النساء فى فضاء الإنترنت

INSTITUTE FOR
WAR & PEACE REPORTING
IWPR

المنهاج التدريبي الخاص بالأمن الرقمي الشامل للمدافعات عن حقوق الإنسان

النساء فى فضاء الإنترنت

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

النساء فى فضاء الإنترنت

INSTITUTE FOR
WAR & PEACE REPORTING
I W P R

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 ركّزت بشكلٍ كبير على منظور النوع الاجتماعي (الجندر). ومؤخرًا، بفضل الجهود المبذولة من الحركات النسائية والنسوية حول العالم، بدأت بالظهور موارد خاصة بالأمن الرقمي تركّز على مسألة النوع الاجتماعي (الجندر) ولكن ما زال التنسيق بين مختلف مكونات مجتمع الأمن الرقمي منقوصًا، وهوضروري لتوسيع مجموعة الموارد بشكلٍ إستراتيجي يلبّي ويسدّ 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. إستنادًا إلى خبرتنا في العمل مع هؤلاء النساء، قمنا بوضع محتوى تدريبي خاص بهدف تقديم مقاربة وُضعت

[١] https://www.facebook.com/iwpr.iraq/

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

استخدام منهاج النساء في فضاء الإنترنت

تم تصميم هذا المنهاج وفقًا لنوعين من المستخدمات: النوع الأول النساء المدربات 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 ألعابٍ تفاعليةٍ ومواد مرئية ومسموعة ومرسومة تقدم توجيهات للمدربات حيث يمكن استخدام وحدات هذا المنهاج إما كجلسات مستقلة عن بعضها البعض، وإما كمكونات لورشة عمل تدريبية متكاملة. هذه التركيبة المكونة من وحدات مختلفة تتيح للمدربات أيضًا إمكانية اختيار محتويات معيّنة تناسب حاجات المشاركات في التدريب. من ناحية أخرى، يمكن للمدربات اختيار إتباع الترتيب المقترح للوحدات وتقديم محتوى المنهاج كاملاً من بدايته إلى نهايته حيث سيستوجب ذلك تقريبًا عشرة أيام كاملة. نحن ننصح اللواتي يرغبن في توفير مثل هذا التدريب، بتقسيم مواده 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 الرقمي والشخصي، قبل الإنتقال 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 أورقمية. الهدف من هذه الجلسات هوتمتين قدرة المشاركات على الفعل، وقدرتهن على التحكّم بأمنهن وهوياتهن. وبالتالي، لابد من أن تكون هذه الجلسات موزعة على كل التدريبات كمساحات للعمل والتفكير الفردي والجماعي، عوضًا عن استخدامها كوحدات مستقلة عن بعضها البعض.

وأخيرًا، تتوفر تمارين عدّة في هذا المنهاج – بعضها تمارين خاصة ببناء الثقة يجب تنفيذها في بداية اليوم الأوّل 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 أيضًا موارد خاصة بجلسات المتابعة التي يجب تنفيذها ضمن فترة الستة أشهر المقترحة.

