع مختلفة لأفعالهم.

٠٧. فقط في حال رغبت بعض النساء بمشاركة تجاربهن مع التحرش على الإنترنت، إسألنهن متى بدأ ذلك؟ من هو المتحرش وفق إعتقادهن؟ هل يعرفنه؟ هل يعتقدن أن أفعال المتحرش لها دافع محدد؟

٠٨. فكرن في دوافع المتحرشين بهن الممكنة - هل حدث هذا التحرش لأنهن نساء؟ لأنهن يدافعن عن حقوق النساء و/ أو الإنسان؟ هل شهدن ممارسة هذا النوع من التحرش ضد شركائهن أو زملائهن الرجال؟ في حال شهدن على ذلك، هل يحدث ذلك بالطريقة نفسها أم بطرق مختلفة؟

الجزء الرابع - توثيق الحوادث والتهديدات

٠٩. في حال سبق أن خضعت المشاركات لجلسة لنبدأ بتوثيق الحالات!، راجعن المستخرجات الرئيسية مع المشاركات مرّة أخرى. وإشرحن كيف أن ممارسة التوثيق جزء مهم من عملية جمع المعلومات حول المتحرشين لإتخاذ القرارات بشأن الإجراءات والخطوات اللاحقة. من بعدها يمكنك الانتقال إلى الجزء الخامس - التحضير

للعمل.

١٠. في حال لم تخضع المشاركات بعد لجلسة لنبدأ بتوثيق الحالات!، إبدأن أولاً بشرح النقاط التالية، التي تركز على أهمية ممارسة التوثيق في معالجة مشكلة التحرش على الإنترنت: ما هو التوثيق؟ التوثيق في هذا السياق يشير إلى مقارنة منظمة وممنهجة لمتابعة حالات الإساءة أو التحرش التي نشهدها في سياق عملنا - والهدف الأساسي منها هو أرشفة الأدلة.

ما هو الحادث؟ الحادث هو أي تطوّر يطرأ إما على الإنترنت أو في الواقع قد يشكّل إساءةً أو تحرشاً - تصنيف التطوّر على أنه حادث أم لا، يعتمد كثيراً على البيئة والظروف التي طرأ فيها وشدّة تأثيره بهذه العوامل. على سبيل المثال، في حال تلقيتن بريداً إلكترونياً يبدو وكأنه محاولة تصيد - وأنتن معتادت على تلقيها غالباً - قد لا يكون ذلك مهماً بما فيه الكفاية لإعتبره حادثاً؛ ولكن في حال كانت منظمتمكن تستعد لإطلاق حملة مهمة وبدأتن بتلقي أعداد كبيرة جداً غير معتادة منها، قد يشكّل ذلك حادثاً ولا بد من توثيقه. مثال آخر على ذلك، في حال كانت منظمتمكن تستعد لإطلاق حملة مهمة وبدأتن بتلقي عدد هائل من طلبات الصداقة على فايسبوك من غرباء.

ما هو سجل التوثيق؟ سجل التوثيق هو المكان الذي يمكنكن فيه الاحتفاظ بسجل بكل الحوادث التي تطرأ، بطريقة منظمة ستساعدكن على الاحتفاظ بمعلومات وأدلة مهمة عن كل حادث، يمكن استخدامها لاحقاً أو اعتمادها كمراجع.

ما الذي يجعل عملية التوثيق بهذه الأهمية؟ التوثيق مفيد كمرجع يستخدم لاحقاً حين تحاولن فهم الوضع بأكمله وربط حوادث مختلفة ببعضها البعض طرأت خلال إطار زمني محدد أو طالت عدداً من الأشخاص من المنظمة نفسها. قد يكشف التوثيق أنماط معينة من الإساءة أو الهجمات الأخرى على الإنترنت، ربما لم تكن لتلاحظنها لولاها، عبر تقديم مجموعة من الأدلة المترابطة. إكتشاف هذه الأنماط يساعدنا في تحديد هوية الخصوم أو في فهم مجريات الأمور والعلاقة بين أنواع معينة من الحوادث وأنواع معينة من الأعمال التي تقومن بها أنتن أو منظمتمكن. وعند التبليغ عن حوادث الإساءة على منصات التواصل الاجتماعي، على سبيل المثال، قد تُطلب أدلة كصور ملتقطة للشاشات أو أسماء الصفحات الشخصية خلال عملية

التحقيق.

١١. والآن، يمكننا تعريف المشاركات بسجل التوثيق - في هذا التمرين، يمكننا الإكتفاء بإستخدام النسخة المخصصة للإترنت، التي يفترض أننا حضرنا نسخ مطبوعة منها للمجموعة - راجع النموذج أدناه:

نموذج سجل التوثيق (على الإترنت)

ملاحظات	إجراءات المتابعة	مستوى الخطر	توصيف محتوى صورة الشاشة	صورة الشاشة (اسم الملف أو نسخ/الصق)	الرابط (URL)	المنصة	ملخص محريات الحادث	التوقيت	التاريخ

١٢. أذكرنا للمشاركات أن هذا النموذج يوفر مثلاً واحداً فقط عن أنواع المعلومات المهمة التي لا بد من جمعها في عملية جمع المعلومات حول المتحرشين. ولهن الحرية في إضافة أو إزالة أي خانة وفقاً لتقديرهن حين يقمن بوضع نماذج خاصة ببيئة عملهن في المستقبل.

١٣. معظم الخانات في هذين النموذجين واضحة الوظيفة؛ ولكن، سيتوجب عليكن مع ذلك شرح العملية لكل عضوة من عضوات المجموعة، عبر وصف موجز لكل واحدة منها (أي ما يجب أن تتابعه المشاركات للمء كل واحدة منها).

١٤. إحرصن على التركيز على خانة مستوى الخطر، فهذه الخانة ذاتية بإمتياز وأقل وضوحاً من الخانات الأخرى. وكيفية تعريف المشاركات و/أو المنظمات لمستويات الخطر مرتبط إلى حد كبير ببيئتهن الخاصة - من المفيد هنا التوقف عن الشرح والطلب من المشاركات تقديم أمثلة عن حوادث يصنفن خطرها كخطر ذو مستوى منخفض أو متوسط أو مرتفع (على سبيل المثال). شددن للمشاركات أنه سيتوجب عليهن التفكير في الأثر المحتمل للحادث (إما على المستوى الشخصي وإما على مستوى المنظمة، وإما الإثنين معاً) عند تعريف بالخطر في هذه البيئة.

١٥. أطلبين من المشاركات البدء بملء نماذج سجلهن بشكلٍ فرديٍّ - إمنحنهن من 10 إلى 15 دقائق لملء أكبر قدر ممكن من الخانات. يمكنهن ملء الخانات بمعلومات مفصلة عن الحوادث الفعلية التي تعرضن لها في حال رغبن في ذلك، ويمكنهن أيضاً استخدام أمثلة افتراضية للتدرّب على ملء النماذج.

الجزء الخامس - التحضير للعمل

١٦. قبل الإنتقال إلى الخطوات التالية من التمرين، يجب أن تنتبه المشاركات إلى عدم النقر على أي رابط يتلقينه أو يجدهه أثناء الإستقصاء عن المتحرّش - فقد تكون هذه محاولات تصيد (إشرحن ذلك للمشاركات في حال لم يكن يعرفن ما هو ذلك) تقوم بتثبيت برمجيات خبيثة على أجهزتهن. شددن على أهمية تفادي تقديم معلومات إضافية عن أنفسكن للمتحرشين؛ بالنسبة للمشاركات اللواتي يقمن بهذا التمرين ولسن معرضات حالياً للمتحرّش على الإنترنت، يفضل أن يتفادين لفت أي إتباه غير ضروري إلى أنفسهن قد يؤدي إلى تحرّش لاحقاً.

١٧. وجّهن المشاركات في الخطوات التالية لبدء عملية جمع المعلومات حول المتحرشين بهن بشكلٍ آمن:

- عليهن جمع أي معلومات متوفرة أصلاً بين أيديهن عن المتحرشين بهن (أو توثيق الحوادث السابقة التي يتذكرنها في سجّل التوثيق)؛
- بعد ذلك، عليهن إختيار المتصفّح الذي سيستخدمه في تحقيقهن - وعلى هذا المتصفّح، عليهن تسجيل خروجهن من كل حساباتهن، وحذف سجّل تصفّحن وملفات تعريف الإرتباط عليه. يمكنهن أيضاً التفكير في إستخدام متصفّح تور لهذا النشاط، في حال سبق لكن أن عرفتهن به؛
- يمكنهن أيضاً التفكير في إنشاء هويات إلكترونية أو صفحات شخصية جديدة لإجراء هذا النشاط (حسابات بأسماء مستعارة على فايسبوك أو تويتر، أو حساب جي مايل مزيف) - ذكرتهن بضرورة الإتباه إلى عدم استخدام أي معلومات في هذه الحسابات

- قد تستخدم لربطها بهوياتهن الحقيقية!
- شددن على أهمية تسجيل الملاحظات خلال هذه العملية - ذكرن المجموعة بما ناقشتنه عن تناولكن أهمية ممارسات التوثيق.
- أطلبن من المشاركات إنشاء ملف مخصص على حواسيبهن لجمع وتخزين المعلومات والأدلة التي يجمعنها - قد تشمل تلك على صور رمزية أو صور شاشات أو أسماء مستخدمين أو حسابات بريد إلكتروني أو حسابات على مواقع التواصل الإجتماعي أو تعليقات على منتديات أو أي ذكر لأماكن تواجدهم الممكنة أو جهات إتصال معروفة أخرى.

الجزء السابع - الأدوات المفيدة

١٨. والآن يمكننا البدء بمشاركة بعض الأمثلة عن الأدوات المفيدة للمشاركات خلال التحقيق الإستقصائي - إن أمكن، قدمن للمشاركات نسخة عن العرض المقدم من قبلكن والذي يحتوي على هذه المعلومات، أو مستند يرد فيه لأتحة بالأدوات والروابط التي يمكنهن الإطلاع عليها لاحقًا بأنفسهن.
١٩. إشرحن كل أداة منها وامنحن المشاركات بضع دقائق لإيجاد كل أداة على الإنترنت وإختبارها (بالإضافة إلى تلك المذكورة هنا، لا ضرر في إضافة أي أدوات أخرى تعرفنها وقد تكون مفيدة أو مهمة):

- البحث على غوغل، أو على داك داك غو^٤ Duck Duck Go;
- بحث متقدم على تويتر^٥ Advanced search on Twitter;
- الإطلاع على موقع Whois.net في حال تمكنن من إيجاد معلومات ناشئة عن موقع للتأكد من توفر أي معلومات عن الشخص المالك للبريد

^٤ <https://duckduckgo.com>

^٥ <https://twitter.com/search-advanced>

- Google reverse image search^٦: محرك البحث عن الصور من غوغل في حال تلقين صوراً أرسومات يمكنهن البحث من خلال الصور هذه
- أدوات خاصة بالبيانات الوصفية في حال تلقين صوراً أو رسومات، يمكنهن التحقق من توفر بيانات وصفية:

- ميتاشيلد^٧ MetaShield
- ميتا بيكس^٨ MetaPicz
- سوشل منشن^٩ Social Mention;
- فولور وونك^{١٠} Follower Wonk;
- نايم تشيك^{١١} NameCheck;

٢٠. إشرح أيضاً أنه من الممكن للمشاركات بناء أنظمة مراقبة مصغرة لتعقب المعلومات على الإنترنت: هذا مفيد جداً في تعقب صفحات شخصية أو أسماء مستخدمين أو هاشتاغات معينة:

- موقع آي إف تي تي^{١٢} IFTTT - بالنسبة لهذا الموقع، إشرح كيف أنه يسمح للمستخدمين بربط تويتر بغوغل درايف من أجل التمكن من تعقب التغريدات وحالات الذكر المرتبطة بإسم مستخدم أو هاشتاغ معين.
- خدمة التنبيه غوغل أليرتس^{١٣} Google Alerts خدمة تويدك^{١٤} Tweetdeck

٢١. وفقاً للوقت المتوفر لكن، يمكن للمشاركات إما إجراء تحقيقاتهن الآن أثناء ورشة العمل، أو يمكنهن القيام به "كفرض منزلي" يقدم في اليوم التالي من التدريب. في كلا الحالتين، ذكّن المجموعة أنه من المفيد، بعد الإنتهاء من جمع المعلومات، التوقف

<https://images.google.com/>^٦
<https://www.elevenpaths.com/technology/metashield/index.html>^٧
<http://metapicz.com/>^٨
<http://socialmention.com>^٩
<https://moz.com/followerwonk/>^{١٠}
<https://namechk.com>^{١١}
<https://ifttt.com>^{١٢}
<https://www.google.com/alerts>^{١٣}
<https://tweetdeck.twitter.com>^{١٤}

قليلاً ومن ثم الإطلاع على إجمالي المعلومات التي جمعناها:

- هل لاحظن أنماطاً معينة؟
- ماذا تخبرهن المعلومات المتوفرة لديهن بشأن هوية المحتملة للمتحرّش بهن؟
- هل يمكنهن الآن توقع الأهداف المحتملة أو أنواع الهجمات؟

المراجع

- <https://summit2015.globalvoices.org/2015/02/do-we-feed-the-trolls-learning-from-our-community/>
- <https://citizenevidence.org/category/how-to-2/tutorials/>



النساء فى فضاء الإنترنت



التحادث الجنسي

باب ٣٩

حان وقت المراقبة!

- الأهداف: تعرّف هذه الجلسة مفهوم "التحادث الجنسي" بإيجاز من المنظور الجندري مع التركيز على أنه يجب النظر إلى أن العنف يبقى عنفاً إن حدث على الإنترنت أو في الواقع.
- الطول: 15 دقيقة
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة: None -
- المواد اللازمة:
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
- مكبرات صوت (الفيديو)

إدارة التمرين

الدخول إلى الرابط https://www.youtube.com/watch?v=YxfWaD_8NRs واختيار فيديو الحالة رقم 1 - إعرضن هذا الفيديو على المشاركات. ما إن ينتهي الفيديو، ناقشن مع المشاركات ما شاهدته - ما رأيهن بالحالة؟ ما الذي يمكنهن القيام به؟

باب ٤٠

التحادث الجنسي

- الأهداف: هذه الجلسة تتابع النقاش عن التحادث الجنسي من منظور جندي الذي بدأ في الجلسة السابقة من هذه الوحدة (حان وقت المراقبة!)، وتُستند إليها للبدء بإقتراح ممارسات وأدوات والتوصية بها لتحادث أكثر أماناً.
- الطول: 40 دقيقة
- الشكل: جلسة
- مستوى المهارة: متوسط
- المعرفة المطلوبة:
- تعريف بمسألة التشفير (التشفير)
- ماذا يمكن لبياناتكن الوصفية أن تفصح عنكن؟ (المناصرة الآمنة على الإنترنت)
- حان وقت المراقبة! (التحادث الجنسي)
- عدم الكشف عن الهوية (عدم الكشف عن الهوية)
- جلسات/تمارين ذات صلة:
- حقوقكن والتكنولوجيا الخاصة بكن¹

¹<https://vrr.im/1151>

- ماذا يمكن لبياناتك الوصفية (Metadata) أن تفصح عنك؟^٢
- تعريف بمسألة التشفير^٣
- حان وقت المراقبة!^٤
- المواد اللازمة:
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
 - شرائح (فيها النقاط المفتاحية الواردة أدناه، وأمثلة عن الحملات المنظمة ضد التحادث الجنسي)
 - مكبرات صوت

إدارة الجلسة

الجزء الأول - وصف مشكلة إجتماعية -

١. إبدأن الجلسة بعرض بعض الأمثلة عن المقالات التي تناول حالات الإبتزاز الجنسي عبر الإنترنت في منطقتنا العربية.
٢. بعد عرضها، قسمن المشاركات إلى مجموعات صغيرة من ثلاثة إلى أربعة أشخاص لتحليل هذه المقالات. إمنحن المجموعة من خمس إلى عشر دقائق لمناقشة الأسئلة التالية:
 - لماذا يحدث هذا النوع من الإبتزاز؟
 - ما سبب غياب آليات محاسبة المبتزين؟

الجزء الثاني - ما هو التحادث الجنسي؟

٣. بعد الإنتهاء من النقاشات ضمن المجموعات الصغيرة، راجعن مع المشاركات ماهية التحادث الجنسي؛ وإحرصن في شرحكن على التشديد على النقاط التالية:

<https://vrr.im/1598٢>

<https://vrr.im/f5d4٣>

<https://vrr.im/27a7٤>

- إلتقاط الصور الشخصية (Selfies) وصور عريّ وإرسالها هو ممارسة لحرية شخصية.
- قد يكون التحادث الجنسي أيضاً فعل من أفعال المقاومة الممتعة ضد العنصرية والتمييز، على أساس الجنس وإستبداد الرجل والحفاظة والمعايير المفروضة على أساس تطبيع المغايرة الجنسية.
- في النهاية، إن كنتن تشاركن صوراً عنكن من هذا النوع أم لا، يجب أن يكون ذلك خياراً محصوراً بكن، ويجب أن يكون ممارسة واعية لحقكن في التعبير عن أنفسكن، وحقكن بالخصوصية في الوقت ذاته.

الجزء الثالث - تحادث جنسي أكثر أماناً؟

٤. في هذا الجزء من الجلسة، يمكنكن البدء بتقديم بعض التوصيات المحددة بشأن الممارسات التي يمكن للمشاركات تطبيقها لتحادث جنسي أكثر أماناً. يجب ألا ننسى أن وجهات النظر تختلف بشأن الهوية وعدم الكشف عنها حين يتعلق الأمر بالتحادث الجنسي: قد تشعر بعضهن براحة أكبر إذا كان التحادث الجنسي مع أشخاص لا يعرفونهن، والعكس صحيح أيضاً.

لا بد لكن هنا أن نتحضرن لكل الإحتمالات - قدمن النصائح أو التوصيات بشأن الأمان الرقمي، إستناداً إلى أولويات أو شكوك المشاركات وبواسطة بعض الإقتراحات التالية على سبيل المثال:

- إبقين آمانات - إحذفن صور العريّ أو الصور الذاتية التي ترسلنها إلى الآخرين من جهازكن مباشرة بعد إرسالها. وعند إرسال الصور، إعتمدن القنوات الأكثر أماناً (مثل تطبيق سيجنال - إطلعن على المزيد من التفاصيل أدناه في المرحلة الخامسة).
- حددن قواعد أو إتفاقات مع الشريك/ة في التحادث الجنسي بشأن عدم مشاركة صوركن (أو في حال كانت المشاركة مقبولة من قبلكن، حددن الأشخاص

وكيفية القيام بهذه المشاركة)، ما نوع التفاصيل التي قد تحتويه صوركن وكيفية تبادل الصور...إلخ.

- خصصن قناة أو تطبيق للتحدث الجنسي - مع أن الطلب من شريك/ة التحدث الجنسي تنزيل تطبيق جديد أو إتباع إجراء معين ليس الأمر الأكثر "إثارة" عند بدء مغامرة جديدة، ولكنه أفضل من إرسال صورة لكن عن طريق الخطأ عبر تطبيق الرسائل النصية القصيرة الإعتيادي إلى الشخص الخطأ!
- إلتقطن الصور بطريقة فنية - إبحثن عن الزوايا الأكثر أماناً وإثارة عند إلتقاط صوركن!

٥. في حال لم تقدمن جلسة ماذا يمكن لبياناتكن الوصفية أن تفصح عنكن؟ (أو في حال لم يتوفر لكن الوقت الكافي لذلك خلال التدريب) خصصن 15 دقيقة خلال هذه الجلسة لشرح ماهية البيانات الوصفية وشاركن بعض الأمثلة - يمكنكن الإستعانة بالأمثلة من تلك الجلسة.