مقاربة نسوية في وضع المنهاج

كما ذكرنا آنفًا، يشتمل هذا المنهاج على رؤية شاملة لمسألة الأمن للمدافعات عن حقوق الإنسان. بما في ذلك ثلاثية الأمن الرقمي والأمن الجسدي والرعاية الذاتية؛ ولكن جوهر التدريب يركّز على الأمن الرقمي. ولإدخال مقاربة نسوية تراعي مسألة الجندر، وضع هذا المنهاج إستنادًا 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. فغالبًا ما تكون المشاركات في تدريبات حول الأمن الرقمي آتيات من بيئات جغرافية وعاطفية فيها مستوى مرتفع من الإجهاد أوالقلق، وغالبًا ما تكون المدافعات عن حقوق الإنسان عرضة للتحرّش والعنف على الإنترنت وفي الواقع. لابد للنساء المشاركات أن يشعرن أن التدريب مكانٌ آمنٌ ومريح. يشعرن فيه أنهن قادرات على مشاركة مخاوفهن وشكوكهن وأحاسيسهن من دون قلق. ويتمكنّ فيه من المشاركة والتفاعل مع الأخريات، لذلك، هذا المنهاج مخصص للمدربات النساء العاملات مع مشاركات نساء. ولكننا نشجّع المدربين الرجال أيضًا 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. إدراكًا منّا أن جميع النساء المشاركات في ورشة عمل ما لا تعتبرن أنفسهن نسويات. تركّز مقاربة 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. وثانيًا عبر طرح أمثلة عن العنف القائم على النوع الاجتماعي (الجندر) 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 يسّهل على المشاركات عملية فهم الحالات المختلفة وبالتالي فهم أهميتها في بيئتهن. رأينا أن اعتماد هذه المقاربة يمكّن النساء المشاركات من ممارسة المهارات الجديدة بإنتظام 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 هوالتركيز على "التفكير الإستراتيجي بشأن الأمن الرقمي" – أي مشاركة مفاهيم في مجال الأمن الرقمي مع المشاركات، عوضًا عن الإكتفاء بالتدريب على لائحة من الأدوات, لذلك خُصص وقت طويل جدًا لتعريف المشاركات بمفاهيم الأمن الرقمي، كالتشفير وإخفاء الهوية والخصوصية والبرمجيات المفتوحة المصدر قبل التدرّب على استخدام 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 تحديدًا. 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 تركّز على مشاركة التجارب وتحديد نقاط الضعف التي تواجهها المشاركات ليس فقط لكونهن نساء ,بل أيضًا 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 أيضًا في هذه الحالة – الهدف من هذه الجلسة مساعدة المشاركات على الإستعداد والتعامل مع الهجمات الرقمية. يأتي هذا المنهاج ليساعد في تقديم معلومات للمشاركات لتتمكنّ 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 أوالمتحرش ,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 اعتماد عادات جيدة في مجال الأمن الرقمي، قد تصبح بدورها جزءًا 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 اكتساب فهم جيّد لحاجات الأمن الرقمي الخاصة بالمشاركات والمساعدة في ضمان توفير تدريب فعّال وتجربة تعلّم لكل ما هومناسب لأهداف وبيئة المشاركات. من شأن معرفة كيفية استخدام المشاركات المحتملات للتكنولوجيا، وكيفية تواصلهن بواسطتها وتحديد ما يعرفنه مسبقًا عن الأمن الرقمي، أن تؤثر بشكلٍ ملحوظ على نطاق المحتوى المقدّم في التدريب.

تقييم الحاجات والمحفزات

يفضّل أن تجري المدربات تقييمًا للحاجات قبل التدريب، من خلال العمل إما مع المشاركات في التدريب أنفسهن وإما مع عضوة ممثلة لمنظمتهن. لا تنسوا أنه إلى جانب ضرورة تقييم حاجات المشاركات بشكلٍ موضوعيّ، لابد أيضًا من فهم محفزات مشاركتهن في التدريب –

هل تسعى المشاركات بشكلٍ فاعل لتحسين قدرتهن على الصمود، أوأنهن يطلبن المساعدة نتيجة حوادث تعرضن لها مؤخرًا أوما زالت مستمرة؟ إضافة إلى ذلك، من وجهة نظر عملية، من شأن معرفة الوقت المتوفر لديكن أن يساعدكن في النهاية على تحديد كمّ المحتوى الذي ستقدّمنه في ورشة عمل واحدة (أوورشات عمل متتالية)؛ وسيتوضح ذلك لكنّ أكثر بفضل مستوى المهارات الجماعي للمشاركات.

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

ما هي خلفية منظمتهن؟ ما شكل تنظيم فريق عمل منظمتهن؟ ما هي البرامج و/أوالنشاطات الأساسية التي تنظمها منظمتهن؟ ما هي بعض الممارسات المرتبطة بالتكنولوجيا التي يعتمدنها؟ كيف ومن أين يحصلن على الإنترنت؟ ما هونوع أوأنواع الحواسيب و/أوالأجهزة المحمولة التي يستخدمنها؟ هل يستخدمن أجهزة منفصلة للعمل والإستعمال الشخصي؟ ما هي أنظمة التشغيل التي يستخدمنها؟ من هي الحركات أوالمجموعات الأخرى التي يتعاونّ معها؟ قد يتم ذلك من خلال ممثل لمنظمتهن (مثلاً كأعضاء تحالف ما) أوبصفة شخصية كناشطات مستقلات. هل سبق لهن أن تعرضن لحوادث أوتهديدات مباشرة لأمنهن الجسدي أوالرقمي؟ قد يرتبط ذلك بأجهزتهن أوبمعداتهن أوبحساباتهن الإلكترونية أوبإعتداء جسدي.

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

في حال أتيحت لكنّ فرصة إجراء عملية تقييم شاملة للمشاركات في التدريب في الوقت الذي يسبق ورشة عملكن، سوف نتوفر أداة بناء قدرات الأمن الرقمي ضمن هذا المنهاج. هذه الأداة مورد قام المعهد بإنتاجه واستخدامه 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 بآلية إحتساب كمي لإختبار المشاركات، من أجل تحديد مستوى مهاراتهن في مجال الأمن الرقمي من جهة، ومن جهة أخرى توفر معلومات نوعية عن نقاط القوّة والمجالات 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 الملاحق[1]

إستراتيجيات التقييم البديلة

في حال العجز عن إجراء عملية تقييم قبل التدريب بشكلٍ مباشر، أوفي 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، أوالمنظمات يجرين عملاً مشابهًا في المنطقة ذاتها التي تعمل فيها المجموعة أوالمجموعات التي ستعملن معها، سيكون من المرجّح أنها تواجه مخاطر أوهجمات مشابهة في طبيعتها لتلك التي تواجهنها المشاركات في تدريبكن. إضافة إلى ذلك، قد تتوفر بعض المخاطر أوالحوادث المعروفة التي يمكنكن ربطها بنوع العمل الذي تقوم به المشاركات في تدريبكن (وبمكان قيامهن به). في حال كنتن ستدربن محاميات توفرن المشورة القانونية لمدافعات أخريات عن حقوق الإنسان، أولصحافيات يفضحن فساد الحكومة، قد تتمكنّ من إجراء بحوث حول بعض التكتيكات التي تستخدمها أوإستخدمتها الحكومات أوبعض الجهات غير الحكومية في بلدهنّ في الماضي ضد أفراد، ولا سيما النساء ممن يقمن بعمل مشابه.

[1] https://cyber-women.com/ar/DISC/

باب ٣

شكر وتقدير

الكتّاب: كُتب 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

التنسيق وصلة التواصل مع معهد صحافة الحرب والسلام: أليخاندرا غارسيا

التعليم والترجمة: نيكولاس سيرا-ليفا

الترجمة إلى الإسبانية: ناديج لوكاس بيريز

تنسيق التعلّم من الند للند والجلسات التجريبية: إستيلا سوريا

خدمات استشارية: تعاونية تيرا كومون[١]

تطوير الموقع وتصميم الرسوم وإنتاج الوسائط: تعاونية كيفير[٢]

[١] https://tierracomun.org/

[٢] https://kefir.red

المراجعات والمتعاونات: عزّة سلطان، كارول واترز، داليا عثمان من تعاونية تاكتيكل تكنولوجي وإستريلا سوريا، إريكا سميث من جمعية "بروغريسف كوميونيكاشنز"، جيجي ألفورد، جينيفر شولتي، لورا كونينغاهم، ليندسي آندرسن، ميغان دوبلوا من إنترنيوز وساندرا أوردونييس.

تم تطوير بعض الجلسات والمعلومات الأخرى في هذا المنهاج من قبل: جمعية "بروغريسف كوميونيكاشنز"، تعاونية تاكتيكل تكنولوجي، مؤسسة كاريزما، "موخيريس أل بوردي"، إليس موروي من تعاونية "سوبفيرسيونس"، داناه بويد، ماريل غارسيا، أليكس دون، سبيروس موناستيريوتيس، في.

النساء فى فضاء الإنترنت

تمارين بناء الثقة

باب ٤

قواعد اللعبة

- **الأهداف:** في هذا التمرين، ستقمن بشكلٍ جماعي بوضع اتفاقات التعايش والمشاركة الخاصة بتدريبكن أي "قواعد اللعبة" مع المشاركات.
- **الطول:** من 8 إلى 10 دقائق
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - الحلوى المخادعة (تمارين بناء الثقة)
  - بينغو المدافعات (تمارين بناء الثقة)
- **المواد اللازمة:**
  - لوح ورقيّ (أولوح أسود أوأبيض)
  - أقلام خطاطة
  - ملصقات ملوّنة (ثلاثة ألوان - يفضّل أن تكون الأحمرأوالزهري الأصفر والأخضر)

- **التوصيات:** الجزء الثاني من هذا التمرين – "إشارات السير" – ينفذ بشكلٍ أفضل إذا كانت المشاركات مزودات ببطاقات عليها أسماؤهن يمكنهن وضع الملصقات الملوّنة عليها (راجعن الإرشادات).