إشرحن أن البيانات الوصفية في الصور غالباً ما توفر معلومات محددة لهوية المستخدم، وهذا أمر لا بد من التنبه له - لا سيما في حال إرسال الصور الذاتية العارية، ولا سيما إن كان الهدف هو عدم الكشف عن هويتكن:

لعدم الكشف عن هويتكن، تفادين إظهار أي عنصر (عناصر) في الصورة قد يحدد هويتكن، وهذه العناصر تشمل ما هو بدني (الوجه، اسم المستخدم) والتفاصيل الأدق (كالأوشام أو الأثاث أو الأمتعة الشخصية في الخلفية أو ثياب معينة)، وأخيراً الآثار الرقمية (البيانات الوصفية للصور، إشارات تحديد الموقع الجغرافي، المعلومات عن الجهاز).

٦. في النهاية، قد ترغبن في إختتام الجلسة بتقديم بعض التوصيات بشأن أدوات محددة قد تستخدمها المشاركات لتحدث جنسي أكثر أماناً مع شركائهن:

ObscuraCam أسكورا كام: هذا التطبيق المخصص للهواتف وهو من إنتاج مشروع غارديان Guardian Project يتيح للمستخدمين "تنظيف" (إزالة) تفاصيل بيانات وصفية محددة من صورهم.

Meet.jitsi منصة ميت.جيتسي: تقدم هذه المنصة المستندة إلى متصفح تشفيراً بتقنية إيدش تي تي بي إس HTTPS وتتيح للمستخدمين إمكانية إنشاء غرف تحادث مؤقتة تستخدم مرة واحدة للتحدث عبر الصوت والصورة.

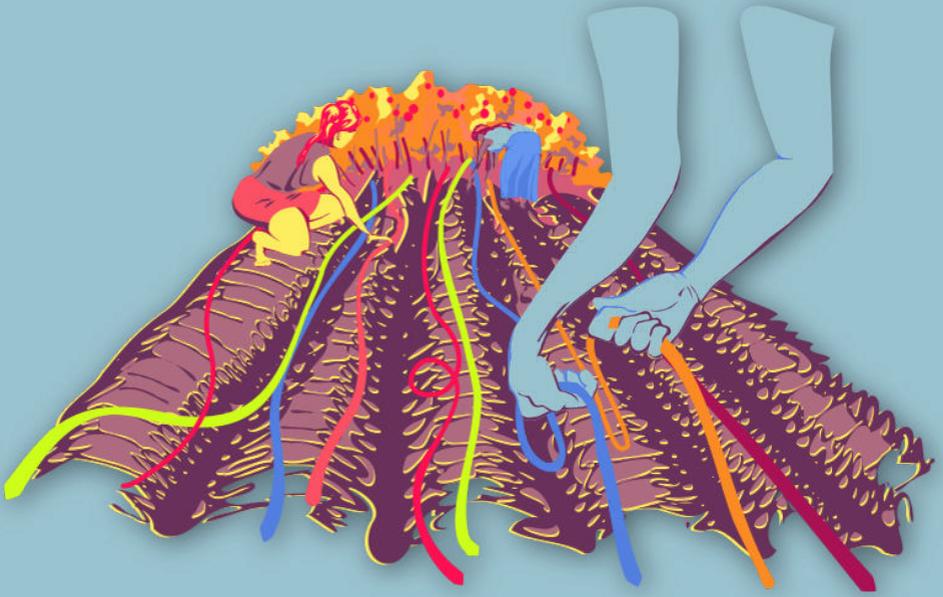
سيجنال أو تليغرام: هذان التطبيقان المخصصان للمراسلة عبر الهواتف يقدمان مستويات متفاوتة من الحماية المشفرة (للبيانات المنقولة بين المستخدمين) بالإضافة لخاصية التحقق من المستخدم؛ يتيح تطبيق سيجنال للمستخدمين تحديد "تاريخ إنهاء" للرسائل أو المحتويات الأخرى المرسلة (على سبيل المثال، يمكن ضبط التطبيق بحيث تختفي صورة مرسلة بعد خمس دقائق من مشاهدتها من قبل الملقى من على جهازه).

المراجع

- http://www.codingrights.org/wp-content/uploads/2015/11/zine_ingles_lado1.pdf
- http://www.codingrights.org/wp-content/uploads/2015/11/zine_ingles_lado2.pdf
- <http://seguridadigital.org/post/148199830243/sextea-con-seguridad-diagrama>
- http://lucysombra.org/TXT/Fanzine_necesito_privacidad.pdf
- <https://guardianproject.info/apps/obsuracam>
- <https://meet.jit.si>
- <https://signal.org>
- <https://telegram.org>
- <https://acoso.online>



النساء فى فضاء الإنترنت



تحديد الحل الأفضل

باب ٤١

نموذج المخاطر القائمة على النوع الإجتماعي

- الأهداف: في هذه الجلسة، ستوجهن المشاركات في عملية من مراحل عدة، أولها تحديد المخاطر المحدقة بهن، كنساء وكمدافعات عن حقوق الإنسان، وثانيها وضع إستراتيجية أمنية فردية للتعامل مع هذه المخاطر.
- الطول: من 40 إلى 5 دقيقة
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- متفاوتة (راجعن التوصيات أدناه)
- جلسات/تمارين ذات صلة:
- لنبدأ بتوثيق الحالات!^١
- الخطط والبروتوكولات الأمنية الخاصة بالمنظمة^٢

<https://vrr.im/899f1>

<https://vrr.im/f75c2>

• المواد اللازمة:

- أقلام خطاطة ملونة

- أقلام وأقلام رصاص

- ألواح ورقية أو لوح أبيض/أسود

• التوصيات: من الممكن تقديم هذه الجلسة بطرق مختلفة: قدم من الجلسة كاملة في بداية التدريب، ومن الجزء الثالث حتى النهاية بعد أن تقدّم أدوات وممارسات محددة أكثر في جلسات سابقة؛ (a) وجّه المشاركات في الجزئين الأول والثاني من هذه الجلسة عند بداية التدريب، ومن ثمّ قدّم من الجزء الثالث حتى النهاية بعد أن تقدّم أدوات وممارسات محددة أكثر في جلسات سابقة؛ (b) قسّم الجلسة إلى ثلاث جلسات صغيرة فردية ابتداءً من الجزء الأول عند بداية التدريب، والجزء الثاني في منتصفه بعد أن تُسنى للمشاركات فرصة مناقشة الأمن الرقمي في بيئاتهن الشخصية، والجزء الثالث عند النهاية بعد أن تقدّم أدوات وممارسات محددة أكثر في جلسات سابقة؛ (c) يمكن تنفيذ محتوى هذه الجلسة في البيئة الفردية الشخصية وضمن منظمة على حدٍ سواء، وهذا مفيد حين يقدم التدريب لأعضاء جماعة أو منظمة مدافعات عن حقوق الإنسان.

من الممكن تقديم هذه الجلسة بطرق مختلفة: قدم من الجلسة كاملة في بداية التدريب، ومن الجزء الثالث حتى النهاية بعد أن تقدّم أدوات وممارسات محددة أكثر في جلسات سابقة؛ (a) وجّه المشاركات في الجزئين الأول والثاني من هذه الجلسة عند بداية التدريب، ومن ثمّ قدّم من الجزء الثالث حتى النهاية بعد أن تقدّم أدوات وممارسات محددة أكثر في جلسات سابقة؛ (b) قسّم الجلسة إلى ثلاث جلسات صغيرة فردية ابتداءً من الجزء الأول عند بداية التدريب، والجزء الثاني في منتصفه بعد أن تُسنى للمشاركات فرصة مناقشة الأمن الرقمي في بيئاتهن الشخصية، والجزء الثالث عند النهاية بعد أن تقدّم أدوات وممارسات محددة أكثر في جلسات سابقة؛ (c) يمكن تنفيذ محتوى هذه الجلسة في البيئة الفردية الشخصية وضمن منظمة على حدٍ سواء، وهذا مفيد حين يقدم التدريب لأعضاء جماعة أو منظمة مدافعات عن حقوق الإنسان. تتضمن هذه الجلسة نقاش مفصّل عن المخاطر الشخصية من وجهة نظر بيئة مدافعات عن حقوق الإنسان - خاصة عند الوصول إلى الجزء الثالث (لا سيما إن كانت هذه الجلسة مقدمة دفعة واحدة وغير مقسّمة إلى أجزاء منفصلة)، قد تبدأ معالم القلق أو الإجهاد

بالظهور على المشاركات. لذا، يصبح من الضروري جداً لكن كدربات أن تقمن بإدارة مستوى الإجهاد في الغرفة. إحرصن على تذكير المجموعة بشكلٍ دوريٍّ أن هذه الجلسة ستركز في النهاية على تحديد الإستراتيجيات والأدوات والشبكات أو الحلفاء القادرين على مساعدتهن على مواجهة المخاطر، هدفكن هو عدم إخافتهن، حيث تتوفر نشاطات كثيرة يمكنهن إعتماها لمكافحة العنف على الإنترنت.

هذه الجلسة مُعدّة إستناداً إلى جلسة وضعتها جينيفر شولتي Jennifer Schulte في معسكر تدريب معهد صحافة الحرب والسلام المخصصة لموضوع الجندر في نيسان/أبريل 2016 في برلين، ألمانيا، بالتشاور مع "دليل إدارة مخاطر الكوارث للإعلاميين الاجتماعيين" (الأونسكو)

إدارة الجلسة

الجزء الأول - تحديد المخاطر والإحتمالات

١. إبدأن الجلسة بنقاش جماعي حول المخاطر المحددة التي تواجهها أو قد تواجهها المدافعات عن حقوق الإنسان - ذكرن المشاركات بالمعنى المقصود من كلمة "خطر": إحتمال حدوث أمرٍ ما قد يتسبب بضرر أو أذية. إكتبن بعض الأمثلة المحددة عن المخاطر التي قدمنها المشاركات - راجعنها بعد أن تحصلن على عددٍ مناسبٍ منها.

٢. وجهن النقاش نحو الطبيعة المتقلبة للمخاطر - إحتمالية حدوث الخطر تبدل وفقاً لعدد من العوامل الخارجية التي تزيد أو تخفض من إحتمالية حدوث الخطر حين تصبح هذه العوامل متوفرة أكثر أو أقل - على سبيل المثال:

يرتفع خطر إعتراض رسالة نصية من قبل الخصوم عند إستخدام تطبيق إرسال الرسائل النصية القصيرة الإعتيادي، ولكنه يخفض في حال أرسلت مشفرة عبر تطبيق كتطبيق سيجنال؛

وعلى نحو مماثل، في حال كان شخص ما ناشطاً مستهدفاً في دولته، خطر إعتراض رسالة

يرتفع بشكل ملحوظ في حال أُرسِلت بواسطة تطبيق الرسائل النصية القصيرة على هاتف متصل بشبكة اتصالات دولته، ولكن منسوب هذا الخطر ينخفض بشكل ملحوظ، في حال أُرسِلت بواسطة تطبيق كتطبيق سيجنال من على شبكة اتصالات في دولة أجنبية؛ ما يرد أعلاه مجرد مثال بسيط عن كيفية تأثير العوامل التقنية الخارجية على احتمالية حدوث خطر ما - ولكن ماذا عن الجندر كعنصر من عناصر الخطر؟ هل المخاطر المحدقة بالمدافعات عن حقوق الإنسان هي ذاتها تلك المحدقة بالمدافعين عن حقوق الإنسان الذين لا يعرفون عن أنفسهم كنساء؟

٣. إرسن جدولاً شبيهاً بالجدول الوارد أدناه على ورقة كبيرة من أوراق الألواح الورقية، وضعن عدداً من المخاطر الرقمية تحت خانة "الخطر الرقمي"، إستخدمن المخاطر المختلفة المناقشة والمشاركة في المرحلة الأولى كأمثلة (إحرصن على ترك الجانب الأيسر خالياً لإضافة أعمدة إضافية لأجزاء أخرى من هذه الجلسة):

الخطر الرقمي	إحتمالية الحدوث

٤. بعد الإنتهاء من اللائحة الواردة أعلاه، ستعملن الآن مع المشاركات على تحديد احتمالية حدوث كل خطر من المخاطر في الواقع - يسهل إجراء هذا التمرين في حال كانت كل المشاركات من الخلفية والبيئة ذاتها (الدولة، نوع النشاط...إلخ)؛ في حال تواجد مشاركات من خلفيات متعددة ومختلفة، قد ترغبن بتقديم شخص إقتراضي كمثال في هذه الجلسة.

٥. يمكنكن تحديد مقياس لقياس احتمالات حدوث هذه المخاطر. على سبيل المثال، يمكنكن إستخدام مقياس بسيط من 1 إلى 5، حيث الدرجة الخامسة تدل إلى أن احتمالية تحوّل الخطر إلى حقيقة "عالية جداً" وحيث الدرجة الأولى تدل إلى أن

إحتمالية تحوّل الخطر إلى حقيقة “منخفضة جداً”. ما الدرجة التي يمكن إعطاؤها لكل خطر؟ يمكن البدء بملء الجدول للمجموعة أثناء مناقشة كل خطر على حدة، وليدو كما يلي:

إحتمالية الحدوث	الخطر الرقمي
1=منخفضة جداً 5=مرتفعة جداً	
4	الفرق على رابط في بريد إلكتروني فيه برمجية خبيثة عن طريق الخطأ!
2	تعرض مكاتبنا للمداومة من قبل الشرطة لمصادرة أقراننا الصلبة أو أجهزة أخرى!

الجزء الثاني - تحديد مدى التأثير

٦. والآن وقد عملت مع المشاركات على تحديد أمثلة عن المخاطر ووضع نظام بسيط لتحديد إحتمالية حدوث كل خطر من المخاطر، إشرحن لمن أنكن ستتقلن الآن إلى المرحلة التالية، ألا وهي تحديد مدى التأثير الحقيقي لهذه المخاطر، أو ما هي نتائجها على الفرد والمنظمة والشبكة... إلخ، في حال صار خطر ما واقعاً.

٧. إشرحن أن آثار المخاطر، تماماً كالمخاطر نفسها، متقلبة هي الأخرى. تعتمد طبيعة التأثير وحدته أيضاً على عدد من العوامل الخارجية. هل ستطال تداعيات آثار المخاطر الفرد أم المنظمة؟ قد تطال الفرد والمنظمة على حدٍ سواء، وفي هذه الحال، ما مدى تشابه أو اختلاف هذين التأثيرين؟

٨. في الجزء التالي من هذه الجلسة، ستقمن بتحديد مقياس لقياس التأثير - قد يستخدم هذا المقياس كأداة قياس كميّ مشابه للذي أستخدم لقياس إحتمالية الحدوث، أو قد يستخدم كأداة قياس نوعي يصف طبيعة وتفاصيل التأثير بدقة. الخيار يعود لكن أنتن والمشاركات - المهم في كل ذلك هو أن تشدد هذه الجلسة على مخاطر وتداعيات محددة بحيث يصبح من السهل على المشاركات فهمها على أنها ليست مجرد مفاهيم نظرية

(لأغراض هذه الجلسة، سنستعين بمقياس كمي).

٥٩. إشرحن للمجموعة أن إستباق رد فعلكن الممكن مع آثار المخاطر جزء مهم من فهم المخاطر وقياسها - إسألن المشاركات عن تفاعلن المحتمل على الصعيد الشخصي تجاه خطر معين؟ ومن ثم ناقشن كيف - تماماً كالأحتمالية والتأثير - ستضعن مقياساً لقياس رد الفعل الذي قد يكون هو الآخر كميّاً أو نوعياً (ولكن لأغراض هذه الجلسة سنستعين بمقياس كمي).

إستناداً إلى ما بدأتن بشرحه في المرحلة الخامسة، سيثبه جدولكن الآن الجدول المبين أدناه كمثال:

رد الفعل	الأثر	إحتمالية الحدوث	الخطر الرقمي
1 - هائل، تحت السيطرة 5 - حالة ذعر وتوتر شديد	1- خطورة منخفضة 5- خطورة مرتفعة	1- منخفضة جداً 5- مرتفعة جداً	النظر على رابط في بريد إلكتروني فيه برمجية خبيثة عن طريق الخطأ!
3	3	4	
5	5	2	تعرض مكتبنا للعداوة من قبل الشرطة لمصادرة أرقامنا الصلبة لأجهزة أخرى!

الجزء الثالث - وضع إستراتيجيات للحلول

١٠. كما سبق وذكرنا في التوصيات، تتضمن هذه الجلسة نقاشاً مفصلاً عن المخاطر الشخصية من منظور بيئة المدافعات عن حقوق الإنسان - قد تبدأ معالم القلق أو الإجهاد بالظهور على المشاركات الآن. إحرصن على تذكير المجموعة بشكلٍ دوريّ أن هذه الجلسة ستركّز في النهاية على تحديد الإستراتيجيات والأدوات والشبكات أو الحلفاء القادرين على مساعدتهن على مواجهة المخاطر؛ هدفكن هو عدم إحاقتهن، حيث تتوفر نشاطات كثيرة يمكنهن إعتمادها لمكافحة العنف على الإنترنت.

١١. والآن وقد قمتن بتحديد وقياس إحتمالية وأثر ورد الفعل الخاصة بكل خطر من المخاطر، إشرحن أن هذا الجزء من الجلسة مخصص للتفكير في الحلول. لكل خطر من المخاطر، إسألن المشاركات: ماذا يمكن أن تفعلن لمعالجة خطر ما و/أو منعه حدوثه؟ الإجابات

المعطاء من قبل المجموعة ستختلف وتبدّل وفقاً للمرحلة التي ستقدم فيها هذه الجلسة خلال عملية التدريب - في حال قدمتم هذه الجلسة في بداية التدريب، قد لا تتوفر لديهن إجابات مفصّلة جداً، ولكن إن قدمتم هذه الجلسة عند نهاية التدريب عندها ستصبح إجاباتهن أكثر إرتباطاً بشأن بعض الأدوات والممارسات.

١٢. إستكمالاً للجدول الذي بدأتم بنائه خلال هذه الجلسة، قمن بإضافة عمود أخير هو عمود “ماذا يمكنني أن أفعل؟” - وفي هذا العمود، أكتبن الإجابات المقدمة من قبل المجموعة خلال المرحلة الحادية عشرة. وبعد الإنتهاء من ذلك، إعرضن الجدول في مكان ظاهر في غرفة التدريب طيلة الفترة المتبقية من ورشة العمل لكي تتمكن المشاركات من إعادة قراءة وتحليل إجاباتهن. قد يساعد ذلك المشاركات في معرفة ما يجب إضافته إلى الجدول إن اقتضى الأمر ذلك، مما يشكّل قاعدة متينة لتصميم بروتوكول أمن رقمي. يرد أدناه نموذج عن الجدول النهائي المثالي:

الخطر الرقمي	إحتماله الحدوث	الأثر	رد الفعل	ماذا يمكنني أن أفعل؟
	1- منخفضة جداً 5- مرتفعة جداً	1- خطيرة منخفضة 5- خطيرة مرتفعة	1 - هائل، تحت السيطرة 5- حالة ذعر وتوتر شديد	
الشر على رابط في بريد إلكتروني فيه برجيّة خيئة عن طريق الخطأ!	3	4	3	تزيلي برجيّة مكافحة فيروسات وتبيها؛ تنبيه الآخرين في شبكتي لمنظمتي في حال ظهر لديهم الرابط ذاته
تعرض مكاتبنا للهداهة من قبل الشرطة لصانرة أفراسا الضالّة أو أجرة أخرى!	4	5	5	القيام بنسخ احتياطية عن بياناتنا بشكل دوري، ونحفظها في مكان آمن خارج مكاتبنا، وتنبيه الآخرين في شبكتنا إذا ما تعرضت معلومات خاصة بهم للكشف

الجزء الثالث - وضع إستراتيجيات للحلول

المراجع

• <https://ssd.eff.org/en/module/assessing-your-risks>

باب ٤٢

القرارات المرتبطة بالأمن الرقمي

- الأهداف: الهدف من هذه الجلسة هو تعريف النساء بعملية التفكير الإستراتيجي النقدي المستخدمة في صنع القرارات الواعية بشأن تنفيذ وتطبيق ممارسات وأدوات الأمن الرقمي، وتحديد الموارد التي ستساعدهن في متابعة المستجدات بعد هذا التدريب.
- الطول: 90 دقيقة
- الشكل: جلسة
- مستوى المهارة: متوسط
- المعرفة المطلوبة:
- معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
- جلسات/تمارين ذات صلة:
- وجهات النظر الشخصية حيال الأمن^١
- كيف يعمل الإنترنت؟^٢
- التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟^٣

<https://vrr.im/9339^١>

<https://vrr.im/7ba9^٢>

<https://vrr.im/47ba^٣>

- المواد اللازمة:
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
 - شرائح بالنقاط المفتوحة الواردة أدناه
 - نسخ عن الرسوم البيانية الخاصة بحالات المدافعات عن حقوق الإنسان (راجع الملاحق)
- التوصيات: بما أن هذه الجلسة تستوجب حد أدنى من المعرفة الأساسية بمفاهيم الأمن الرقمي، يفضل تقديمها في تدريب على عدة أيام أو كجزء من ورشة عمل قصيرة المدّة، تركز أكثر على تصميم البروتوكولات الأمنية الفردية.