إدارة التمرين

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

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

الجزء الأوّل – قواعد اللعبة

١. إشرحن باقتضاب الخلفية المذكورة أعلاه للمشاركات، ومن بعدها أطلبن منهن تقديم أمثلة عن اتفاقات تعايش يشعرن أنها مهمة وضرورية لضمان راحتهن طيلة فترة ورشة العمل. يمكنكن البدء بمثال تقدمنه 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 إذنكن".

٢. على لوح ورقي أو لوح أسود أوأبيض، أكتبن كل إتفاق تتفق عليه المجموعة فورًا. وما أن تشعرن بأنها كافية، إقرأن كل الاتفاقات بصوتٍ عالٍ – إسئلن المشاركات إن كانت قواعد التعايش الخاصة بالمجموعة هذه تناسبهن. ما لم يُذكر ذلك سابقًا أو في حال عرضتن ذلك كمثال أوليّ عن الاتفاقات هذه، من شأن الإتفاق حول استخدام الحواسيب والهواتف خلال الجلسات أن يساعدكن أيضًا.

٣. ذكرن المجموعة بأن هذه الاتفاقات ستبقى معروضة وواضحة طيلة فترة التدريب، وأنهن قادرات على تعديلها في أي وقت كان بعد المناقشة والإتفاق على ذلك مع كافة أعضاء المجموعة. إحرصن أيضًا 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 الاتفاقات على لائحتكن قد توفر مستويات متفاوتة من الراحة ضمن المجموعة. بالنسبة لهذه الاتفاقات، كتلك المرتبطة بالتماس الجسدي أو التصوير، يفضل أن تقدمن للمشاركات طريقة لتحديد معايير الراحة الخاصة بهن لمشاركتها مع بعضهن البعض.

٥. وزعن الملصقات الملوّنة لكل مشاركة من المشاركات، مع الحرص على إعطائهن ملصقات 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 ينصّ 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 ملوّنة مرتبطة بذلك الإتفاق – على سبيل المثال:

الأحمر/الزهري: "التماس الجسدي يضايقني 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 اختيار ملصقة ملوّنة خاصة بهن تتناسب 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 الإثنين أو ثلاثة. في حال وجود أكثر من إثنتين أو أكثر، أطلبن من المشاركات كتابة حرف خاص بكل واحدة منها (مثلاً: "تاء" للتماس الجسدي أو"صاد" للصور).

المراجع:

باب ٥

بينغو المدافعات

- **الأهداف:** ستبدأن أنتن والمشاركات بالتعريف عن أنفسكن لبعضكن البعض في تمرين كسر الجليد هذا، المصمم على شكل لعبة تفاعلية تشجّع المشاركات على
- **الطول:** من 12 إلى 15 دقيقة (وفقًا لعدد أعضاء المجموعة)
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - الحلوى المخادعة (تمارين بناء الثقة)
- **المواد اللازمة:**
  - جداول بينغولكل مشاركة (معبئة مسبقًا بأسماء المشاركات)
  - بطاقات كرتون بيضاء
  - أقلام/أقلام رصاص (العدد الكافي لكل المشاركات)

إدارة التمرين

قد تكون عملية تذكر الأسماء والتعرّف على الوجوه عملية صعبّة بالنسبة لبعض الأشخاص مقارنة بالأشخاص الآخرين. تمرين "كسر الجليد" هذا سيساعد المشاركات على تذكّر هذه التفاصيل وفي الوقت عينه سيتيح لهن 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 مسبقًا بأسماء كل المشاركات (راجعن المثل الوارد أدناه) – يمكنكن أيضًا إضافة أسماؤكن على الأوراق إذا أردتن ذلك.

مثال عن ورقة بينغو معدّة مسبقًا:

شفيقة	زينة	سميرة
جولييت	منى	فاطمة
نهى	فرح	صوفيا
ماريا	سارة	ليلى

٣. إشرحن للمجموعة قواعد سير اللعبة:

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

أثناء قراءتكن للأسماء، ستقوم المشاركات بوضع دائرة حول كل إسم وارد على أوراق البينغو الموجودة معهن.

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

٤. أطلبن من الفائزة قراءة اسم المشاركة الأولى من الصف الرابح بصوت عالٍ – على

المشاركة المذكورة الوقوف وترداد أسمها ومن ثمّ إضافة تفصيل ما (إخترن هذا التفصيل مسبقًا وأطلعنهن بذلك كجزء من إرشاداتكن) على سبيل المثال نشاط تحب أن تقوم به في أوقات فراغها، أوفيلمها المفضّل أوأغنيتها المفضلة أوطبقها 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 إستخدمنها في الخطوة رقم 3 وضعنها جانبًا.