إدارة الجلسة

الجزء الأوّل - المقدمة

٠١. إبّان بسؤال المشاركات عن عدد المرات التي طرحن فيها على مدربة أو خبيرة أخرى سؤالاً عن الأمن الرقمي، فتلقين إجابات مختلفة في كل مرة بحسب الشخص الذي طرح عليه السؤال - هذا أمرٌ محيرٌ، أليس كذلك؟ أحياناً حين نطلب نصائح عن الأمن الرقمي، قد لا يشرح الأشخاص الذين يقدمون لنا المساعدة سير العملية، بل يكتفون "بحلّ المشكلة" على أجهزتنا من دون أن يشرحوا ما قاموا به - ألا تفضلن معرفة ماهية الحلّ المناسب لكي تتمكنن من تطبيقه مرة أخرى في حال واجهتن المشكلة مرّة أخرى؟
٠٢. إشرحن لمن أن الهدف من هذه الجلسة هو تعريف المجموعة بعملية التفكير النقدي الإستراتيجي المستخدمة في صنع القرارات الواعية بشأن تطبيق وتنفيذ ممارسات وأدوات الأمن الرقمي، وتحديد الموارد التي من شأنها مساعدتهن على متابعة المستجدات بعد التدريب. ناقشن فكرة أن الأمن الرقمي ليس محصوراً فقط بتزليل تطبيقات جديدة، بل تشمل أيضاً معرفة ممارساتك جيداً وإتخاذ قرارات واعية لبناء بيئة أكثر أماناً لكن.

الجزء الثاني - كيف تم بناء البرمجيات التي تستخدمها؟

٣. إعرضن أو إشرحن مرّة أخرى للمشاركات بعض الأدوات أو المنصات التي سبق لكن أن قمتن بتقديمها للمشاركات (مثلاً: سيجنال، برمجية إيتش تي تي بي إس إفريوير، أسكوراكام، سكايب، تليغرام، إنلخ) - أطلبن منهن تحديد نوع كل برمجية منها إستناداً إلى المعلومات المتاحة لهن، من قبيل الموقع الإلكتروني الخاصة بالأداة.

٤. إشرحن ما هي البرمجيات التجارية (المغلقة المصدر): ما هي خصائص هذا النوع من البرمجيات (قدمن أمثلة عن برامج). ما هي تداعيات استخدام هذا النوع من البرمجيات على الأمن الرقمي؟

٥. إشرحن ما هي البرمجيات المفتوحة المصدر: ما هي خصائص هذا النوع من البرمجيات (قدمن أمثلة عن برامج). ما هي تداعيات استخدام هذا النوع من البرمجيات على الأمن الرقمي؟ إحرصن أيضاً على توضيح ما هو مجتمع البرمجيات المفتوحة المصدر والتدقيق في البرمجيات لمزيد من التوضيح.

٦. إشرحن عن مشاريع البرمجيات الحرة والمفتوحة المصدر (Free/Libre and Open Source Software FLOSS): ما هي خصائص هذا النوع من البرمجيات (قدمن أمثلة عن برامج). ما هي تداعيات استخدام هذا النوع من البرمجيات على الأمن الرقمي؟

الجزء الثالث - التفكير في المستخدمين؟

٧. في حال سبق لكن أن قدمتن جلسة بمن ثقتن؟ من وحدة "إعادة النظر بعلاقتنا بالتكنولوجيا"، ذكرن المجموعة بالأمثلة عن الخصوم التي قدمنها؛ وفي حال قدمتن تمرين نموذج المخاطر القائمة على النوع الاجتماعي، ذكرن المجموعة بنموذج المخاطر الذي أنشأته معاً.

الهدف من كل ذلك في النهاية تعزيز فكرة أن لكل شخص فينا حاجات خاصة به أو أن الجميع لا يواجهون المخاطر ذاتها من حيث الأمن الرقمي:

- عند البحث عن حلّ في مجال الأمن الرقمي، عليكن تعلّم أكبر كمية من المعلومات عن الحاجة التي تمّ تحديدها. ماذا تردن فعله أو جعله أكثر أماناً؟ ما هو المكان الأكثر أماناً الذي يمكنكن الإحتفاظ فيه بأمرٍ ما؟ ممن نحن بحاجة للحماية؟
- فكرن في المنصات أو الأدوات المستخدمة من قبلكن حالياً - إلى أي مدى أو هل من الممكن أن توافقن على إستبدالها بمنصات أو أدوات جديدة أو تغيير طريقة استخدامكن لمنصاتكن أو أدواتكن الحالية؟
- إلى أي مدى تؤثر القدرة على الاتصال على أي حلّ ممكن في مجال الأمن الرقمي؟ هل تتوفر لكن عادةً إمكانية اتصال ثابتة وموثوق بها بالإنترنت، أو هل تحتجن إلى العمل من دونها لفترات طويلة؟
- في حال كنتن تفكرن في حلّ في مجال الأمن الرقمي ضمن بيئة منظمة أو جماعة، فكرن في الأجهزة أو أنظمة التشغيل المختلفة المستخدمة من قبل أعضاء تلك المجموعة - هل سينجح الحلّ لدى الجميع؟ هل سينجح الحلّ لدى أغلبية الأعضاء؟

الجزء الرابع - التفكير في الأدوات

٨. الأسئلة التالية هي أسئلة لا بد من طرحها عند التفكير في إستخدام منصة أو أداة جديدة - إشرحن ذلك للمشاركات. لا حاجة لشرحها والإجابة عنها كلها (فهي أسئلة محددة جداً)، ولكن إحرصن على قراءتها بصوتٍ عالٍ وإشرحن بإيجاز سبب أهمية كل واحد منها:
 - هل البرمجية مجانية ومفتوحة المصدر؟
 - هل تعرفن من برمج الأداة، أو من مؤل المشروع؟
 - هل هي متوفرة بلغتكن؟
- إبحثن عن منشورات مدونات أو أي موقع يأتي على ذكر الأداة على الإنترنت، ماذا وجدتن؟ متى أدخل التحديث الأخير على الأداة؟ هل النسخة المتوفرة نسخة ثابتة من

الأداة؟ هل توفر جهة ما الدعم التقني للأداة أم هي مدعومة من متطوعين/ات؟ ما مدى سهولة إعدادها؟ هل خضعت الأداة للاختبار أو التدقيق؟ هل الأداة متوفرة لنظام التشغيل الذي تستخدمه على أجهزتك؟ تحقق من شروط الخدمة الخاصة بالأداة - هل توافقن عليها أم تبدو لكن مرئية؟ في حال كانت الأداة أو المنصة تستعين بخوادم عن بعد، هل تعرفن أين تتواجد هذه الخوادم؟ هل قام مطورها في يوم من الأيام بتسليم بيانات أي مستخدم إستجابة لطلب حكومة ما؟ كيف تُخزن المعلومات على خوادمها؟ هل هي مشفرة، وإن كان الأمر كذلك هل يمتلك المشروع طريقة لفك التشفير والوصول إليها؟ في حال ساورتك أي شكوك، إبحثن عن طريقة للتواصل مباشرة مع المطورين والتحدث معهم.

٩. ذكّن المجموعة مرّة أخرى أن لا وجود لحلول أو توصيات في مجال الأمن الرقمي قابلة للتطبيق في كل مكان ولجميع الناس- فليست كل الأدوات مناسبة لكل المستخدمين. التعامل بطريقة إستراتيجية مع الأدوات والممارسات الخاصة بالأمن الرقمي مرتبط إلى حد كبير بمعرفتنا لأنفسنا كمستخدمين، وإختيار الأدوات المناسبة لكل واحدة منّا إستناداً إلى معرفتنا لظروفنا الخاصة.

١٠. وضّح للمجموعة أن عدداً كبيراً من برمجيات الأمن الرقمي تتضمن تشفيراً بدرجات متفاوتة - فسّرّن للمشاركات أنه في حال كان التشفير خاصية مهمة بالنسبة لهن، يوصى إذاً بإستخدام البرمجيات المفتوحة المصدر. فالبرمجيات المفتوحة المصدر قابلة للتدقيق من قبل المجتمع من أجل ضمان عدم وجود أي أبواب خلفية، في حال لا تشمل أداة برمجية ما خاصية التشفير، ولم يكن التشفير عاملاً مهماً في عملية صنع القرار، قد يكون إستخدام البرمجيات المفتوحة المصدر أقل أهمية (مع أنه أبخس ثمناً حتماً).

١١. أكبّن هذا الجزء من الجلسة عبر تقسيم المشاركات إلى مجموعات من 3 إلى 4 أشخاص كحد أقصى - وضّحن مجموعاتهم الصغيرة، أطلبن منهن وضع لأئحة ببعض أدوات الأمن الرقمي التي يعرفنها، والإجابة عن الأسئلة الواردة أعلاه عن كل أداة. أثناء قيامهن بذلك، يتوجب على كل مجموعة مناقشة الإيجابيات والسلبيات التي يجدها في كل أداة

من الأدوات على لائحتهن - إمنحن المشاركات من 10 إلى 15 دقائق من الوقت لإتمام هذه المرحلة، وعلى كل مجموعة تقديم نتائج عملها عند إنهاء الوقت.

الجزء الخامس - التدريب على التفكير في الحلول

١٢. قدمن للمشاركات مجموعة من الرسوم البيانية عن حالات مدافعات عن حقوق الإنسان (راجعن الملاحق) وأطبلن منهن البقاء ضمن مجموعاتهم من المرحلة السابقة - إحرصن على توفر حالات كافية لتزويد كل مجموعة بواحدة منها. لا تقدمن مكوّن الحل للمجموعات - خلال هذه المرحلة، يتوجب على المشاركات العمل معاً للتوصل إلى حلولهن الخاصة إستناداً إلى المعلومات المقدمة لهن خلال هذه الجلسة وما قد يعرفنه مسبقاً عن أدوات الأمن الرقمي.

الجزء السادس - الموارد اللازمة للتمكن من متابعة المستجدات

١٣. لا بد للمشاركات في تدريبيكن أن تتوفر لديهن إمكانية الوصول إلى المزيد من الموارد بعد إنهاء التدريب، التي يمكنهن العودة إليها للمحافظة على تدريبيهن والتمكن من متابعة المستجدات بشأن الأدوات أو الممارسات الجديدة التي تنتج عن مجتمع الأمن الرقمي. إلكن بعض الموارد المقترحة التي يمكن تقديمها للمشاركات:

- الهدوء وفن جعل التكنولوجيا تعمل لصالحك // Tactical Technology Collective (تاكتيكل تكنولوجي)^٤
- موقع "سيكيوريتي إن آي بوكس Security in a Box (فرونتاين ديفنדרز Frontline Defenders وجماعة تاكتيكل تكنولوجي)^٥
- مشروع "سورفايلنس سلف ديفينس" Surveillance Self-Defense (مؤسسة إلكترونيك فرونتير)^٦

^٤ https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual

^٥ <https://securityinabox.org>

^٦ <https://ssd.eff.org/en/module/choosing-your-tools>

اختباري: يمكن أيضاً وضع لائحة بمنظمات مختلفة تستطيع المشاركات متابعتها (على الإنترنت عموماً وعلى تويتر، إنخ) للوصول إلى المزيد من المعلومات عن الأمن الرقمي في بلدانهم.

باب ٤٣

أنا صاحبة القرار

- الأهداف: الهدف من هذه الجلسة هو توجيه المشاركات في عملية التفكير النقدي الإستراتيجية لإتخاذ القرارات بشأن أدوات أو ممارسات محددة في مجال الأمن الرقمي
- سيتمن بتطبيقها لأنفسهن.
- الطول: 15 دقيقة
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- ممارسة التطبيقية بواسطة أدوات وممارسات الأمن الرقمي من التدريب السابق
- القرارات المرتبطة بالأمن الرقمي (تحديد الحلّ الأفضل)
- جلسات/تمارين ذات صلة:
- وجهات النظر الشخصية حيال الأمن^١
- كيف يعمل الإنترنت؟^٢

^١<https://vrr.im/93391>

^٢<https://vrr.im/7ba92>

- التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟^٣
- القرارات المرتبطة بالأمن الرقمي^٤
- المواد اللازمة:
 - رسومات عن أدوات السلامة الرقمية (يفضل أن تتوفر نسختين أو ثلاث من كل واحدة منها، ولكن ليس ما يكفي لكل مشاركة من المشاركات)
 - التوصيات: كدربات، غالباً ما نفرض منظورنا الخاص عن ممارسة الأمن الرقمي على المشاركات، إما عن قصد إنطلاقاً من نوايا حسنة، وإما عن غير قصد. ولكن، لا بد لنا أن نتذكر - بصفتنا مدربات وخبيرات - أن المشاركات غير مجبرات على استخدام الأدوات التي نعلمهن عنها، أو التكيف مع الممارسات التي نعتبرها "الأكثر أماناً".

إدارة التمرين

١. إفتتح الجلسة بشرح كيف أن بناء ممارسة في مجال الأمن الرقمي عبارة عن عملية متكررة وغالباً ما تكون صعبة على أي شخصٍ كان. تستند هذه الجلسة على العمل الذي بدأتته خلال جلسة القرارات المرتبطة بالأمن الرقمي من هذه الوحدة التي بدأت المشاركات خلالها تحديد الأدوات الممارسات الخاصة بهن.
٢. ضع الرسومات الخاصة بأدوات السلامة الرقمية (ستبحثن أنتن عن الرسوم) على طاولة أو أي سطح مسطح آخر - يجب أن يكون ذلك في وسط غرفة التدريب، أو أي مكان مركزي وظاهر لكل المشاركات
٣. أخبرن المشاركات أنهن على الأرجح سيلاحظن أنهن تعرفن على عدد من الأدوات المعروضة على الطاولة قبل هذه الجلسة - من قبيل مفاتيح بي جي بي PGP أو تطبيق سيجنال أو أويسكورا كام أو إيتش تي بي إس إيفريوير. ذكرن المجموعة أنه كما سبق أن ذكرتن في مراحل سابقة من التدريب، هنّ من سيتوجب عليهن إختيار الأدوات

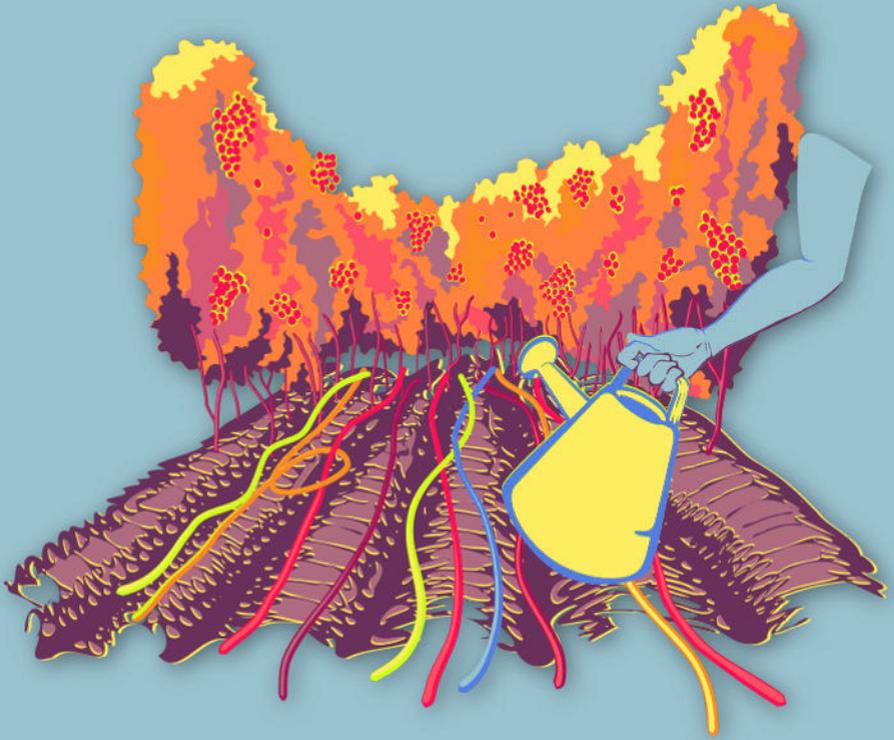
^٣<https://vrr.im/47ba>

^٤<https://vrr.im/043a>

-
- المناسبة لمن ولحاجاتهم وليس أنتن كمدربات أو متخصصات تقنياً أو أي شخص آخر.
٤. أطلبين من المشاركات التقدم نحو الطاولة واختيار من بين رسومات الأدوات الموجودة هناك، تلك التي يعتبرنها مهمة لمن ولحاجاتهم الفردية، وتلك التي سيستمرن في التدرّب على استخدامها والإستمرار في إستخدامها بعد إنتهاء التدريب بأكله.
٥. بعد أن تختار كل المشاركات أدواتهن، أطلبين من كل واحدة منهن شرح سبب إختيارهن للأدوات التي إخترنها - عليهن الوقوف أو الجلوس في حلقة حول الطاولة، ومن ثمّ، يعرضن واحدة تلو الأخرى خياراتهن وأسبابها إلى أن تقمن جميعاً بذلك. لا بد لمن أيضاً من ذكر إن وجدن أي أداة أردن إختيارها ولكن إخترنها الأخرى قبلهن.
٦. والآن، إسألنهن إن كنّ يعتقدن أن بعض الأدوات الأخرى غير متوفرة على الطاولة - حتى إذا كن لا يعرفن اسمها (أو حتى لا يعرفن إن كانت موجودة أم لا) أطلبين منهن التعبير عن أي مخاوف ما زالت تساورهن إذ لا تعالجها كما يجب أي أداة من الأدوات التي توفرت لديهن.
٧. إختتمن الجلسة بالتفكير جماعياً حول كيفية مشاركة المعرفة، وأنه على اللواتي إخترن أداة أردنها مشاركات أخريات أيضاً (ولكن لم يستطعن لعدم توفر ما يكفي منها) مشاركتها وتبادلها لكي نتكن جميعاً من "التعلّم" من بعضنا البعض.



النساء في فضاء الإنترنت



التخطيط المسبق

باب ٤٤

الخطط والبروتوكولات الأمنية الخاصة بالمنظمة

- الأهداف: في هذه الجلسة، ستقمن بتسيير عملية سنتفدها المشاركات لوضع خطة أمنية والبروتوكولات المرتبطة بها التي يمكنهن إستخدامها لتطبيق إجراءات الأمن الرقمي في منظماتهن.
- الطول: 90 دقيقة
- الشكل: جلسة
- مستوى المهارة: متوسط
- المعرفة المطلوبة:
- بمن تثقن؟ (تمارين بناء الثقة)
- الممارسة التطبيقية بواسطة أدوات وممارسات الأمن الرقمي من التدريب السابق
- نموذج المخاطر القائمة على النوع الاجتماعي (تحديد الحلّ الأفضل)
- جلسات/تمارين ذات صلة:
- بمن تثقن؟^١

<https://vrr.im/bd0d1>

- وجهات النظر الشخصية حيال الأمن^٢
 - كيف يعمل الإنترنت^٣؟
 - نموذج المخاطر القائمة على النوع الاجتماعي^٤
 - الخطط والبروتوكولات الأمنية الخاصة بالمنظمة^٥
- المواد اللازمة:
- نموذج المخاطر من تمرين نموذج المخاطر القائمة على النوع الاجتماعي
 - نماذج مطبوعة لبروتوكولات أمنية (راجعن مثال النموذج أدناه)
- التوصيات: هذه الجلسة مناسبة للمشاركات القادמות من المنظمة أو الجماعة ذاتها، بما أن النشاطات الواردة أدناه تركز على وضع خطة أمنية على مستوى المنظمة - وعملية تصميم كل هذا سيساعدنا في تعزيز ممارستها وتنفيذها بشكل مستمر من قبل النساء المشاركات. لا بد من متابعة عملية تنفيذ الخطة التي وضعتها المشاركات - وإن أمكن ذلك، تواصلن معهن كل أسبوعين أو ثلاث للتحقق من التقدم المحقق (إلى جانب الإجابة على الأسئلة التي قد يطرحنها أثناء هذه العملية). إحرصن على عدم ممارسة الضغط على المشاركات بشأن استخدام أدوات معينة أو طريقة تنفيذها أثناء القيام بالمتابعة - إكتفين بكل بساطة بتقديم الدعم لهن والتواجد معهن والإجابة على الأسئلة أو المخاوف التي تساورهن وتقديم التوصيات عند الحاجة لذلك. في حال شعرت المشاركات بضغطٍ يمارس عليهن، قد لا يتشجعن للحصول على مشورتكن بشأن مشكلة ما عاجلها، ولن يرتحن لمشاركة بعض الصعوبات الفعلية عند نشوئها.

<https://vrr.im/9339٢>

<https://vrr.im/7ba9٣>

<https://vrr.im/c0c3٤>

<https://vrr.im/f75c٥>

إدارة الجلسة

الجزء الأول - عودة إلى نموذج المخاطر

٠١. إبدأن الجلسة بالتشديد على أهمية بناء نموذج مخاطر قبل وضع مسودة خطة وبروتوكولات. ذكرن المشاركات أن الأمن الرقمي هو عملية شخصية قبل أي شيء آخر - وفي حال كان هدفهن وضع مسودة خطة أمن رقمي وتنفيذها على مستوى المنظمة، إشرحن لهن أن هذه العملية ستضمن:

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

الجزء الثاني - انخطط في مواجهة البروتوكولات

٠٢. إشرحن للمشاركات الفرق بين خطة أمن رقمي وبروتوكول أمن رقمي. الفكرة الرئيسية التي يجب إيصالها هي أن:

- الخطة إطار عام للتغييرات الرئيسية التي يجب أن تحددها المنظمة أو الجماعة

كعناصر أساسية لرفع مستوى الأمن الرقمي الخاص بها. الخطط هي عملية واضحة المعالم، لها بداية ولها نهاية.

• البروتوكول عبارة عن مجموعة إجراءات أو تدابير مرتبطة بالأمن الرقمي وكل واحدة منها مرتبطة بنشاط أو عملية معينة ضمن المنظمة أو الجماعة. البروتوكولات فعلياً عبارة عن ممارسات دائماً تبقى فاعلة عندما يكتمل تطبيق خطة أمن رقمي معينة، وتتطور مع الوقت إستجابةً للتغيرات في بيئات المخاطر والتحديات.

قد من أمثلة عن الخطط والبروتوكولات للمشاركات - على سبيل المثال، الأنشطة كالمسرح أو المشاركة في مظاهرات عامة يخصص لكل نشاط منها بروتوكول أمن رقمي خاص؛ البنود الواردة في خطة أمن رقمي قد تتضمن خضوع الموقع الإلكتروني الخاص بالمنظمة للتدقيق، والتحقق من توفر برنامج مكافحة الفيروسات مثبت على كل حاسوب، وإدخال إستعمال خاصية جي بي جي GPG لتشفير رسائل البريد الإلكتروني.

الجزء الثالث - وضع خطة وبروتوكولات على مستوى المنظمة

٣. هذه الجلسة مناسبة لمجموعات المشاركات الآتيات من المنظمة أو الجماعة ذاتها، إذ قد يستطعن إغتنام الفرصة للتعاون على وضع خطتهن وبروتوكولاتهن الخاصة بشكلٍ جماعي. ولكن، إن لم يكن الوضع كذلك إلا للجزء من المشاركات، يمكن عندها للواتي لا ينتمين لأي منظمة أو مجموعة العمل على وضع خطتهن وبروتوكولاتهن الشخصية.

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

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

٥. ذكرن المشاركات أنه على الرغم من التركيز في هذا التدريب على الأمن الرقمي، علينا التذكر دائماً أن نأخذ الإجراءات الشاملة بعين الاعتبار. أطلبين من المشاركات التفكير في الإجراءات التي يجب إتخاذها من أجل أمنهن الجسدي ورعايتهن الذاتية عند وضع مسودة خططهن وبروتوكولاتهن الأمنية.

٦. بعد ذلك، بعد أن ينتهين من وضع مسودتهن الأولى لجدول الخطة، أطلبين من المشاركات وضع لائحة بأنشطة أو إجراءات منظمتهن التي ستحتاج برأيهن لبروتوكولات خاصة بها.

٧. بعد إن تنتهي المشاركات من وضع مسودة جدول الخطة ولائحة أنشطتهن التي تحتاج لبروتوكولات أمنية، يفضل تخصيص بعض الوقت لكي يتمكن الجميع من مشاركة خططهن. يعد ذلك فرصة قيمة للمشاركات ليتعلمن من مقاربات الأخريات؛ ولكن، لا تنسين أن بعضهن قد لا تشعرن بالإرتياح لمشاركة نقاط ضعف منظمتهن أو شخصهن لعدم وثوقهن بهن. لمعالجة هذه المشكلة بشكلٍ فعّال، قد يتوجب عليكن الطلب من المجموعة مشاركة العناصر الرئيسية فقط من خطتهن (العمود الرابع من الجدول "إجراءات التخفيف") والإحتفاظ بالمعلومات الأخرى أي "التهديدات والمخاطر" و"نقاط الضعف المحددة" لأنفسهن.

الجزء الرابع - ما هي الخطوات التالية؟

٠٨ ناقش خطوات المتابعة مع المشاركات - سيحتج تنظيم إجتماع خاص ضمن منظمتهن لتشارك المعلومات الأساسية والخلصات الرئيسية من هذه الجلسة، بالإضافة إلى تمرين نموذج المخاطر القائمة على النوع الإجتماعي وتمرين بمن نثقن؟ - والأهم في هذه الجلسة هي اللائحة بالأنشطة والإجراءات التي تحتاج لبروتوكولات أمنية خاصة بها. يجب مناقشة هذه الخطة والتوافق عليها كفريق، وتحديد فترات زمنية معقولة لتنفيذها - وخلال التفكير ذلك، سيتوجب على المشاركات أيضاً تذكر أن عضوات أخريات في منظمتهن سيحتجن لتدريب على ممارسات و/أو أدوات معينة في مجال الأمن الرقمي من أجل أن يصبح التنفيذ الكامل ممكناً.

باب ٤٥

خطط وبروتوكولات الأمن الرقمي: إعادة تنفيذها بعد التدريب

- الأهداف: في هذه الجلسة، ستستند المشاركات إلى جلسة التخطيط والبروتوكولات الأمنية الخاصة بالمنظمة. ستتم هنا عرض مجموعة توصيات تساعد المشاركات في تسهيل عملية إعادة تنفيذ الخطط والبروتوكولات بعد التدريب ضمن منظماتهم.
- الطول: 40 دقيقة
- الشكل: جلسة
- مستوى المهارة: متوسط
- المعرفة المطلوبة:
- بمن نثقن؟ (تمارين بناء الثقة)
- الممارسة التطبيقية بواسطة أدوات وممارسات الأمن الرقمي من التدريب السابق
- نموذج المخاطر القائمة على النوع الاجتماعي (تحديد الحل الأفضل)
- الخطط والبروتوكولات الأمنية الخاصة بالمنظمة (التخطيط المسبق)
- جلسات/تمارين ذات صلة:

- بمن نثقن؟^١
- وجهات النظر الشخصية حيال الأمن^٢
- كيف يعمل الإنترنت؟^٣
- نموذج المخاطر القائمة على النوع الاجتماعي^٤
- الخطط والروتوكولات الأمنية الخاصة بالمنظمة^٥
- المواد اللازمة:
 - شرائح (فيها النقاط المفتاحية الواردة أدناه)
 - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض

إدارة الجلسة

الجزء الأول - وضع خارطة بالهيكليات والعوائق التنظيمية

١. ضمن مجموعات من شخصين، أطلبين من المشاركات وصف منظماتهن:
 - كم عدد الأشخاص المشاركين/ات فيها؟
 - كم مرة يلتقون في الأسبوع/السنة؟
٢. ضمن الثنائيات من الخطوة السابقة، أطلبين من المشاركات الآن تشارك مع بعضهن البعض، بعض العوائق أو التحديات التي يتوقعن مواجهتها ضمن منظماتهن عند تقديم خططهن الأمنية والتعبير عن الحاجة للبدء بعملية التنفيذ.

<https://vrr.im/bd0d1>

<https://vrr.im/93392>

<https://vrr.im/7ba93>

<https://vrr.im/c0c34>

<https://vrr.im/f75c5>

الجزء الثاني - تسيير تنفيذ المنظمة

٣. بعد أن تنتهي المجموعات من مناقشة النقاط المذكورة أعلاه، شارك بعض الأوفكار التي قد تساعد المشاركات في تسيير عملية تنفيذ خططهن وبروتوكولاتهن الأمنية ضمن منظماتهن بعد التدريب:

- أوصينهن بأن يعرضن ذلك كبداية لعملية تفكير - سيتطلب تنفيذ الخطة ووضع البروتوكولات واختيارها الكثير من الوقت، وستمر المنظمة في مرحلة تكيف إلى أن يعتاد أفرادها على هذه التغييرات. ومع ذلك، يجب أن يحرصن على التشديد أن التفكير بشكلي نقدي أكثر بشأن الأمن التنظيمي خطوة في الطريق الصحيح.
- حذرن المشاركات أنهن سيتلقين بعض الرفض بسبب مصطلح "بروتوكول" بما أن معناه أصبح تقنياً ومشحوناً أكثر من اللازم؛ يجب أن يذكرن الأخريات في منظماتهن أن البروتوكولات ليست إلا إتفاق بشأن المخاطر والتهديدات المحدقة بهن، والالتزام بجلها معاً عبر تحديد إجراءات إستراتيجية لمصلحة المنظمة ومهمتها.
- شددن على أهمية التعاون والإشراك في عملية التنفيذ. يجب أن تعمل المشاركات مع فرق مختلفة ضمن منظماتهن على تقييم مستويات المخاطر في فريقهن، ومن ثم مشاركة نتائج هذا التقييم والخطوات اللاحقة مع بقية زميلاتهن. شددن أيضاً على أن يحرصن المشاركات على إفساح المجال للأخريات في منظماتهن من أجل تقديم الملاحظات بشأن الخطط والبروتوكولات الأمنية - بما أن مهام أشخاص مختلفين ستأثر بطرق مختلفة بهذه التدابير الجديدة، لا بد لهن من تقادي إضافة أعباء جديدة على مهام أي شخص كان.
- أطلبن من المشاركات التفكير في طرق أخرى لإشراك فرق مختلفة من المنظمة بشكلي جماعي - إحدى تلك المقاربات الممكنة هي أن يقترحن "هيئة أمن رقمي" تشمل ممثلات (لديهن ما يلزم من معرفة لإتخاذ قرارات) عن كل فريق أو مجال عمل، مهمتها الإشراف على تنفيذ الخطة الأمنية. ومن ثم يمكنهن تنفيذ

- هذه العملية بشكل تدريجي، فيركّز أولاً على الموظفين ذوات المستوى الأعلى وألبده مع فرق معينة ومن ثمّ توسيع رقعة المشاركة. المقاربة الفضلى ستختلف كثيراً من منظمة لأخرى.
- في الختام - أطلب من المشاركات مشاركة بعض الأفكار التي لديهن والتي قد تساعد في تسيير عملية التنفيذ في منظماتهن.

الجزء الثالث - طرح المسألة

- ٤. أطلب من المشاركات على هيكلية أساسية لطرح هذه المسألة المهمة لمناقشتها ضمن منظماتهن - قد يكون ذلك عبارة عن مجموعة أسئلة، أو خطة تدريب ممكنة خاصة بهن تتضمن جلسات وتمارين معينة مرتبطة ببيئة المخاطر التنظيمية.
- ٥. ذكرن المجموعة أن تنبه للمتطلبات اللوجستية اللازمة، ولا سيما عامل الوقت - قد لا يتوفر للأخريات في منظماتهن الوقت الكافي لتخصيص فترة ما بعد الظهر كاملةً، أو يوم كامل أو فترة أطول من ذلك حتى للتدريب. وتطلب عملية تغيير عادات قديمة وقتاً طويلاً والكثير من الصبر، لذا يفضل أن تبحث المشاركات عن طرق لطرح هذه المسائل (أو التدريبات) خلال الاجتماعات الدورية الموجودة أو خلال تجمعات أخرى. إليكن هيكلية بسيطة قد تتبعها المشاركات لزيادة مستوى الوعي بشأن مواضيع معينة - تبدأ هذه بنقاش حول أهمية الأمن الرقمي بالنسبة للمنظمة، ومن ثم يأتي دور الجلسات (من هذا المنهاج) التي تعرض تفاصيل أكثر عن مواضيع الأمن الرقمي - وتعود مسألة إختيار كيفية إجراء هذه النقاشات للمشاركات:

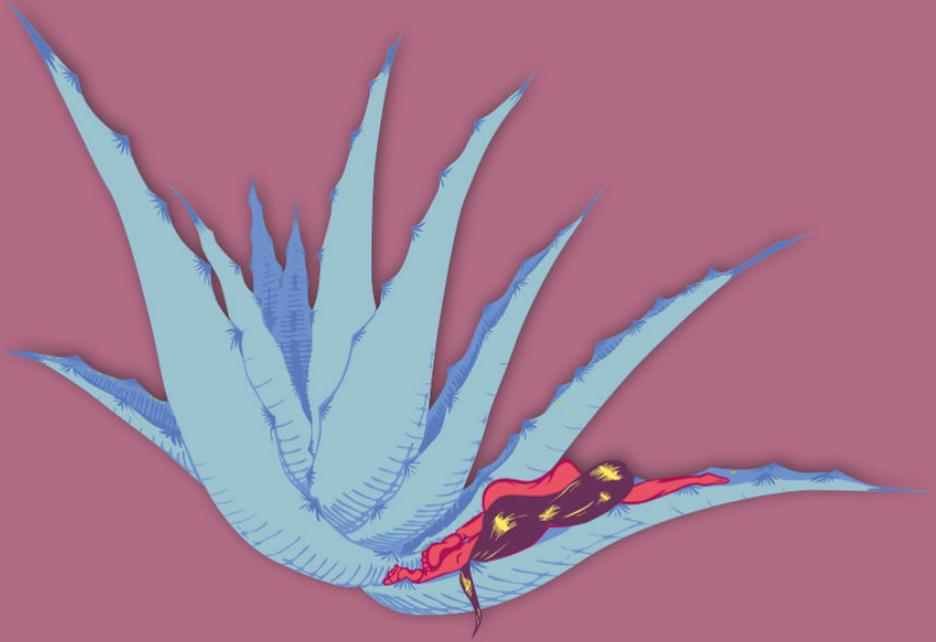
- نقاش: ما أهمية الأمن الرقمي بالنسبة لمنظمتنا
- الجلسة: [كيف يعمل الإنترنت؟ (أسس الأمن الرقمي، الجولة الأولى)]
- الجلسة: [لنبدأ بتوثيق الحالات! (العنف ضد المرأة على الإنترنت)]
- الجلسة: [الهواتف المحمولة، الجزء الأول (هواتف محمولة أكثر أماناً)]
- الجلسة: [الاتصالات المشفرة (التشفير)]

• الجلسة: [نموذج المخاطر القائمة على النوع الاجتماعي (تحديد الحلّ الأفضل)]

٠٦. ذكرن المشاركات أن هذه ليست سوى مقارنة مقترحة - لمن الحرية في تعديل الجلسات والمواضيع وفقاً لما يريته مناسباً. لا بد أن تكنّ متواجداً أثناء قيام المشاركات بعملية التنفيذ في منظماتهن (قدر المستطاع) لتوفير الدعم والإجابة على الأسئلة التي قد تساورهن.



النساء فى فضاء الإنترنت



الرعاية الذاتية

باب ٤٦

بناء الرعاية الذاتية النسوية

- الأهداف: يقدم هذا التمرين للمشاركات فرصة التفكير في أهمية الرعاية الذاتية في حياتهن اليومية، مما يتيح لهن وضع تعريف للرعاية الذاتية في بيئة خالية من الحكم المسبق.
- الطول: 30 دقيقة
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- بمن نثقن؟^١
- وجهات النظر الشخصية حيال الأمن^٢
- المواد اللازمة:
- كرة مطاطية (أو أي شيء صغير من الممكن رميه من شخص لآخر)
- التوصيات: الرعاية الذاتية جزء أساسي من ممارسة الأمن الرقبي الشامل، ومن الضروري تعزيزها وتشجيعها بشكل دائم. - يوصى بأن توزع تمارين هذه الوحدة على إمتداد

^١ <https://vrr.im/bd0d1>

^٢ <https://vrr.im/93392>

فترة التدريب.

في هذه الجلسة وفي كل جلسات تدريبيكن، تنبهن دائماً لقدرات النساء البدنية وحدودها المختلفة.

يفضل تقديم هذا التدريب في بداية التدريب أو في بداية يوم تدريبي ماء؛ وبما أنه تمرين يستند إلى التفكير والإستنباط، إحرصن على أن يفصل وقت طويل بينه وبين التمارين الأخرى المرتبطة بالرعاية الذاتية.

هذا التمرين مستمد من محتوى دليل منظمة نساء على الحافة (Mujeres Al Borde) "الرعاية الذاتية والتعافي النسوي في الحالات الصعبة"

إدارة التمرين

١. إبدأن التمرين بتقديم فكرة الرعاية الذاتية - إسلأن المشاركات إن كنّ يعرفن هذا المفهوم أو سعنن به قبل الآن. عرّفن المجموعة بمفهوم الرعاية الذاتية وإشرحن أن هذا التمرين سيركّز على الرعاية الذاتية كممارسة نسوية في سياق عمل المدافعات عن حقوق الإنسان.
٢. الآن، إشرحن كيف سينفذ هذا التمرين البسيط:

أطلبن من المشاركات الوقوف وإمنحنهن بعض الوقت للتحركّ في الغرفة وتمديد عضلاتهن - ومن ثمّ، أطلبن منهن الوقوف في حلقة. سنبداًن برمي كرة صغيرة بلطف (أوأي شيء من الممكن رميه من شخص لآخر) إلى إحدى المشاركات. عندما تلتقطنها، ستسلأنهن سؤالاً لإستنباط أفكارهن بشأن جوانب الرعاية الذاتية بما أنها مرتبطة بهن شخصياً (يمكنكن الإستعانة بالأمثلة الواردة أدناه). بعد أن يجبن على الإسئلة، سترمي المشاركات الطابة إليكن من جديد؛ وعندها سترمينها إلى مشاركة أخرى وتكررن العملية الواردة أعلاه. يمكنكن الإستمرار في التمرين، إلى أن تسنى فرصة الإجابة عن سؤال لكل مشاركة من المشاركات. إليكن بعض الأمثلة عن الأسئلة التي قد تستخدمنها في هذا التمرين (لا تترددن في طرح أي أسئلة مشابهة تتمحور حول الرعاية الذاتية تخطر في بالكن):

ما هي الرعاية الذاتية بالنسبة لـكن؟ ما هي الرعاية الجماعية؟ ما الفرق بينهما؟ هل الرعاية الذاتية مسألة تعالجها منظماتكن أو مجموعاتكن أو جماعاتكن؟ هل تمارسن الرعاية الذاتية؟ ما هي ممارسات الرعاية الذاتية الخاصة بكن؟ هل يصعب عليكم التفكير بأنكن جديرات بالرعاية؟ هل يصعب عليكم التفكير في شخص جدير بالرعاية؟ كمدافعات عن حقوق الإنسان، هل تعتقدن أننا نميل أكثر لتقديم الرعاية الذاتية للآخرين على حساب أنفسنا؟ هل تشعرن أنكن منتهيات لما تحتاج له أجسادكن وأرواحكن؟

٣. من بعد أن يحصل كل شخص على فرصة الإجابة على سؤال واحد، أو يعبر عن أفكاره أو ممارساته المرتبطة بالرعاية الذاتية، إختتمن النقاش بتقديم ملخص سريع عما شاركنه المجموعة - هل هذه مجموعة من النساء اللواتي لا يعرفن مفهوم الرعاية الذاتية كممارسة متعمدة، وربما لا يمارسنها في أغلب الأحيان (أو لا يمارسنها أبداً)؟ قد تكون مجموعة النساء هذه تعرف مفهوم الرعاية الذاتية جيداً وتمارسه بشكلٍ منتظم؟ أو ربما المجموعة فيها بعض النساء اللواتي يعرفن جيداً ماهية الرعاية الذاتية وبعض آخر لا يعرف عنه الكثير، ويمكنهن التعلم من بعضهن البعض؟ ركّزن على أي معلومات أو ممارسات تشاركها المجموعة - وإحرصن على التركيز على أي عنصرٍ إيجابي يقمن به بشكلٍ جيد!