٦. بعد أن تنتهي الفائزة من منادة الأسماء الواردة في السطر الفائز، إشكرنهن ومن ثمّ إقرأن 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 وأيضًا إختتمن التمرين بتذكير المجموعة بأنكن ستبدأن بخوض غمار مغامرة جديدة معًا، وأن معرفة والتعرّف على كل عضوة من عضوات المجموعة ضروري لضمان نجاح مغامرتكن.

اختياري: بنهاية التمرين،إامنحن 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 أيضًا على ذلك (وهذا عنصر إيجابي دومًا في عملية التدريب!)

باب ٦

الحلوى المخادعة

- **الأهداف:** ستبدأن أنتن والمشاركات بالتعريف عن أنفسكن لبعضكن البعض خلال تمرين كسر الجليد هذا، المصمم على شكل لعبة تفاعلية تشجّع المشاركات على التعرّف على بعضهن البعض بدون الإكتفاء بمعرفة الأسماء.
- **الطول:** من 5 إلى 8 دقيقة (وفقًا لعدد المشاركات في المجموعة)
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - قواعد اللعبة (تمارين بناء الثقة)
- **المواد اللازمة:**
  - كيس أو كيسين من قطع الحلوى الصغيرة

إدارة التمرين

١. قدمن الحلوى لكل المجموعة وقلن لهن أن يأخذن ما طاب لهن منها. بعض المشاركات ستأخذن عددًا كبيرًا والبعض الآخر ستأخذن عددا أقل. ويمكنكن أيضًا أخذ بعضٍ من الحلوي.

٢. ما إن يأخذ الجميع بعضًا من قطع الحلوى، إكشفن عن "الخدعة" للجميع , حيث لكل قطعة أخذنها، 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 يتمتعن به في عملهن

بلد أو مكان يرغبن في زيارته

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

الغلاف الأحمر = أمنيات أو أهداف شخصية

الغلاف الأخضر = أمر ما يتمتعن به في عملهن

الغلاف الأزرق = بلد أو مكان يرغبن في زيارته

باب ٧

بمن تثقن

- **الأهداف:** في هذا التمرين، ستوجّهن المشاركات في عملية تفكير بهدف 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 ستتمكنّ من مواءمة محتوى الجلسات المختلفة بشكلٍ أفضل مع بيئاتهن الخاصة.
- **الطول:** 15 دقيقة
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - الخطط والبروتوكولات الأمنية الخاصة بالمنظمة (التخطيط المسبق)
  - الخطط والبروتوكلات الخاصة بالأمن الرقمي: عملية إعادة التطبيق بعد التدريب (التخطيط المسبق)
  - نموذج المخاطر القائمة على الجندر (تحديد الحلّ الأفضل)
- **المواد اللازمة:**

- أوراق كبيرة متعددة من أوراق اللوح الورقيّ.

إدارة التمرين

١. 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

٢. إعطين الجميع 5 دقائق للإجابة عن الأسئلة التالية بشكلٍ فرديّ؛ وأثناء قيامهن بذلك، أطلبن منهن أيضًا تحديد ما إذا كانت إجابتهن على كل سؤال ستتغير إذا أجبن عليها في بيئتهن الشخصية في مقابل الإجابة عنها في سياق عملهن/نشاطهن:

بمن نثقن؟

بمن تعتقدن أنكن قادرات على الوثوق في ما يتعلّق بمعلوماتكن؟

بمن تعتقدن أنكن غير قادرات على الوثوق في ما يتعلّق 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.

٣. ما إن ينتهي الوقت المخصص، قسمن المشاركات إلى مجموعات صغيرة من 3 إلى 4 أشخاص كحد أقصى لمناقشة إجاباتهن مع بعضهن البعض – بعد مرور 10 دقائق، على كل مجموعة أن تشارك مع المجموعات الأخرى ما ناقشنه.