٤. إسألن المجموعة - هل المسؤوليات التي تتولاها كمدافعات عن حقوق الإنسان مختلفة عن تلك التي يتولاها الرجال؟ ناقشن الأعباء الاجتماعية التي يتوقع منهن حملها، لا سيما دور مقدمات الرعاية - الرعاية بالمنزل والعائلة وأحياناً حتى العمل والزملاء - التي يفرضها المجتمع غالباً على النساء.

٥. حللن كيف تؤثر هذه المسؤوليات الإضافية على عملهن كمدافعات عن حقوق الإنسان، وقن بمقارنتها مع التحديات التي يواجهها الرجال. يمكنكن هنا التطرق أيضاً لمسألة الشعور بالذنب الذي ينتاب المدافعات عن حقوق الإنسان في أغلب الأحيان - إذ علمن الإختبار في حالات كثيرة بين نشاطهن وحياتهن الشخصية وعائلاتهن ويشعرن، بغض النظر عن خيارهن، أن إعتماذ خيار ما يعني إهمال الخيارات الأخرى إلى حدٍ كبير.

٥٦. بعد هذه النقاشات، إختتمن التمرين عبر سؤال المشاركات عما إذا كنّ يرغبن في طرح ممارسات رعاية ذاتية تضاف إلى عملية التدريب؛ قد يعني ذلك على سبيل المثال، تأخير موعد التدريب قليلاً كل يوم، أو تخصيص فترات أقصر وأكثر للإستراحة وتناول وجبات طعام معينة معاً،...إلخ.

باب ٤٧

لمسة محبة

- الأهداف: في هذا التمرين الهادف للإسترخاء، ستبني المشاركات علاقات مع بعضهم البعض من خلال لمس بعضهم البعض، ما يعكس فعل تقديم الحنان والمحبة والرعاية وتلقيها.
- الطول: 20-30 دقيقة
- الشكل: تمرين
- مستوى المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- قواعد اللعبة^١
- بناء الرعاية الذاتية النسوية^٢
- المواد اللازمة:
- فرش أو بطانيات
- مخدات أو وسادات
- موسيقى هادئة

^١ <https://vrr.im/e441>

^٢ <https://vrr.im/143b>

• التوصيات: الرعاية الذاتية جزء أساسي من ممارسة الأمن الرقمي الشامل، ومن الضروري تعزيزها وتشجيعها بشكل دائم. - يوصى بأن توزع تمارين هذه الوحدة على مختلف أنحاء التدريب. في هذه الجلسة وفي كل جلسات تدريبيك، تنبهوا ولا تنسوا أن لكل امرأة قدرات جسدية مختلفة. يجب ألا تنسين أنتن والمشاركات الأخرى التنبه والوضع في الاعتبار أنه بعض النساء قد لا يشعرن بالإرتياح في حال لمستن نساء آخريات (لا سيما في بعض الثقافات) - لهذا السبب، يفضل تنفيذ هذا التمرين مع مجموعات من النساء اللواتي يعرفن بعضهن البعض ويثقن ببعضهن البعض. في حال إختارت بعض النساء عدم المشاركة في هذا النشاط، أخبرنه أن ذلك مقبول تماماً من قبلكن. أكدن لمن أنهن لن يدفعن إلى القيام بأي أمر يعجزهن وذكرنه أنه يمكنهن المشاركة عبر الإستلقاء والإسترخاء لبضعة دقائق من خلال التنفس بعمق وبطء. لإنشاء بيئة تشجع على الإسترخاء ومراجعة الذات، قد ترغبون بإضاءة بعض الشموع أو البخور أو تشغيل موسيقى هادئة خلال هذا التمرين.

هذا التمرين مقتبس من محتوى دليل الرعاية الذاتية من منظمة "آي إم ديفنדרز" IM Defenders Self-Care Manual

إدارة التمرين

١. رتبين البطانيات والوسادات على شكل حلقة على الأرض - أطلين من نصف المجموعة الإستلقاء على ظهورهن في الحلقة، ورؤوسهن موجهة نحو وسط الحلقة وكأنهن يشككن بتلات زهرة. أطلين منهن إغماض أعيونهن والإسترخاء. إحرصن على وجود مساحة تكفي لشخص واحد على الأقل بين كل مشاركة.
٢. أطلين من النصف الآخر من المجموعة التمرکز في المساحات الموجودة بين مشاركات النصف الأول من المجموعة، وأن يجلسن بالقرب من ركب المشاركات المستقلات.
٣. ستقدن هذه الجلسة بواسطة صوتكن، إشرحن للمجموعة الجالسة أنهن سيمنحن "لمسة محبة" للنساء المستقلات إلى جانبهن. سيلبسهن بطريقة محترمة وغير مزعجة ستصفونها

لهن الآن. وأولئك اللواتي يزججنهن لمس الأخریات، يمكنهن وضع أيديهن على رأس أو كتف شريكتهن فقط أو بكل بساطة إغلاق أعيونهن والإستماع إلى صوتكن.

٤. بصوت هادئٍ ونبرة لطيفة، ستعطين النساء الجالسات إرشادات متعددة بشأن لمسات الحبة، التي تفصل بينها دقيقتان أو ثلاثة دقائق. ذكروا الجميع أن التنفس مهم جداً في هذا التمرين - عليهن جميعاً التنفس ببطء وإستنشاق الهواء من أنوفهن وإخراجها من أفواههم:

- التوجيه الأول: إلمسن وحركن بأيديكن ببطء على رأس شريكتهن.
- التوجيه الثاني: إلمسن وحركن بأيديكن ببطء على جبهة شريكتهن.
- التوجيه الثالث: إلمسن وحركن بأيديكن على كتف شريكتهن.
- التوجيه الرابع: إلمسن وحركن بأيديكن على أيدي وأصابع شريكتهن.

٥. مع تقدم المجموعة في هذا النشاط، تحدثن عن:

• مدافعات عن حقوق الإنسان، لا وقت لدينا عادةً لأنفسنا. وبالتالي المشاركات اللواتي يقمن بلبسة الحنان لشريكتهن يمنحنهن فرصة نادرة للإسترخاء والشعور بأن أحداً يهتم لأمرهن.

• الأعباء والمسؤوليات الاجتماعية الملقاة على كاهل النساء - كمدافعات عن حقوق الإنسان وأمّهات وأخوات، يتوقع منا دائماً الإهتمام بالآخرين ولكن هل نهتم بأنفسنا؟ ففي حياتنا نادراً ما يتاح الوقت لنهتم بأنفسنا على الصعيد الفردي أو الجماعي.

٦. بعد أن تنتهي المشاركات الجالسات من لمس أيدي وأصابع شريكتهن، أطلبن من النساء المستقلات بعد بضعة لحظات من فتح أعينهن، تبادل الأماكن مع شريكتهن. وكررن العملية ذاتها لكي يحصل الجميع على فرصة التلقي.

باب ٤٨

أنظري

- الأهداف: في هذا التمرين، ستبتعد النساء عن أي إحساس بالرتابة والإستياء والحزن والرغبة في الإنقطاع عن الناس عبر تفعيل رغبتهن بالحلم والتمتع بالحياة.
- الطول: 20 دقيقة (بحسب حجم المجموعة)
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
 - بناء الرعاية الذاتية النسوية^١
 - لمسة محبة^٢
 - المواد اللازمة:
 - ذهن متفتح وهادئ
- التوصيات: الرعاية الذاتية جزء أساسي من ممارسة الأمن الرقمي الشامل، ومن الضروري

^١ <https://vrr.im/143b>

^٢ <https://vrr.im/e04d>

تعزیزها وتشجيعها بشكل دائم. یوصی أن توزعن تمارین هذه الوحدة على إمتداد فترة التدريب.

في هذه الجلسة وفي كل جلسات تدريبك، تنبهن دائماً لقدرات النساء البدنية وحدودها المختلفة.

هذا التمرین مقتبس من محتوى دليل منظمة نساء منظمة نساء على الحافة (Mujeres Al Borde) "الرعاية الذاتية والتعافي النسوي في الحالات الصعبة"

إدارة التمرین

١. إبدأن بشرح مدى سهولة طغيان الشعور بالرتابة والإستياء والحزن والرغبة في الإنقطاع عن الناس التي يجب تحطيمها في الحياة اليومية للناشطات والمدافعات عن حقوق الإنسان.

٢. واصلن شرح ذلك، وخلال التمرین، سنتناول المشاركات تلك الأحاسيس التي يشعرن بها حين يعانين أو يشعرن بالضيق أو يفقدن البوصلة - سيقمن بذلك عبر تفعيل نقطة طاقة تقوم وفقاً للطب التقليدي الشرقي، بتفعيل الرغبة في الحلم والوقوع في حب الحياة من جديد.

٣. أطلبن من المشاركات الجلوس في حلقة، إما على كراسين وإما على الأرض.

٤. وجهن المجموعة في الخطوات التالية (كرن هذه العملية ثلاث مرّات):

حددن مكان نقطة الطاقة - هي موجودة بين العينين، تحت الحاجبين وفوق عظمة الأنف تماماً.

خذن نفساً عميقاً واحبسنه.

بواسطة إبهامك، إضغطن على نقطة الطاقة - وأثناء عملية الزفير، فكرن بشيء يلهمك ويشعركن بحب الحياة.

٥. إختمن الجلسة بتشجيع المشاركات على الإستعانة بهذه التقنية في كل مرّة يشعرن فيها بأنهن بحاجة لإستعادة الإحساس بالإستقرار والإبتعاد عن أحاسيس اليأس أو الحزن.

تحدثن مع المشاركات حول أن الشعور بالخوف أو التعب أو الاستياء أحياناً ليس عيباً
وأن الجميع يمر بمثل هذه الحالة من وقت لآخر.

باب ٤٩

التفكير في الرعاية الذاتية (إستنتاجاتنا)

- الأهداف: يقدم هذا التمرين للمشاركات فرصة التفكير في ممارسات الرعاية الذاتية الخاصة بهن - لا سيما تلك التي يقمن بها بشكلٍ جيد أصلاً، وتلك التي يمكنهن تحسينها وتلك التي يتوجب عليهن إتمامها.
- الطول: 20-30 دقيقة (وفقاً لتقديركن)
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
- جلسات/تمارين ذات صلة:
 - أنا صاحبة القرار^١
 - بناء الرعاية الذاتية النسوية^٢

^١<https://vrr.im/8204>

^٢<https://vrr.im/143b>

- لمسة محبة^٣
- أنظري^٤
- المواد اللازمة:
 - مرآة لكل مشاركة
 - ملصقات مدوّرة Dot stickers
 - اختياري: تستطيع المشاركات استخدام صورة لهن بدل المرآة (أطلبن منهن جلبها قبل التدريب)
- التوصيات: الرعاية الذاتية جزء أساسي من ممارسة الأمن الرقيي الشامل، ومن الضروري تعزيزها وتشجيعها بشكل دائم. يوصى أن يتم توزيع تمارين هذه الوحدة على طيلة فترة التدريب.
- لإنشاء بيئة مؤاتية للإسترخاء ومراجعة الذات، يمكنكن إضاءة شموع أو حرق البخور أو تشغيل موسيقى هادئة تبعث على الإسترخاء خلال هذه التمارين.

إدارة التمرين

١. قدمن لكل مشاركة مرآة صغيرة أوفي حال عدم إستخدام المرايا، أطلبن منهن جلب صور لهن. وزعن الملصقات المدوّرة عليهن.
٢. إشرحن لهن أنكن ستقرأن مجموعة من الجمل التي يتوجب على المشاركات الإجابة عنها سلباً أم إيجاباً. في كل مرّة يُجبَن سلباً على إحدى الجمل، عليهن وضع ملصق مدور على المرآة أو على صورتهم.
٣. يرد أدناه لأئحة بالجمل التي يمكنكن إستخدامها خلال هذا التمرين؛ ولكن، إستناداً إلى ما تعرفنه عن المجموعة (ومدى إرتياح المشاركات لبعضهن البعض على المستوى الفردي) يمكنكن إضافة جمل أو تفادي أخرى:

^٣<https://vrr.im/e04d>

^٤<https://vrr.im/19b8>

- كل ليلة، إنال ما لا يقلّ عن ثماني ساعات من النوم واستيقظ مرتاحة وأنا جاهزة لبدء نهاري؛
 - خلال الأشهر الست/ السنة الماضية، إتحت لي فرصة التمتع بعطلة وإستغلتها؛
 - اتبع حمية غذائية صحيّة وأقوم بتمارين رياضية بشكلٍ منتظم، للمحافظة على صحّة وإتزان جسمي وذهني؛
 - أخصص دائماً بعض الوقت لنفسي للمطالعة أو النوم أو لقضاء وقت ممتع مع الأصدقاء والعائلة؛
 - حين أمرض، أرتاح في المنزل للتعافي والتركيز على الشفاء وليس على عملي؛
 - حين يتوجب عليّ القيام بمهمات كثيرة، أرفض دائماً تولي مهام إضافية؛
 - أخضع للفحوصات النسائية التي يوصي بها الأطباء كل ستة أشهر؛
 - أخصص الوقت الكافي لتوضيح وحلّ أي سوء تفاهم مع أحبائي أو زملائي في العمل حين تنشأ أي نزاعات؛
 - أحافظ على نظام عمل من 8 ساعات في اليوم، أحترمه وتحترمه منظمتي؛
٤. بعد الإنهاء من طرح الأسئلة، إسألن المشاركات - ماذا يرين في المرآة (أو في صورهن)؟ إجمع المجموعة في حلقة وناقشن تأثيرات أعباء العمل الزائدة عن حدها، أو الممارسات الإجتماعية السيئة في العمل، أو لرعاية غير الكافية للجسد والذهن على الأفراد، وكيف أنها تجعل شخصياتنا باهتة وتخفي جوهر دواخلنا.
٥. تجولن على المشاركات الجالسات ضمن الحلقة وأسألن المستعدات منهن تحديد هدف أو نيّة معيّنة - هذه النيّة يجب أن تكون العزم على البدء برعاية الذات عبر القيام بإحدى نشاطات الرعاية الذاتية المذكورة آنفاً بشكلٍ منتظم.

باب ٥٠

فعل الرفض

- الأهداف: هذا التمرين عبارة عن فرصة للنساء للتفكير في الأعباء المفروضة عليهن - كنساء أو مدافعات عن حقوق الإنسان أو ناشطات - وكيف يمكنهن تبرير الحاجة للرعاية الذاتية لأنفسهن بشكل أفضل.
- الطول: 10 إلى 15 دقيقة
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
- جلسات/تمارين ذات صلة:
 - لا يوجد
- المواد اللازمة:
 - الصدق والحساسية
- التوصيات: الرعاية الذاتية جزء أساسي من ممارسة الأمن الرقبي الشامل، ومن الضروري تعزيزها وتشجيعها بشكل دائم. يوصى أن توزع تمارين هذه الوحدة على طيلة فترة التدريب. بعض النساء قد لا يشعرن بالإرتياح لمشاركة قصصهن (راجعن أدناه)، في

هذه الحالة يمكنهن مشاركة قصة صديقة أو أخت أو زميلة في العمل.

إدارة التمرين

١. قدمن التمرين عبر التحدث مع المجموعة عن الضغوطات التي يمارسها المجتمع على النساء - أي الأعراف الاجتماعية والثقافية التي تفرض على النساء مثل العمل ضعيفي أو ثلاثة أضعاف أكثر من الرجال لإثبات جدارتهن على سبيل المثال.
٢. تحدثن عن تحمّل المدافعات عن حقوق الإنسان أعباء إضافية - ومن ضمنها، أعباء العمل والإحساس بالذنب جراء الفشل في إنجاز المهام في الموعد المحدد أو تحقيق الأهداف، والرعاية المتوقعة من قبلهن تجاه حاجات الآخرين قبل حاجاتهن الخاصة على سبيل الذكر لا الحصر.
٣. والآن، إشرحن للمشاركات أنه في هذا التمرين، سيحظين بفرصة التفكير في الأعباء التي يحملنها. إبدأن بتقسيم المجموعة إلى مجموعات من شخصين.
٤. أطلبن من كل مجموعة من شخصين إخبار بعضهما البعض قصة عن حادثة أردن خلالها رفض أمرٍ ما، ولكن لم يتمكن من ذلك - هذه فرصة كان يمكنهن فيها رفض أي عمل إضافي أو أي طلب لخدمة ما أو تلبية إلتزام آخر ولكن لم تستطعن فعل ذلك في الواقع. يمكنكن البدء بإخبار قصة من قصصكن، عن حادثة أردن الرفض فيها - على سبيل المثال:
- كنت أخطط لتناول طعام العشاء مع صديقتي، ولكن أثناء تواجدي في العمل، طلب مني البقاء حتى وقت متأخر لحلّ مشكلة طرأت على أحد المشاريع المهمة. لم استطع الرفض، ولكن أردت ذلك فعلاً.
٥. بعد أن تنتهي كل مجموعة من إخبار القصص، أطلبن منهن الآن إعادة سرد قصتهن على بعضهن البعض؛ ولكن هذه المرة سيغيّرن قصتهن ويفترضن أنهن رفضن فعلاً.
٦. إخبزن المشاركات أنه يمكنهن، إذا أردن ذلك، عند إخبارهن النسخة البديلة لقصصهن

إضافة كيفية شرحهن سبب رفضهن للمسؤول/ة عنهن أو زميلهن/زميلتهن أو أي شخص
يطلب منهن أمرًا ما. هذه الإضافة إختيارية ولكن قد تشكل طريقة جيدة للتفكير
بشكلٍ صحي بأهمية تخصيص وقت لأنفسهن.

باب ٥١

رسالة حب إلى نفسي

- الأهداف: يفترض أن يوفر هذا التمرين المساحة والوقت الكافيين للمدافعات عن حقوق الإنسان للتفكير في أنفسهم وفي مخاوفهم والإجراءات التي يمكنهم إتخاذها للتخفيف من الضغوطات المفروضة عليهم.
- الطول: 20 دقيقة
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- لا يوجد
- المواد اللازمة:
- أوراق وأقلام
- جهاز عرض وحاسوب محمول/حاسوب (لعرض الجمل الواردة أدناه)
- اختياري: في حال تفضلن عدم الإستعانة بجهاز عرض لهذا التمرين، يمكننا كتابة الجمل الواردة أدناه على ورقة وركي كبيرة أو على لوح إعلاني

- التوصيات: الرعاية الذاتية جزء أساسي من ممارسة الأمن الرقمي الشامل، ومن الضروري تعزيزها وتشجيعها بشكل دائم. يوصى أن توزع تمارين هذه الوحدة على طيلة فترة التدريب. وفقاً للمجموعة التي تعملن معها (والوقت المتوفر لكن لهذا التمرين) فكّرن في إختتام ذلك بجلسة تفكير في الرعاية الذاتية وأهميتها. إسألن المشاركات - متى كانت المرّة الأخيرة التي سألن فيها أنفسهن كيف يشعرن؟ هل نشاطهن يؤثر على صحتهن؟ كيف يهتمن بالموارد الأهم لديهن في نشاطهن (ألا وهي أنفسهن)؟

إدارة التمرين

١. على شريحة معدّة مسبقاً أوورقة من أوراق لوح ورقيّ إعرضن على المشاركات ما يلي:
عزيزتي،
تحية طيبة وبعد،
أنا أراقبك مؤخراً، وأعلم أنك تتمرّين بظروف صعبة فيما يخص....
أعلم أيضاً أنك خائفة على....
أردت فقط أن تعرفي أن...
تذكرني أنك بارعة جداً في....
أعتقد أنه يتوجب عليك....
حاولي أن..... في الأسابيع القادمة.
مع محبتي،
نفسك
٢. وزعن ورقة لكل مشاركة - أطلبن منهن ملء الفراغ إلى جانب "عزيزتي" بإسمائهن،
ومن ثمّ إكمال الجمل الأخرى الموجودة أمامهن.

٣٠٣ . ذكرن المشاركات أنهن غير مضطرات لمشاركة رسالتهن مع بقية المجموعة - فهذا نشاط شخصي إلى حدٍ كبير.



النساء فى فضاء الإنترنت



تمارين الختام والمراجعة

باب ٥٢

الحكواتيات

- الأهداف: هذا التمرين الحركي سيساعدكن على رفع مستوى نشاط و طاقة المشاركات والمحافظة على تركيز وإهتمام المجموعة. يقدم هذا التمرين إستراحة من المحتوى التدريب التقني، وفي الوقت عينه هو مرتبط بمواضيع الأمن الرقمي.
- الطول: 10 إلى 15 دقيقة (وفقاً لحجم المجموعة)
- الشكل: تمرين
- مستوى المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- قصتها مع التكنولوجيا¹
- المواد اللازمة:
- كراسي (تحديداً أقل بعدد واحد كرسي عن عدد المشاركات)

¹<https://vrr.im/c865>

إدارة التمرين

- ٠١ إسألن المشاركات إن كنّ يعرفن لعبة "سلّة الفاكهة" (إن كنّ لا يعرفنها، يمكنكن سؤالهن عن لعبة "الكراسي") - إشرحن لهن أن هذه اللعبة نسخة معدّلة بإدخال اللمسة النسوية إليها.
- ٠٢ ربّين الكراسي على شكل حلقة وأطلبين من المشاركات الجلوس عليها - يفترض أن يكون عدد الكراسي أقلّ بعدد واحد كرسيّ عن عدد المشاركات وبالتالي ستبقى مشاركة واحدة واقفة.
- ٠٣ زودن كل مشاركة بإسم امرأة بارزة في مجال التكنولوجيا أو العمل النسوي (الخيار يعود لكنّ) - يمكنكن حتى إستخدام أسماء النساء ذاتها التي تحدّثن عنها في جلسة قصتها مع التكنولوجيا. زودن المشاركات عدّة بالاسم ذاته.
- ٠٤ إشرحن للمشاركات من هن الحكواتيات - هن نساء يجمعن النساء حولهن ليخبرن ويسردن قصصاً وحكايات - وقلن لهن أنهن معاً سيشتكّن مجموعة حكواتيات يتبادلن قصصهن الخاصة!
- ٠٥ إبداً التمرين بقصة (من نسج الخيال) عن بعض النساء المتخصصات في عالم التكنولوجيا اللواتي يردن تكريمهن:
- في كل مرة يبيى على ذكر اسم من أسماء هؤلاء النساء، سيتوجب على المشاركات اللواتي زودتنهّن بإسمها أن يغيّرن مقاعدهن بسرعة (المشاركة التي كانت واقفة يمكنها أن تحاول إيجاد كرسي فارغ لتجلس عليه). المشاركة التي تبقى واقفة سيتوجب عليها الإستمرار في إختراع بقية الحكاية إلى أن تذكر ميسرة الجلسة اسم آخر فتغيّر المشاركات مقاعدهن مجدداً. في حال ذكرت ميسرة الجلسة كلمة "حكواتية" خلال القصة، فهذا يعني أنه سيتوجب على الجميع الوقوف بسرعة وتغيير المقاعد.
- ٠٦ كررن الخطوات المذكورة أعلاه مرّات عدّة إلى أن ترد أسماء كل النساء أو إلى أن تحصل كل مشاركة على فرصة سرد جزء من الحكاية.

باب ٥٣

القِدْرُ المِغْلِي (المِرْجَل)

- الأهداف: رتب المساحة المخصصة للمشاركة في التمرين. عند العمل مع مجموعة، قد يميل أشخاص معينين إلى التحدث أكثر من غيرهم - الغاية من هذا التمرين هو توعية المشاركين لهذا الجانب من الواقع، وفي الوقت عينه، تشجيع المشاركات اللواتي لا يتكلهن كثيراً، على المبادرة والتعبير عن أنفسهن.
- الطول: 15 إلى 20 دقيقة (وفقاً لحجم المجموعة)
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- لا يوجد
- المواد اللازمة:
- قصاصات ورقية معدة مسبقاً (من 3 إلى 5 قصاصات لكل مشاركة)
- وعاء أو حوض

• التوصيات: تمرين القِدْر المغلي (المِرْجَل) تمرين قد يستفاد منه طيلة فترة تدريبك - في حال تقديمه في بداية ورشة العمل، يمكنك استخدام هذا التمرين في كل مرّة تطرحن سؤالاً على المجموعة خلال الجلسة. بهذه الطريقة، نتاح للجميع فرصة التحدّث أكثر من العادة، واللواتي ينجلن من الإجابة على الأسئلة المطروحة ستكون لديهن فرصة الشعور براحة أكبر. يتركز هذا التمرين على نقاش جماعي، حول أي موضوع كان؛ ولكنه فعّال أكثر حين يكون موضوع النقاش يركّز على موضوع من مواضيع التدريب. يمكنك تقديم موضوع جديد، أو استخدام هذا التمرين كعملية مراجعة لموضوع تمت مناقشته مسبقاً - الخيار يعود لكن.

إدارة التمرين

- ١. أطلبن من المشاركات الجلوس في حلقة حول الوعاء أو الحوض - سيرمز ذلك إلى القِدْر المغلي (المِرْجَل). قدمن لكل مشاركة 3 قصاصات ورقية.
- ٢. إشرحن قواعد سير النقاش: في كل مرّة نتكلم إحداهن، عليهن رمي قصاصة ورقية واحدة في القِدْر المغلي (المِرْجَل). وحين تنتهي القصاصات لدى مشاركة ما، يصبح ممنوعاً عليها التكلّم.
- ٣. إطرحن موضوعاً وسيرن النقاش عبر طرح سلسلة من الأسئلة على المجموعة. على سبيل المثال، في حال كان الموضوع عن البرمجيات الخبيثة والفيروسات، يمكنك طرح الأسئلة التالية:
ما هي البرمجيات الخبيثة؟
ما هي الأنواع المختلفة من البرمجيات الخبيثة التي تعرفنها؟
هل تتوفر أنظمة تشغيل محصّنة ضد الإصابة بالبرمجيات الخبيثة؟
هل سبق لحاسوبك أو هاتفك أن أصيب ببرمجيات خبيثة؟ في حال حدث ذلك لكن من قبل، كيف إكتشفت ذلك؟

ما هي بعض الطرق التي يمكننا من خلالها حماية أجهزتنا من الإصابة بالبرمجيات الخبيثة؟

٤. أكلن النقاش إلى أن تنفذ القصاصات من جميع المشاركات - يمكن إعادة تفعيل النقاش في حال رغبته بذلك، عبر الانتقال إلى موضوع جديد وإعادة القصاصات إلى جميع المشاركات.

باب ٥٤

أزهار النسويات

- الأهداف: من بعد يوم حافل بالتدريب على الأمن الرقمي (لا سيما في اليوم الأول أو اليومين الأولين من التدريب) وجهن المشاركات في هذا التمرين لتحفيزهن وتشجيعهن على الإستمرار.
- الطول: 10 دقائق
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
 - غير ضرورية
 - جلسات/تمارين ذات صلة:
 - لا يوجد
 - المواد اللازمة:
 - قصاصات ورقية صغيرة
 - قلم
 - أزهار (حقيقية أم ورقية/بلاستيكية)
- التوصيات: يمكن إجراء هذا التمرين مرّات عدّة في مختلف مراحل التمرين - يمكنك إختتام اليوم الأول أو الأوّل والثاني به. في حال لم تجدن أزهار طبيعية، يمكنكن تعلّم

كيفية صنع زهور ورقية على هذا الرابط: https://www.youtube.com/watch?v=_dq1tthtiu8o

إدارة التمرين

١. قبل البدء بهذا التمرين، سيتوجب عليك التحضير له مسبقاً:
 - أكتبين رسائل تشجيع قصيرة على قصاصات الورق الصغيرة - إليكن بعض الأمثلة:
 - بعد هذه التجربة، لن تحتجن لشخص "متخصص تقنياً" بعد اليوم.
 - هناك مجتمع خاص بالنساء/النسويات موجود وسيحميني.
 - آخذ نفساً عميقاً وأعيد ضبط حاسوبي.
 - أنا قادرة على القيام بذلك - فقد أنجزت أموراً أصعب من قبل.
 - لا تملك أجهزتي سطوة سحرية عليّ - أنا أمسك بزمام الأمور.
 - الشخص الوحيد القادر على إتخاذ القرارات بشأن ممارستي للأمن الرقمي هو أنا.
 - بعد أن تكتبن هذه الجملة، ضعن كل قصاصات الورق داخل الأزهار.
٢. أطلبن من المجموعة الجلوس ضمن حلقة وإسألنهن - كم مرّة شعرتن بالإحباط أو بسيطرة التكنولوجيا عليكن؟ ذكرن الجميع أن هذا طبيعي جداً، على الرغم من التحديات التي نواجهها كمدافعات عن حقوق الإنسان.
٣. درن على الحلقة وقدمن لكل امرأة زهرة واحدة - أطلبن منهن الإحتفاظ بها، ولكن من دون فتحها الآن.
٤. أخبرن المجموعة قصة عن تجربة مزعجة تعرضتن لها كمدربات، أو إحدى تجاربكن الأولى في مجال الأمن الرقمي. أخبرنهن أنكن تفهمن تجاربهن مع تحديات التكنولوجيا وذكرنهن أنهن قادرات على تحطيط أي مشكلة إذا عملن مع بعضهن البعض.

٥. والآن، أطلبين من المشاركات فتح أزهارهن - درن على الحلقة وأطلبين من كل واحدة قراءة الرسالة الموجودة فيها بصوت عالٍ. إسألن إن كنَّ يرغبن في مشاركة أحاسيسهن أو العبر المستخلصة من اليوم هذا، وما إذا كنَّ يرغبن في مشاركة ما تعنيه الرسالة لهن.

باب ٥٥

الحلقة السحرية

- الأهداف: يقدم هذا التمرين خاتمة مناسبة لعملية التدريب أو لجلسة واحدة، تقوم خلالها المشاركات بتحديد نيتهن بالإستمرار في مشاركة ما تعلمنه مع الأخريات.
- الطول: 30 دقيقة
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- لا يوجد
- المواد اللازمة:
- ورقة وقلم

إدارة التمرين

١. تزداد المعرفة أو التجارب الجديدة فائدة عند مشاركتها وتعاطيها مع أشخاص آخرين. إشرح أن الهدف من هذا التمرين هو أن تحدد المشاركات نية الإستمرار في مشاركة مع تعلمه خلال عملية التدريب مع الآخرين.
٢. أطلب من المجموعة تشكيل حلقة - يمكنهن الجلوس على الأرض أو على كراسٍ أو الوقوف، وفقاً لما يناسب الجميع.
٣. بما أن اسم هذا التمرين هو "الحلقة السحرية"، إبدأن التمرين بالتحدث عن أهمية ورمزية الحلقة السحرية التقليدية:
 - منذ فترة ما قبل التاريخ كانت الطقوس السحرية تمارس ويحتفل بها حيث يشكل المشاركون فيها حلقة حيث يُعتقد أنه من خلال الطاقة المنبعثة بين الأشخاص الواقفين على شكل حلقة، من الممكن طرد الأرواح الشريرة وإبقاء الأرواح الخيرة؛
 - عند تشكيل حلقة، من الممكن لكل الأشخاص فيها رؤية بعضهم البعض على مسافة واحدة - فكل شخص يشغل المستوى ذاته الذي يشغله الآخرون، ولا نزاع على القيادة - لذا يثق الجميع بالقيادة.
 - تحقق الحلقات التوازن في تدفق الطاقة، فالجميع يقدم القدر ذاته الذي يتلقاه؛ لا أحد يحتل المركز الأول أو المركز الأخير - الجميع متساوٍ.
٤. أطلب من كل مشاركة كتابة شيء ترغب في مشاركته على ورقة مع الشخص الواقف إلى يمينها - قد يكون ذلك أي شيء: فكرة أو أغنية أو قصيدة أو شيء مهم بالنسبة لها تعلمته خلال التدريب. ما أن ينتهي الجميع من كتابة شيء، أطلب منهن ثني الورقة عند المنتصف.
٥. على كل مشاركة حمل الورقة المطوية التي كتبت عليها بيدها اليمنى. إشرح لمن أن اليد اليمنى ترمز لقدرة الفرد على مساعدة الآخرين وأن اليد اليسرى ترمز لحاجته للتبادل - يجب على المشاركات الآن الإمساك بأيدي بعضهم البعض في الحلقة، فتمسك اليد

-
- اليني لكل شخص اليد اليسرى للشخص الواقف إلى يمينه.
٥٦. على الجميع الآن إعطاء الرسالة المكتوبة للشخص الواقف إلى يمينه ونقلها من يده اليني إلى يد الملتقي اليسرى.
٥٧. على الجميع الآن قراءة ما على الورقة التي تلقينها - يمكنهن إما القيام بذلك بصوت عالٍ أو بصمت.
٥٨. أثناء قراءتهن للرسائل، تحدثن مع المجموعة عن فكرة التآخي بين النساء - الحب بين النساء اللواتي ينظر إليهن على أنهن متساويات وحليقات لبعضهن البعض، يبنين علاقات تضامن وتعاضد تحمين من العنف والظلم وإنعدام المساواة التي تواجهنها في حياتهن اليومية من أجل غدٍ أفضل. إشرحن لمن أنكن معاً، تدعمن بعضكن البعض ضمن علاقات أخوية نسائية وعبر مشاركة المعرفة والمعلومات مع بعضهن البعض.

باب ٥٦

الفوازير!

- الأهداف: غالباً ما تكون التدريبات مكثفة جداً، وتقدّم كميات كبيرة من المعلومات يجب إستيعابها في مدة قصيرة. هذا التمرين أداة يمكنك إستخدامها لإختبار معرفة وفهم المشاركات وفي الوقت عينه تقدّم بيئة مسلية ومريحة تساعد على إزالة الإحساس بالإجهاد.
- الطول: 15 دقيقة
- الشكل: Exercise
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- غير ضرورية
- جلسات/تمارين ذات صلة:
- لا يوجد
- المواد اللازمة:
- مصطلحات وحقائق عن أدوات السلامة الرقية
- شريط لاصق أو دبابيس
- موسيقى (لتشغيلها في الخلفية)
- التوصيات: في حال صعب على بعض المشاركات التوصل إلى إجابات على الفوازير

الخاصة بالمصطلحات والحقائق الخاصة بأداة الأرقي، في حين أن أخريات أنجزن التمرين في مجموعتهن من شخصين، يمكن للواتي أنجزن التمرين مساعدة الأخريات على معرفة الإجابات على الأدوات المعطاة لهن.

إدارة التمرين

١. أطلبين من المشاركات الوقوف في خط واحد وهنّ يدرن ظهورهنّ إليكن - بواسطة الشريط اللاصق أو الدبابيس، ثبتن أحد المصطلحات والحقائق الخاصة بأدوات السلامة الرقمية على ظهر كل مشاركة. احرصن ألا ترى أيّ منها المصطلح أو الحقيقة المصقاة المعطاة لهن!
٢. بعد الإنهاء من ذلك، أطلبين من المشاركات توزيع أنفسهن في مساحة كبيرة فارغة في الغرفة (يمكن ترتيب ذلك عبر إزالة الكراسي أو المكاتب). إشرح لهن أن المصطلح أو الحقيقة المصقاة على ظهر كل واحدة منهن تمثل مفهوماً أو أداة ناقشناها خلال التدريب.
٣. ضمن بعض الموسيقى - يمكن للمشاركات الآن التحرك بحرية في المساحة المتاحة. يمكنهن مدّ أجسادهن أو المشي أو التحرك بأي طريقة يرغبن بها (ولكن عليهن عدم التوقف عن الحركة). إشرح لهن أنه حين توقفن الموسيقى، على الجميع التوقف عن الحركة والبقاء في مكانه.
٤. أوقفن الموسيقى وأطلبين من كل مشاركة تشكيل ثنائي مع أقرب شخص إليهن. على إحدى المشاركتين إظهار ظهرها للمشاركة الأخرى التي ستحاول حينها التعبير عنه بواسطة الحركات أو التعابير الجسدية فقط، أي عن الكلمة أو المفهوم المصق على ظهرهن. بعد إن تمكن المشاركة من معرفة الجواب الصحيح، سيتبادلن المواقع مع شريكتهن ويكررن العملية - ينتهي التمرين حين تعرف كل المشاركات الجواب الصحيح عن المصطلح أو الحقيقة الخاصة بالأداة المصقاة على ظهورهن.

باب ٥٧

سباق الأمن الرقمي

- الأهداف: لإختتام التدريب بنشاط، ستوجهن المشاركات في سباق مشوق لمراجعة المعرفة بشأن السلامة الرقمية التي تعلمنها.
- الطول: 45 دقيقة (وفقاً لسرعة المشاركات)
- الشكل: تمرين
- مستوي المهارة: أساسي
- المعرفة المطلوبة:
- تتغير وفقاً لما تم تقديمه خلال التدريب.
- جلسات/تمارين ذات صلة:
- تتغير وفقاً لما تم تقديمه خلال التدريب.
- المواد اللازمة:
- أقلام وأوراق لكّابة الرسائل ومغلقات
- أوراق مطبوعة بالأسئلة (واحدة لكل مشاركة)
- مكان واسع في الخارج أو مساحة في الداخل فيها غرف وممرات مختلفة
- التوصيات: محتوى الحالات الذي ستستخدمه في هذا السباق يعتمد على المحتوى الذي

تم تقديمه خلال التدريب - بما أن الهدف من هذا النشاط هو إجراء مراجعة شاملة للتدريب، يفضل أن يجرى السباق في نهاية التدريب. الغاية من السباق هذا أيضاً مساعداً لتكن أثنين كمدربات على تحديد مكان قوة المشاركات والمجالات التي تحتاج فيها للمزيد من التدريب أو الدعم. هذا السباق مصمم بشكلٍ يتيح للمشاركات فرصة تطبيق ما تعلمنه خلال التدريب على المستوى العملي المباشر - لهذا السبب، لا بد أن تركز الحالات المقدمة للمشاركات في هذا التمرين (أمثلة عن الحالات متوفرة أدناه) على سيناريوهات الإستجابة المباشرة للحوادث عوضاً عن التوصية بإجراءات وقائية.