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

إعادة النظر بعلاقتنا بالتكنولوجيا

باب ٨

وجهات النظر الشخصية حيال الأمن

- **الأهداف:** ستقدمن في هذه الجلسة مفهوم الأمن الشامل للمشاركات، حيث أن كل واحدة منهن تأتي إلى قاعة التدريب بحوافزها وأسباب رفضها وعوائقها وأفكارها المسبقة الشخصية المرتبطة بالأمن الرقمي والجندر والتكنولوجيا. ستشجّع هذه الجلسة المشاركات على تحديد معنى مفهوم "الأمن" بالنسبة لهن كأفراد.
- **الطول:** 90 دقيقة
- **الشكل:** Session
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - بمن نثقن؟ (تمارين بناء الثقة)
  - حقوقكن والتكنولوجيا الخاصة بكنّ (إعادة النظر بعلاقتنا بالتكنولوجيا)
  - نموذج المخاطر القائمة على الجندر (تحديد الحلّ الأفضل)
- **المواد اللازمة:**
  - أوراق مسطّرة أو غير مسطّرة بقياس (٤أ) A4 (إعطين أكثر من ورقة واحدة

لكل مشاركة)
- شرائح (فيها النقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
- أوراق اللوح ورقيّ

إدارة التمرين

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

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

ما هي السلامة بالنسبة لكن؟

ما هو الأمن بالنسبة لكن؟

ما الذي يجعلكن تشعرن بالأمن والأمان؟

في أي مجالات تعتقدن أنه يمكن تطبيق هذين المفهومين؟

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

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

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

عناصر الأمن الشامل الثلاث

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

الجزء الثاني – ما هو الأمن الرقمي بالنسبة لكن؟

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

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

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

الجزء الثالث – تحديد الحوافز وأسباب الرفض والحواجز

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

ما السبب الذي يدفعهن للتعرّف أكثر على مسألة الأمن الرقمي؟

ما هي الأسباب الشخصية التي دفعتهن لحضور ورشة العمل؟

ما الذي يتوقعن الحصول عليه من هذا التدريب؟

هل لديهن أسباب شخصية تدفعهن إلى رفض الأمن الرقمي؟

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

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

الجزء الرابع – المعتقدات الخاطئة المتداولة بشأن الأمن الرقمي والجندر والتكنولوجيا

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

الرفض والحواجز التي حددتها المشاركات في القسم السابق:

١. "الأمن الرقمي صعب."

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

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

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

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

مسيرة الأمن الرقمي التي سنبدأ بخوض غمارها الآن، هدفها تزويدكن بالمعلومات

التي تحتجن إليها لإتخاذ القرارات الصحيحة المناسب بشأن أمنكن الرقمي والتي تركز بشكلٍ أكبر على تعلّم المزيد عن المنصات التي نستخدمها أصلاً، وتداعيات اختيار أدوات أوممارسات معيّنة على أنفسنا وعلى عملنا، وعلى تحسين الطرق التي نستخدم فيها التكنولوجيا في حياتنا اليومية.

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

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

٤. "لا أعرف شيئًا عن الأمن الرقمي!"

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

حياتهن الشخصية.

اختياري: بالنسبة لهذا المعتقد بالذات، من المفيد أن تخصصن بضع دقائق تطلبن فيها من المشاركات تقديم أمثلة عن ممارسات سبق لهن أن طبقنها ومتعلقة بالأمن الرقمي. أكتبن هذه الممارسات على ورقة من أوراق اللوح الورقيّ لتكون معروضة أمام المجموعة وإعرضنها في مكان واضح للعودة إليها طيلة فترة التدريب.

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

الأمن الرقمي لا يقتصر فقط على ما تقمن به على الإنترنت – فالممارسات خارج الإنترنت، كالإطلاع بشكلٍ دوري على المعلومات (الأرقام والصور والمستندات والملفات الصوتية وملفات الفيديو... إلخ) التي خُزنت من قبلكن على حاسوبكن وهواتفكن الذكية (و"غير" الذكية) ومفاتيح اليواس بي، بالإضافة إلى الإدراك الجسدي لمكان وجود أجهزتكن أو لمن لديه إمكانية الوصول إليها مهمة بالقدر ذاته – حتى لولم تكن متصلة بالإنترنت. لابد أيضًا من معرفة التطبيقات والبرمجيات المثبتة على أجهزتكن – لأنه أحيانًا، من أجل الوصول إلى معلومات معيّنة على الأجهزة، قد نضطر لتثبيت تطبيقات جديدة 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 تكنولوجي" Tactical Technology "أنا وظلي" [1]:

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

قد تظنن أنه ليس لديكن ما تخفينه، ولكن فكرن لبرهة بأنواع المعلومات التي

تشاركنها: مع معن تتكلمن أوتتواصلن بشأنها؟ ما هي القنوات التي تستخدمنها للقيام بذلك؟ هل هذه القنوات عامة أو متاحة بطريقة أخرى أمام الجميع للإطلاع عليها؟

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

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

الجزء الخامس – الملاحظات الختامية

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

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

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

نحن وحدنا فقط نعرف ممارسات الأمن الرقمي المناسبة لنا، ونحن وحدنا الأقدر على

اختيار الممارسات الأفضل التي تعتبر مناسبة للتطبيق من الناحية العملية.