إدارة التمرين

الجزء الأول - الإعداد للسباق

١. قبل البدء بالتمرين، عليكن إتخاذ قرار بعدد المراحل والحالات التي سيتضمنها السباق - لأغراض العرض، تستند هذه الإرشادات إلى سباق من خمس مراحل (حالة لكل مرحلة). لا تنسين إدراج الإرشادات الخاصة في كل حالة لتحديد المراحل التي يجب أن تنتقل إليها المجموعات بعد حلها لكل واحدة.
٢. وزّعن المراحل الخمسة بالتساوي في المساحة المتاحة لكن، يمكن أن تكون جميعها في الغرفة ذاتها (أوفي غرف مختلفة في حال كانت متاحة لهن) - يفضل أن ينفذ هذا التمرين في مساحات مختلفة، إذ من شأن ذلك أن يزيد من نسبة التنافس والحماس في هذا الإختبار. إن أمكن ذلك، حاولن إيجاد مكان لهذا الإختبار خارج مكان التدريب حيث تعملن أثنين والمشاركات - سيمنحكن ذلك دفعاً إيجابياً نظراً لتغيير المكان.
٣. ستضمن كل مرحلة حالة يتوجب على المشاركات حلها بواسطة ما تعلمنه من التدريب، بالإضافة إلى أي مجموعة أدوات تقدمنها لهن (راجعن أدناه). يفضل أن يجرى الإختبار ضمن مجموعات متنافسة، وكل مجموعة تبدأ الإختبار من نقطة مختلفة وعبر طريق مختلف، لكي يختلف الوقت المتاح للإجابة وتفاذي الإزدحام عند أي مرحلة.

إليكن أدناه الموارد التي تحتاجن لها للإعداد للاختبار:

المورد الأول: ترتيب المراحل ودليل مسار الفرق

الثاني الفريق	الأول الفريق
المرحلة الخامسة (الإطلاق)	المرحلة الأولى (الإطلاق)
المرحلة الثالثة	المرحلة الثانية
المرحلة الأولى	المرحلة الثالثة
المرحلة الرابعة	المرحلة الرابعة
المرحلة الخامسة	المرحلة الخامسة
النهاية! E! خط	النهاية! خط

المورد الثاني: الأدوات النخاسة بالحالة

الرقم	الأداة
1	خاصة إفتراضية شبكة
2	للفيروسات مكافحة برمجية
3	مجهول إلكتروني بريد وحساب تور متصفح
4	(بي) جي بي (مفاتيح تشفير
5	أميني بروتوكول
6	الفورية الإستجابة إجراءات
7	الجندر على القائمة المخاطر نموذج

المورد الثالث: الحالات الأمثلة

الحالة رقم 1

إنتهت مخرجة سينمائية لتوها من تصوير فيلم وثائقي عن الإختفاءات القسرية في مصر. في مساء أحد الأيام، ترك مكتبها بعد إجتماع عمل متأخر قاصدةً منزلها لإرسال الوثائق إلى المتعاونين معها وأقاربها، بالإضافة إلى الضحايا والخبراء الذين قابلتهم من أجل الفيلم. ولكنها ما أن وصلت إلى المنزل، إكتشفت أن شقتها تعرضت لمدهامة - والأسوأ في ذلك كله، هو أنها إنتهت لأن الحاسوب المحمول الذي يحتوي على الملف الوثائقي النهائي مفقود (ولا يتوفر أي نسخ إحتياطية له). بماذا تنصحن في هذه الحالة؟

الإجابة النموذجية الأداة الواجب إستخدامها (من ضمن مجموعة الأدوات) إجراءات الاستجابة الفورية

التوصيات:

- إطلاع الأشخاص الذين عملت معهم بما حدث، لاسيما أولئك الذين ساهموا في إنتاج الفيلم؛
- تغيير كل كلمات السرّ الخاصة بحساباتها على الإنترنت وتمكين تقنية التحقق بخطوتين حيث تكون متوفرة؛
- تحديد بروتوكول أمني للتعامل مع التسجيلات المنقحة وتوزيعها في المستقبل؛
- سؤالها عما إذا يتوفر معها نسخ إحتياطية مادية أو على السحابة الإلكترونية لتسجيلات غير منقحة أو مقابلات مصورة أو صور.... إلخ، يمكنها إستعادتها وتخزينها بشكل آمن؛
- مراجعة أي ملفات يمكن إستعادتها لمعرفة ما لا يزال متوفراً معها، بالإضافة إلى تحديد مواقع الأجهزة أو المعدات التي إستخدمتها لتسجيل الوثائقي وتمقيحه؛

الحالة رقم 2

سارة ناشطة - قريباً جداً، سبتبدأ بالعمل مع مجموعة من الناشطات على توثيق جرائم قتل النساء في لبنان. سيتوجب عليهن تشارك المستندات على الإنترنت ومناقشة معلومات حساسة عبر الهاتف، وسيكلف عدد منهن بمهمة السفر إلى مدن معينة لإجراء مقابلات مع عائلات. بماذا توصين؟

الإجابة النموذجية الأداة الواجب إستخدامها (من ضمن مجموعة الأدوات): البروتوكولات الأمنية

التوصيات:

- إعقدن إجتماعاً للمجموعة لإجراء عملية تقييم للمخاطر
- إتفقن على إجراءات الأمن الرقمي التي سيتوجب على المجموعة تنفيذها بالإضافة إلى بروتوكول السفر
- إتفقن على إستخدام تطبيق آمن لتبادل الرسائل كتطبيق سيجنال
- إكتشفن الطرق الآمنة لتبادل المستندات، وربما تشفيرها بواسطة تقنية جي بي جي أو إرسالها عبر خدمة بريد إلكتروني آمنة كتوتانوتا أورايزاب.

الحالة رقم 3

منى منسقة مشروع مخصص لتحقيق العدالة للنساء في بلدها. تلقت منى دعوة لتقديم عرض عن عملها في الخارج، عند وصولها إلى المطار تكتشف أن بيانات الإتصال بالإنترنت قد نفذت على هاتفها وقررت عدم شراء تعبئة للبيانات أو لدقائق الإتصال لأنها ستترك البلاد. أثناء إنتظارها للطائرة، أرادت الإطلاع على بريدها الإلكتروني عبر وصل هاتفها بشبكة الإنترنت اللاسلكية الخاصة بالمطار، ماذا يتوجب عليها فعله؟

الإجابة النموذجية الأداة الواجب إستخدامها (من ضمن مجموعة الأدوات): الشبكات
الإقتراضية الخاصة

الحالة رقم 4

مريم صحافية مغربية تجري تحقيقاً في حالة إختلاس أموال. لهذه الغاية، قدمت طلبات حصول على معلومات من حكومتها. ما هي الطريقة التي توصين بإستخدامها من قبلها لتقديم هذه الطلبات بشكلٍ آمن

الإجابة النموذجية الأداة الواجب إستخدامها (من ضمن مجموعة الأدوات): متصفح تور
وحساب بريد إلكتروني مجهول الهوية

الحالة رقم 5

جماعة نسوية تدافع عن حق المرأة في إتخاذ القرارات تتعرض للمضايقة منذ أسبوع على شبكات التواصل الإجتماعي، ماذا يمكن فعله لحماية أنفسهن؟

الإجابة النموذجية الأداة الواجب إستخدامها (من ضمن مجموعة الأدوات): نموذج المخاطر
القائمة على الجندر
التوصيات:

يمكن للجماعة تحليل المخاطر الناجمة عن الهجمات، وآثار وإحتمالات إرتفاع منسوب الخطر أو التصعيد في مستوى العنف، وبهذه الطريقة تعريف وتحديد الأدوات والإستراتيجية اللازمة للتعامل معها..

الجزء الثاني - إستعداد، تأهب، إنطلاق!

٤. قسمن المشاركات إلى فرق وفقاً لعدد أفراد المجموعة - لكي تتسنى للجميع فرصة المشاركة والمساهمة بشكلٍ متساوٍ، يوصى ألا يتخطى عدد أعضاء كل مجموعة الخمس مشاركات. لا تنسين أنه على كل فريق إختيار اسم مبتكر خاص به!

٥. والآن بعد أن الإنتهاء من تشكيل الفرق وتجهيز المراحل، إشرحن قواعد سباق الأيمن الرقيي للمشاركات:

• وفقاً للمسارات وترتيب المحطات المحدد في دليل ترتيب المحطات ومسارات الفرق، أشرن لكل فريق المحطة التي يجب أن يبدأ منها والمحطة الأخيرة بالنسبة له - إحرصن على الإشارة إلى مكان كل محطة للمشاركات قبل البداية لكي لا تضل الفرق الطريق! يمكنكن وضع أرقام بجانب كل مرحلة.

• على الفرق إيجاد حلّ لكل حالة عند كل محطة بواسطة ما تعلمنه من التدريب ومجموعة الأدوات المقدمة هن - يمكنهن إعتتماد أسلوب الإبتكار في إجاباتهن: تماماً كما هو الحال في الواقع، فلا حلول جاهزة لإسقاطها على أي مشكلة من أي حجمٍ كانت!

• أتركن للفرق بعض الوقت لتجهيز أنفسها - ومن ثمّ نادين "إستعداد، تأهب، إنطلاق!"

• الفريق الأوّل الذي ينتهي من حلّ جميع الحالات عند كل محطة ويعود إلى نقطة الإنطلاق هو الفريق الفائز

٦. بعد أن تنهي الفرق المسار الكامل للسباق، إختتمن النشاط عبر الوقوف ضمن حلقة. في هذه الحلقة، على كل فريق شرح إجاباته الخاصة بكل حالة، وشرح العملية التي إعتمدها لمعرفة الحلول. قدمن ملاحظات لكل فريق أثناء تقديمه للتوصيات في كل حالة.



النساء في فضاء الإنترنت



INSTITUTE FOR
WAR & PEACE REPORTING

I W P R

الملحق

باب ٥٨

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 لمدرّبكم فهم مستوى ممارسات الأمن الرقمي ضمن منظماتكم ومراقبة أي تقدّم حصل في هذا المجال على حدٍ سواء بفضل التدريب الذي ستلقونه 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 استخدمها في عملي والتي تم تحديثها: (الرجاء وضع دائرة

حول الجواب المناسب)

لم تحدث مطلقاً (صفر نقاط)

في الأشهر الستة الماضية (نقطة واحدة)

خلال الأيام الثلاثين الماضية (خمسة نقاط)

منذ أكثر من ستة أشهر (صفر نقاط)

لدينا النظام الأحدث مثبتاً على هذا الحاسوب (خمسة نقاط)

هي قيد التحديث حالياً (ثلاث نقاط)

لا أعرف هذه المعلومة (صفر نقاط)

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

لم تحدث مطلقاً (صفر نقاط)

منذ أكثر من سنة (نقطة واحدة)

خلال الأشهر الستة الماضية (نقطتان)

خلال الأيام الستين الماضية (ثلاث نقاط)

خلال الأيام الثلاثين الماضية (أربع نقاط)

تم إنشاء نسخ احتياطية للبيانات خلال الأيام الأربعة عشر الماضية (خمسة نقاط)

لا أعرف (صفر نقاط)

3. هل قرصكم الصلب أو خدمة السحابة الإلكترونية مشفرة؟

نعم، كلاهما مشفر (خمسة نقاط)

لا (صفر نقاط)

إحداهما فقط مشفّر (ثلاث نقاط)

لا أعرف (صفر نقاط)

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

4. الحاسوب الذي استخدمه في عملي مزوّد ببرمجيات أصلية مرخصة (على سبيل المثال مايكروسوفت ويندوز، مايكروسوفت أوفيس، أدوبي فوتوشوب، أدوبي إيلسترايتر، كوريل درو، مكافخ فيروسات) أو برامج برمجيات مفتوحة المصدر (أوبن أوفيس، سكريبوس)

كل البرامج مقرّصة (صفر نقاط)

بعض البرامج مقرّصة (نقطة واحدة)

معظم البرامج برامج أصلية مرخصة (نقطتان)

كل البرامج مرخصة وأصلية (خمسة نقاط)

معظم البرامج برامج مفتوحة المصدر (نقطتان)

كل البرامج برامج مفتوحة المصدر (خمسة نقاط)

لست متأكدًا/متأكدةً (صفر نقاط)

5. برامج مكافحة الفيروسات مملّحة على الحاسوب والهاتف المحمول المستخدمين من قبلي في

عملي وهي محدّثة وتُشغّل في كل مرة يتم تشغيل الجهاز.

نعم، الحاسوب والهاتف المحمول (خمسة 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 مكافحة 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 (خمسة نقاط)

لا (صفر نقاط)

جهاز واحد فقط من هذين الجهازين مزود بكلمة سرّ

7. شبكة الإنترنت اللاسلكي الموجودة حيث أعمل مزودة بكلمة سرّ مختلفة عن تلك التي

زودني بها مقدم خدمة الإنترنت، وتتماشى كلمة السرّ هذه مع معايير كلمات السرّ القوية (المعايير:

1. تتضمن 25 حرفاً 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 (خمسة

نقاط)

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

جزئياً - لم يطبق إلا معيار واحد من المعايير الخاصة بكلمات السرّ المذكورة أعلاه (ثلاث

نقاط)

جزئياً - تغيّرت كلمة السرّ ولكن لم يطبق أي معيار من معايير كلمات السرّ القوية (نقطة

واحدة)

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

لم أستخدم يوماً شبكات الإنترنت اللاسلكي في الفنادق أو المطارات أو المقاهي إلا إذا

كنت متصلاً بخدمة شبكة افتراضية خاصة. (خمسة نقاط)

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

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

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

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

نعم (خمسة نقاط)

لا (صفر نقاط)

لبعض المستندات فقط (ثلاث نقاط)

في حال أجبت بالإيجاب، ما هي أداة التشفير التي تستخدمونها؟

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

استخدم دائماً التشفير للبريد الإلكتروني أو الرسائل النصية القصيرة أو المحادثات لنقل بيانات حساسة (خمسة نقاط)

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

نادراً ما استخدم التشفير للبريد الإلكتروني أو الرسائل النصية القصيرة أو المحادثات لنقل بيانات حساسة (نقطتان)

لا استخدم أبداً 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 (خمسة نقاط)

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

نعم (خمسة 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 الاجتماعي، الحساب المصرفي، أطلع)

نعم (خمسة نقاط)

لا (صفر نقاط)

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

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

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

نعم - فكرت بالموضوع وأشعر أنني بأمان وفقاً لإدارتي الحالية لهوياتي على الإنترنت (خمسة نقاط)

لا - لم أفكر بالموضوع (صفر نقاط)

جزيئاً - أعتبر أنه من المنطقي إنشاء هويات مختلفة أو غير مكشوفة على الإنترنت ولكنني لم أجري أي تغيير بعد (نقطتان)

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

نظراً لوضعي، من المنطقي بالنسبة لي استخدام اسمي الفعلي وهويتي الحقيقية في كل حساباتي على مواقع التواصل الاجتماعي (خمسة نقاط)

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

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

أي تخزين سلسلة المفاتيح وبأي شكل؟

16. أثناء تصفحك، هل تستخدمون المواقع المزودة بروتوكول نقل النص التشعبي الآمن (HTTPS)?

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

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

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

كل منشوراتي ظاهرة للعموم على مواقع التواصل الاجتماعي (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 الاجتماعي (خمسة نقاط)

لا أعرف كيف أضبط إعدادات الإدارة على أي من حساباتي على مواقع التواصل الاجتماعي (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 (نقطتان)

أتوقع وصولها (ثلاث نقاط)

أعرف المرسل ويكون المرسل متحققاً منه (نحس نقاط)

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

نعم (نحس نقاط)

لا (صفر نقاط)

أحياناً (نقطتان)

لا أعرف ما هذا (صفر نقاط)

ما هي الأدوات الآمنة التي تستخدمونها؟

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

نعم (نحس نقاط)

لا (صفر نقاط)

فقط في مكثي (نقطتان)

فقط في منزلي (نقطان)

فقط لبعض الأجهزة (نقطان)

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

باب ٥٩

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 إيدناه.

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

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

نماذج لجدول 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 وفقاً لسيناريويشتمل على ورشة عمل تعرف بالأمن الرقمي، تمتد ليوم واحد ونصف اليوم مع مجموعة من المدافعات عن حقوق الإنسان أو جماعة نسائية، وتركز بشكل أساسي على تقييم المخاطر بشكل عام. ويفضل أن تكون النساء المشاركات في ورشة العمل هذه قد أصبحن بنهايتها قادرات على تحديد المخاطر المحدقة بهن، وقادرات على التعبير بشكل أوضح عن حاجات الأمن الرقمي الخاصة بهن.

جدول الأعمال هذا يشتمل على جلسات حول أسس الأمن الرقمي وممارسات الرعاية الذاتية وتقنيات توثيق حالات الإستغلال أو التهديدات 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 بكن (إعادة النظر بعلاقتنا بالتكنولوجيا)
٦. التمرين: نموذج المخاطر القائمة على الجندر (تحديد الحل الأفضل)
٧. التمرين: بناء الرعاية الذاتية النسوية (الرعاية الذاتية)
٨. الجلسة: بناء كلمات سر 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 الأول (هواتف محمولة أكثر أماناً)
١٣. الجلسة: لنبدأ بتوثيق الحالات! (العنف ضد المرأة على الإنترنت)
١٤. التمرين: أزهار النسيويات (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 وفقاً لسيناريويشتمل على ورشة عمل تعرف بالأمّن الرقمي تمتد ليوم واحد مع مدافعات عن حقوق الإنسان بدأن لتوهن بالتعامل مع حوادث تحرش على الإنترنت. ويفضّل أن تكون النساء المشاركات في ورشة العمل هذه قد أصبحن بنهايتها قدرات على التعبير بشكل أوضح عن حاجات الأمّن الرقمي الخاصة بهن، وقادرات بسرعة أكبر على تحديد إشارات أوأمّاط الخطر الدالة على حالات العنف القائم على النوعي الاجتماعي (الجندر) على الإنترنت .

يتضمن جدول الأعمال هذا جلسات خاصة للتعريف بالأمّن والسلامة على المستوى الشخصي، وبممارسات الأمّن الرقمي الأساسية وبالتعرّف على أمّاط الإستغلال والتحرش

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

تدريب على تقييم المخاطر ليوم واحد للدفاعات عن حقوق الإنسان اللواتي يتعاملن مع التحرش على الإنترنت

المدة الزمنية التقريبية اللازمة: 7 ساعات

جدول أعمال هذا التدريب مخطط له وفقاً لسيناريويشتمل على ورشة عمل تعرف بالأمن الرقمي تمتد ليوم واحد، مع مدافعات عن حقوق الإنسان يتعاملن مع حوادث التحرش على الإنترنت المستمرة، واللواتي يحتجن للدعم في وضع خطط أمنية وإستراتيجيات للتعامل معها. يفضل 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 جداول 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 للمدافعات مبتدئات عن حقوق الإنسان، لم يتعرفن بعد (أو يعرفن القليل) على الممارسات الأمنية الرقمية. بما أنه يشمل تعريفاً بأسس الأمن الرقمي وممارسات تقييم المخاطر، مع التركيز بشكلٍ واضحٍ أيضاً على إستراتيجيات الرعاية الذاتية في الوقت عينه، يعتبر جدول أعمال هذا التدريب مناسباً 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، سيحصّر جدول الأعمال هذا المجموعة للخضوع لتدريب متابعة متوسط المستوى (راجع تدريب متوسط المستوى ممتد على ثلاثة أيام الوارد أدناه)؛ إلا أنه من الممكن استخدامه أيضاً لورشة عمل مستقلة.

- ٠١ التمرين: قواعد اللعبة (تمارين بناء الثقة)
- ٠٢ التمرين: بينغو المدافعات (تمارين بناء الثقة)
- ٠٣ الجلسة: وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)
- ٠٤ التمرين: بمن نثقن؟ (تمارين بناء الثقة)
- ٠٥ الجلسة: حقوقك والتكنولوجيا الخاصة بكنّ (إعادة النظر بعلاقتنا بالتكنولوجيا)
- ٠٦ الجلسة: كيف يعمل الإنترنت؟ (أسس الأمن الرقمي، الجولة الأولى)
- ٠٧ التمرين: أزهار النسويات (تمارين اختتام والمراجعة)
- ٠٨ التمرين: نموذج المخاطر القائمة على الجندر (تحديد الحلّ الأفضل)
- ٠٩ التمرين: فعل الرفض (الرعاية الذاتية)
- ٠١٠ الجلسة: بناء كلمات سرّ قوية (أسس الأمن الرقمي، الجولة الأولى)
- ٠١١ 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 حاسوبك (أسس الأمن الرقمي، الجولة الأولى)
١٥. الجلسة: ماذا يمكن لبياناتك الوصفية أن تفصح عنك؟ (المناصرة الآمنة على الإنترنت)
١٦. التمرين: ماركو بولو (هواتف محمولة أكثر أماناً)
١٧. الجلسة: الهواتف المحمولة، الجزء الأول (هواتف محمولة أكثر أماناً)
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 للدفاعات اللواتي سبق لهن أن خضعن لتدريب تمهيدي (راجعي تدريب متوسط المستوى ممتد على ثلاثة أيام الوارد أعلاه) ويفترض أن يقدم كتدريب متابعة. فستواه التقني أعلى بشكل ملحوظ من جدول أعمال التدريب التمهيدي، ويركز على التطبيقات العملية لمفاهيم الأمن الرقمي، بالإضافة إلى مهارات التفكير النقدي من أجل اتخاذ قرارات مستندة إلى معرفة بشأن استخدام الأدوات. كما يعالج مواضيع معينة بشكلٍ معمقٍ أكثر كعلاقة النساء بالتكنولوجيا والخصوصية والتشفير والمحافظة على سرية الهوية.