اختياري: في حال كان تدريبكن سيدرج ذلك كنتيجة مرغوبٍ بها فأن الوقت الآن مناسب لتشرحن للمشاركات أنهن سيكتبن خططهن الفردية الخاصة بالممارسات والأدوات التي سيطبقنها خلال تقدمكن معًا في المسيرة التدريبية. يجب أن تتضمن مثل هذه الخطط الأهداف الشخصية التي ستشجعهن على التقدّم بسرعتهن الخاصة.

المراجع

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

باب ٩

حقوقكن والتكنولوجيا الخاصة بكن

- **الأهداف:** يتخلل هذه الجلسة نقاش حول العلاقة بين الحقوق والتكنولوجيا – ستساعدن حينها المشاركات على تحديد التهديدات المحدقة بحقوقهن ومن ثمّ سيتعرفن على بعض مفاهيم الأمن الرقمي الأساسية ذات الصلة.
- **الطول:** 50 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)
  - بمن نثقن؟ (تمارين بناء الثقة)
  - تعريف بمسألة التشفير (التشفير)
  - المحافظة على سريّة الهوية (المحافظة على سريّة الهوية)
  - الخصوصية (الخصوصية)
  - كيف يعمل الإنترنت؟ (أسس الأمن الرقمي)

- إنترنت نسوي (العنف على الإنترنت ضد النساء)

- **المواد اللازمة:**
  - أوراق لوح ورقيّ.
  - أقلام خطاطة ملوّنة
  - نسخ عن تقارير ومقالات عن الحقوق الرقمية من بلدان أو مناطق المشاركات (نسخة واحدة لكل 3 إلى 4 مشاركات)
- **التوصيات:** أوراق لوح ورقيّ. أقلام خطاطة ملوّنة نسخ عن تقارير ومقالات عن الحقوق الرقمية من بلدان أو مناطق المشاركات (نسخة واحدة لكل 3 إلى 4 مشاركات)

إدارة الجلسة

الجزء الأوّل – ربط الحقوق بالتكنولوجيا

١. قسمن المشاركات إلى مجموعات صغيرة من 3 إلى 4 أشخاص كحد أقصى، ومن ثمّ أعطين كل مجموعة ورقة كبيرة أو ورقتين كبيرتين من أوراق اللوح الورقيّ وبعض الأقلام الخطاطة. ستحظى كل مجموعة بعشر دقائق للتفكير في لائحة من حقوق الإنسان - مهمة الاختيار والتعريف بهذه الحقوق تعود إلي اختيار كل مجموعة- عليهن كتابتها على ورقة اللوح الورقي.

٢. بعد أن تنتهي مهلة العشر دقائق هذه، ستطلبن من كل مجموعة النظر إلى اللائحة التي قامت المجموعة بوضعها – يتوجب عليهن الآن مناقشة علاقة حقوق الإنسان هذه بالتكنولوجيا خلال عشر دقائق أخرى (على سبيل المثال، "ما أثر التكنولوجيا على حقوق الإنسان؟"). لتوضيح المسألة، يمكنكن تقديم مثال عبر رسم الصلة بين التكنولوجيا وحق من حقوق الإنسان وارد على لائحة إحدى المجموعات. يمكنهن كتابتها على ورقة كبيرة أخرى إذا أردن ذلك، ولكن ذلك ليس ضروريًا.

٣. بعد أن تنتهي مدة العشر دقائق الأخرى، شاركن مع كل مجموعة رزمة معدّة سابقًا من التقارير والمقالات عن الحقوق الرقمية (راجعن قسم المواد اللازمة). إعطين كل مجموعة مدة 15 دقيقة ليقمن 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. إشرحن للمشاركات أن التقارير التي تم تقديمها لهن هي مجرد أدوات إرشادية ففي حال كنّ يعرفن بحالات أو تهديدات أخرى، يمكنهن إضافتها أيضًا.