في حال كنتن تعملن مع مشاركات من المنظمة ذاتها، سيقدم هذا التدريب لهن أيضاً 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 الحل الأفضل)

-
٥٣. الجلسة: قصتها مع التكنولوجيا (إعادة النظر بعلاقتنا بالتكنولوجيا)
 ٥٤. التمرين: إطرحي عليّ ما تريدينه من أسئلة! (الخصوصية)
 ٥٥. الجلسة: التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟ (الخصوصية)
 ٥٦. الجلسة: الحملات الآمنة على الإنترنت (المناصرة الآمنة على الإنترنت)
 ٥٧. الجلسة: الهواتف المحمولة، الجزء الثاني (أسس الأمن الرقمي، الجولة الأولى)
 ٥٨. الجلسة: تعريف بمسألة التشفير (التشفير)
 ٥٩. الجلسة: التواصل المشفّر (التشفير)
 ٥١٠. التمرين: القدر المعلي (المرجل) (تمارين الختام والمراجعة)
 ٥١١. الجلسة: التخزين والتشفير (أسس الأمن الرقمي، الجولة الثانية)
 ٥١٢. التمرين: الصديقة السرية (الحفاظة على سرية الهوية)
 ٥١٣. الجلسة: الحفاظة على سرية الهوية (الحفاظة على سرية الهوية)
 ٥١٤. الجلسة: القرارات الخاصة بالأمن الرقمي (تحديد الحلّ الأفضل)
 ٥١٥. الجلسة: الخطط والبروتوكولات الأمنية الخاصة بالمنظمة (التخطيط المسبق)
 ٥١٦. 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 للهدافات اللواتي سبق لهن أن خضعن للتدريب التمهيدي والتدريب المتوسط المستوى (راجعى الأمثلة السابقة) وبتن جاهزات لتجربة متقدمة أكثر.

تركز ورشة العمل هذه، التي تعتبر تكتيكية أكثر بطبيعتها مقارنة بالتدريبات السابقة، بدرجة أقل على رفع مستوى المعرفة النظرية إلى مستوى وضع ممارسات خاصة بأدوات معينة. وتركز أكثر على تطبيق مهارات التفكير النقدي وصنع القرارات وفقاً لسيناريوهات تستند إلى الواقع (سيتمكن ذلك كمدريبات من إجراء عمليات تقييم أشمل المدى التقدّم الإجمالي للمجموعة).

- ٠١ التمرين: الفوزيرا! (تمارين الختام والمراجعة)
- ٠٢ الجلسة: المواقع الإلكترونية الأكثر أماناً (المناصرة الآمنة على الإنترنت)
- ٠٣ التمرين: المزيد من الهويات الإلكترونية! (المحافظة على سرية الهوية)
- ٠٤ الجلسة: لنعد إلى خانة الصفر! (أسس الأمن الرقمي، الجولة الثانية)
- ٠٥ التمرين: الاستقصاء عن المعلومات الشخصية الخاصة بالمتصيد (العنف ضد المرأة على الإنترنت)
- ٠٦ الجلسة: الخطط والبروتوكولات الخاصة بالأمن الرقمي: عملية إعادة التطبيق بعد التدريب (التخطيط المسبق)
- ٠٧ التمرين: لسة محبة (الرعاية الذاتية)
- ٠٨ التمرين: خلاصة الأمن الرقمي (تمارين الختام والمراجعة)

باب ٦٠

موارد إضافية

منظمة "حقوق البرمجة"^١

تقود نساء برازيليات منظمة تجري بحثاً 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

<https://codingrights.org>^١

<https://cuidatuinfo.org>^٢

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 بشكل أكبر - في وجه كل المصاعب - من أجل أن يتمكنوا من التمتع بحقوقهم/ن والتمكن من التمتع واللعب وتفكيك النظام الأبوي.

موقع ويكي أمن النوع الاجتماعي 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.

<https://derechosdigitales.org>^٣

<https://feministinternet.org>^٤

<https://gendersec.tacticaltech.org>^٥

<https://karisma.org.co>^٦

مشروع “أنا وظلي”^٧

يساعدكم مشروع “أنا وظلي” من منظمة “تاكتيكل تيك” في التحكم في آثار بياناتكم، ومعرفة ما إذا كنتم تتعرضون للتعقب وتعلم المزيد عن قطاع البيانات.

“انسحاب من برنامج برزيم”^٨

الانسحاب من برامج التجسس على البيانات العالمية مثل برنامج برزيم 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 تعرفت حديثاً على عالم الأمن الرقمي، يمكنك الإطلاع على دلائل التكتيكات التي تتناول المبادئ الأساسية، بما في ذلك النصائح حول كيفية استخدام منصات التواصل الاجتماعي والهواتف المحمولة بشكل أكثر أماناً.

<https://myshadow.org>^٧

<https://prism-break.org>^٨

<https://r3d.mx>^٩

<https://securityinbox.org>^{١٠}

مشروع حماية الذات من المراقبة^{١١}

نصائح وأدوات وإرشادات خاصة بإجراء اتصالات أكثر أماناً على الإنترنت.

مشروع "لنسترجع التكنولوجيا"^{١٢}

هذا المشروع نداء للجمع، ولا سيما النساء والفتيات، لإسترجاع القدرة على التحكم 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 الاجتماعية وأيضاً للأشخاص المهتمين بالتحويلات الاجتماعية والسياسية.

“بلا خوف”^{١٦}

إلى الشارع من دون خوف، أدوات ضد القمع.

العنف على الإنترنت هو عنف أيضاً (فيديو)^{١٧}

العنف على الإنترنت هو عنف أيضاً.

نصائح سريعة بشأن المساحات^{١٨}

نصائح سريعة بشأن تسيير مساحات التعلم حول الأمن الرقمي تراعي الحساسيات الجندرية. دليل وضعه معهد صحافة الحرب والسلام ومنظمة “سوشل تيك” Social، Tic، يتضمن مواد قدمتها إنديرا كورنييليو 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-18>

digital-security.pdf

موقع “لفل أب”^{١٩}

موارد حول التدريب على السلامة الرقمية العالمية.

<https://level-up.cc/>^{١٩}



النساء في فضاء الإنترنت

INSTITUTE FOR
WAR & PEACE REPORTING



مقدمة

باب ٦١

سياسة استخدام البيانات - سايبير ويمن

تمّ تحديث هذه الوثيقة في الرابع من أيلول / سبتمبر 2018.

السياق

قبل الخوض في تفاصيل مُحددة حول كيفية استخدامنا للبيانات التي تم إنشاؤها على هذا الموقع وما يمكنك القيام به لتصبح ضليعاً في كل هذا، سنقدم نظرة عامة عن السياق.

نبذة عن المشروع

تم إنشاء مناهج "سايبير ويمن" وتطويرها من قبل معهد صحافة الحرب والسلام (IWPR) كجزء من مشروع السلامة والتوعية والعمل (SAWA) وتمّ تمويلها من خلال مكتب الديمقراطية وحقوق الإنسان والعمل (DRL) في وزارة الخارجية الأمريكية.

تم تصميم تطبيق الويب وتطويره من قبل منظمة "كيفير" Kéfir، إضافةً إلى واجهة الويب وتصميم الرسوم. وتتولى منظمة "كيفير"، حتى الوقت الحاضر، مسؤولية إدارة الخادم حيث يتم استضافة هذا المشروع.

للاطلاع على المزيد من المعلومات حول مشروع "سايبير ويمين" أنقر هنا.

الحق في الخصوصية

يُعرف الحق في الخصوصية بأنه حق من حقوق الإنسان وهو منصوص عليه بشكل صريح في المادة 12 من الإعلان العالمي لحقوق الإنسان لعام 1948 كما يلي:

"لا يجوز تعريض أحد للتدخل التعسفي في خصوصياته أو أسرته أو منزله أو مراسلاته، أو لجملات على شرفه وسمعته. ولكل شخص حق الحصول على الحماية القانونية من مثل هذه التدخلات أو تلك الجمالات".

القوانين

بصرف النظر عن حقوق الإنسان، هناك قوانين محددة للبيانات. ربما كنت قد سمعت مؤخراً عن القانون العام لحماية البيانات؟ GDPR دخل "القانون العام لحماية البيانات" حيز التنفيذ في 25 أيار / مايو عام 2018. تم تصميم هذا القانون الأوروبي لحماية المواطنين بشكل أفضل من انتهاكات الخصوصية والخروقات التي يمكن أن تتعرض لها البيانات. ويحدد هذا القانون الجديد بشكل عام كيفية تعامل الشركات مع بيانات عملائها.

ولكن، للأسف، لا ينطبق هذا القانون على جميع السياقات ولا يكفي وحده. إذ تتمتع بعض السلطات القضائية بفهم جيد للخصوصية وتغطيها بشكل جيد، أما البعض الآخر فهي متأخرة في هذا المجال. وهناك مجموعات وأشخاص يعملون جاهداً في الخطوط الأمامية من أجل حصول الجميع بشكل متكافئ على الحق في الخصوصية.

ألق نظرة على بيان رابطة الاتصالات التقدمية حول "القانون العام لحماية البيانات".

الامتثال

يجب أن تُوفّر جميع مواقع الويب والمنصات التي يزورها المواطنون والحماية بموجب قوانين حماية البيانات، مستنداً قانونياً إلزامياً يشرح كيف يتم جمع معلومات التعريف الشخصية والاحتفاظ بها ومشاركتها.

معلومات التعريف الشخصية (PII) هي أي معلومات تتعلق بشخص مُحدّد ("موضوع البيانات")؛ وباستخدام هذه المعلومات من الممكن تحديد هذا الشخص بشكل مباشر أو غير مباشر. تشمل معلومات التعريف الشخصية بعض العناصر الحساسة، على سبيل المثال لا الحصر: الاسم، ورقم الضمان الاجتماعي، ورخصة القيادة، وأرقام التعريف الحكومية الأخرى؛ والجنسية، والوضع القانوني، والجنس، والعرق / الإثنية؛ تاريخ ومكان الميلاد؛ وأرقام الهواتف الخلوية المنزلية والشخصية؛ وعنوان البريد الإلكتروني الشخصي وعنوان البريد وعنوان المنزل؛ واليول الدينية؛ والمعلومات المالية، والمعلومات الطبية، ومعلومات حول الإعاقة؛ ومعلومات عن الزوج، والحالة الاجتماعية، ومعلومات عن الأطفال، ومعلومات الاتصال في حالات الطوارئ.

إن جمع واستخدام البيانات ليس بالضرورة أمراً مضرًا. وعادةً، يتم استخدامها لتلبية متطلبات إعداد التقارير القانونية والمتعلقة بالتمويل وتحسين الأدوات. المهمّ هو أن يتم جمع البيانات وتخزينها ومعالجتها ومشاركتها بطريقة شفافة.

التزام "سايبير ويمن" بالخصوصية

بغض النظر عن الالتزام بجد أدنى معين من المعايير، تم تصميم منصة "سايبير ويمن" من قبل بعض الناشطين بهدف تحقيق الخصوصية مع التركيز على قيمتها واعتمادها من حيث الممارسة وكوجهة نظر أخلاقية.

نحن لا نتفادى تحديد الأفراد فحسب، بل نؤمن بعدم توليد بيانات يمكن استخدامها لمصالح لا تتوافق مع مصالح أولئك الذين يزورون هذه المنصة.

عادة، تكون سياسات استخدام البيانات مجردة، ومطبوعة بأحرف صغيرة ومبهمة تماماً. ويعكس هذا الافتقار إلى الشفافية وحسّ المسؤولية بهدف إخفاء التفاصيل الخاصة باستخدام البيانات والتعاون مع أطراف ثالثة قد لا يُحبّدهم المستخدمون.

بالنسبة لـ"ساير ويمين"، تمثل سياسة استخدام البيانات امتداداً للمشروع: فرصة للتعرف على حقنا في الخصوصية، وكيف يمكن أخذها في عين الاعتبار، وما هي التدابير المحددة التي يمكننا تطبيقها.

ما الذي نقوم به

ملفات تعريف الارتباط والتعليمات البرمجية للأطراف الثالثة

عند زيارة صفحة ويب، قد يتم تحميل بعض الأجزاء من الصفحة من مجالات (domains) وخوادم غير تلك التي طلبت زيارتها. هذه ميزة أساسية للنص التشعبي، (hypertext) ولكنها تشكل مشكلة خطيرة بالنسبة للخصوصية. على شبكة الويب الحديثة، غالباً ما تُستخدم الصور والتعليمات البرمجية المضمنة ملفات تعريف الارتباط وطرقاً أخرى لتتبع عادات التصفح (غالباً لعارض الإعلانات). يُطلق على المجالات التي تقوم بذلك اسم "الأطراف الثالثة المتتعبة" "third party trackers".

ملفات تعريف الارتباط الخاصة بالإنترنت هي ملفات نصية يُخزنها موقع الويب في جهاز الكمبيوتر الخاص بك عند زيارتك لهذا الموقع، بحيث "يتذكر" في حال قمت بزيارته في المستقبل معلومات معينة مثل تفضيلاتك اللغوية أو معلومات تسجيل الدخول.

لا تُستخدم منصة "ساير ويمين" ملفات تعريف الارتباط أو أي نوع من التعليمات البرمجية للأطراف الثالثة.

لاتصالات

يجب أن تصف مواقع الويب التي تتضمن نماذج اتصال (contact forms) سبب طلبها لهذه المعلومات وما ستفعله بعد ذلك. على سبيل المثال، إذا كان سيتم استخدامها في رسائل إخبارية أو حفظها في قاعدة بيانات.

لا تُستخدم منصة "ساير ويمين" نماذج الاتصال. لكن يمكن الاتصال بالقيمين على

المشروع على البريد الإلكتروني contacto@cyber-women.com وطلب المعلومات المتعلقة
بالخصوصية على privacy@cyber-women.com.

تمَّ أيضاً إدارة حسابات البريد هذه من قبل “كيفير” التي تلتزم بتطبيق إجراءات الأمن
الحديثة، مع الاحتفاظ بسجلات البيانات الغير قابلة للتحديد والمعلومات الضرورية لعمل نظام
البريد والتي يتم حذفها بعد أسبوع واحد.

يتم الوصول إلى حسابات البريد الإلكتروني عبر بريد الويب (webmail) وعملاء البريد
الإلكتروني، مع الأخذ بعين الاعتبار الممارسات الأمنية المذكورة في المناهج الدراسية.

سجلات وإحصائيات الويب

تقوم الخدمات والتطبيقات التي تعمل عادة على جهاز ما بحفظ نوع ما من السجلات.
ويوفر هذا الأمر بعض المعلومات التي قد تساهم في تحسين الأدوات أو حل المشاكل المحتملة
التي قد تطرأ على هذا الجهاز. هذه المعلومات مفيدة عموماً ولكنها تحتوي على معلومات
تعريف شخصية مثل عناوين بروتوكول الإنترنت IP addresses وأسماء المستخدمين التي يمكن
استخدامها لتحديد سلوك الأشخاص إلى حد ما. ولهذا السبب من المهم إخفاء هوية الأشخاص
في هذه السجلات بطريقة آمنة.

لا تقوم خوادم “كيفير” بتسجيل عناوين بروتوكول الإنترنت، بل تسجل فقط زيارات
على أنها مجهولة المصدر، وتقوم بإزالة هذه المعلومات بعد أسبوع.

تجمع منصة “ساير وبين” بعض الإحصاءات، من خلال <https://sinapsis.kefir.red>،
النسخة الذاتية لبرنامج Piwik/Matomo التي تستضيفها “كيفير”، مما يعني أن معهد صحافة
الحرب والسلام و”كيفير” فقط يستطيعان الوصول إلى هذه البيانات. وتم تكوين هذا البرنامج
بحيث لا يقوم بتسجيل أي معلومات قد تُحدد الزوار الفرديين، مثل عناوين بروتوكول الإنترنت.
أيضاً، يتم تحويل جميع الزيارات الفردية إلى بيانات إحصائية ثم يتم التخلص منها بعد شهر.
يحترم برنامج Matomo أيضاً ميزة “عدم التعقب” “Do-Not-Track” للمتصفحات حيث لا
يتم تسجيل أي معلومات إذا تم استعمالها.

جافا سكريبت Javascript

يستخدم موقع "ساير ويمين" جافا سكريبت.

- zepto.min.js: زيتو Zepto هي مكتبة جافا سكريبت للمتصفحات الحديثة مع واجهة برمجة تطبيقات متوافقة مع jQuery
- agency.js: يستند موقع "ساير ويمين" على نسق Jekyll Agency الذي يعطي قائمة هذا الموقع تصميم مستجيب "Responsive".

إذا قمت بتعطيل JavaScript (باستخدام برنامج معين، أو من خلال ملحق "plugin" معين أو من خلال تكوين المستعرض الخاص بك)، سيستمر الموقع في العمل. أما على أجهزة الشاشة الصغيرة، فستظهر القائمة في أسفل الصفحة.

التغييرات على هذه السياسة

قد يتم تحديث هذا المستند في المستقبل. راجع هذه الصفحة للاطلاع على التحديثات.

جهات الاتصال

يمكن إرسال جميع الأسئلة المتعلقة بسياسة استخدام البيانات إلى privacy@cyberwomen.com.

ما يمكنك القيام به

يمكنك أيضاً المساهمة في الحفاظ على خصوصيتك. كوننا لا نجمع البيانات إلا بموافقتك، ونقوم بتخزينها لفترة محدودة من دون تحديد المصدر ولا نشارك مع الأطراف الثالثة إلا المعلومات العامة بهدف الحصول على التمويل، لا يعني ذلك أن الوسطاء المحتملين الآخرين يعرضون خصوصيتك للخطر.

- اقرأ مناخ "ساير ويمين" واتبع الممارسات الأكثر أماناً
- قم بتثبيت البرنامج المساعد للمتصفح "Privacy browser Badger" الذي يراقب الخصوصية
- قم بتهيئة متصفح Firefox لتعطيل التعقب.

كيف أقوم بتغيير إعدادات ملفات تعريف الارتباط الخاصة بي؟

تسمح معظم متصفحات الويب بالتحكم في معظم ملفات تعريف الارتباط من خلال إعدادات المتصفح. لمعرفة المزيد حول ملفات تعريف الارتباط، بما في ذلك كيفية

معرفة ملفات تعريف الارتباط التي تم تعيينها، قم بزيارة <https://aboutcookies.org> أو
<http://www.allaboutcookies.org/>

تعرف على كيفية إدارة ملفات تعريف الارتباط في المتصفحات الشائعة:

- جوجل كروم Chrome؛ Google
- مايكروسوفت ايدج Edge؛ Microsoft
- موزيلا فايرفوكس Firefox؛ Mozilla
- متصفح الانترنت الخاص بـمايكروسوفت Internet Explorer؛ Microsoft
- أوبرا Opera؛
- أبل سفاري Safari. Apple

للعثور على معلومات تتعلق بالمتصفحات الأخرى، قم بزيارة موقع مطور المتصفح.
لإلغاء تتبع غوغل أناليتكس Google Analytics عبر جميع مواقع الويب، قم بزيارة
<http://tools.google.com/dlpage>.