٤. ما إن تنتهي مدة الخمسة عشرة دقيقة، إعطين المشاركات إستراحة قصيرة ومن ثمّ أطلبن من كل مجموعة تقديم عملها لبقية المشاركات بشكلٍ 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 تذكيرهن 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 بجلسة "وجهات النظر الشخصية حيال الأمن" من هذه الوحدة، لا تنسين أن تفكرن أيضًا 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 الأوّل، إشرحن للمشاركات أنكن ستقدمن لهن بعض مفاهيم الأمن الرقمي الجوهرية بالإضافة إلى تداعيات ملموسة على الحقوق: المحافظة على سريّة الهوية والخصوصية والتشفير. في بعض البيئات، قد يكون إدخال مسألة الالتفاف والإفلات من المراقبة (circumvention) أيضًا ضروريًا كأحد هذه الأمثلة.

٨. إبدأن بتذكير المشاركات بمدى أهمية قيامهن بهذه الخطوة الضرورية بإتجاه معالجة مسألة

أمنهن الرقمي عبر هذا التدريب، وأنهن الآن سيبدأن بمسيرة تعلّم كيفية مواجهة بعض التهديدات المحدقة بهن:

في حال سبق لكن أن غطيتن جلسة وجهات النظر الشخصية حيال الأمن من هذه الوحدة، إستذكرن 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 إستنادًا إلى خبرتكن الخاصة.

٩. أطلبن من المشاركات التطوّع 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. كرّرن المرحلة التاسعة ولكن عالجن مفهوم المحافظة على سريّة الهوية هذه المرّة – أطلبن من المشاركات تفسير ما يعنيه لهن مفهوم المحافظة على سريّة الهوية، وإشرحنه أووضحن بإيجاز أي شكوك قد تساور المشاركات بواسطة أمثلة ممكنة أو مناسبة قدر الإمكان. ويتوجب عليكن مرّة أخرى إيجاد طرق لتشجيع المشاركات على إستعادة حقهن بالمحافظة على سريّة الهوية، وإحرصن أيضًا على توضيح الفوارق بين الخصوصية والمحافظة على سريّة الهوية كمفهومين منفصلين.

١١. بعد الإنتهاء من النقاشات والشروحات السابقة عن الخصوصية والمحافظة على سريّة 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 وقمن بربطها بالنقاشات السابقة حول الحقوق الرقمية والخصوصية والمحافظة على سريّة الهوية.

١٢. لإختتام هذه الجلسة، إقترحن بعض المنظمات التي تقدم الدعم والمناصرة للحقوق

الرقمية في بلدان أو مناطق المشاركات، لكي يتمكّن من البحث عنها والتعرّف عليها بأنفسهن – على سبيل المثال، في حال كنتن تعملن مع "فرونتلاين ديفندرز" Front-line Defenders، "إلكترونيك فرونتيرز فاونداشن" EFF، لجنة حماية الصحفيين CPJ، "أيفكس" ifex، " منظمة تاكتيكل تكنولوجي كوليكتيف Tactical Technology Collective، منظمة تبادل الإعلام الاجتماعي SMEX، "آي ركس" IREX، و"إنترنيوز" 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 جندري مضرّ.
- **الطول:** 20 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - إنترنت نسوي (العنف على الإنترنت ضد النساء)
  - الحكواتيات (تمارين الختام والمراجعة)
- **المواد اللازمة:**

- صور نساء مختلفات من عالم التكنولوجيا (مع الأسماء)
- نبذة عن كل إمرأة (كمرجع للمدربات)
- خيط أو حبل (بطول مترٍ واحد)
- مشابك/ملاقط ملابس أو ملاقط حديديّة (واحد أو إثنين لكل صورة)

• **التوصيات:** المستند التالي عبارة عن مرجع غنيّ بقصص متنوعة عن نجاحات النساء في التكنواوجيا مناسب لهذه الجلسة (باللغة العربية): https://www.cyber-arabs.com/wp-content/uploads/2018/02/10-ي ف-ت ادئار-ءاس ن-pdf.اي ج ول ون ك ت ل ا

إدارة الجلسة

١. إشرحن للمشاركات أن هذه الجلسة ستكون بمثابة تمرين للمجموعة لإنشاء ذاكرة جماعية تقرّ وتعترف 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 بعيدًا 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؟

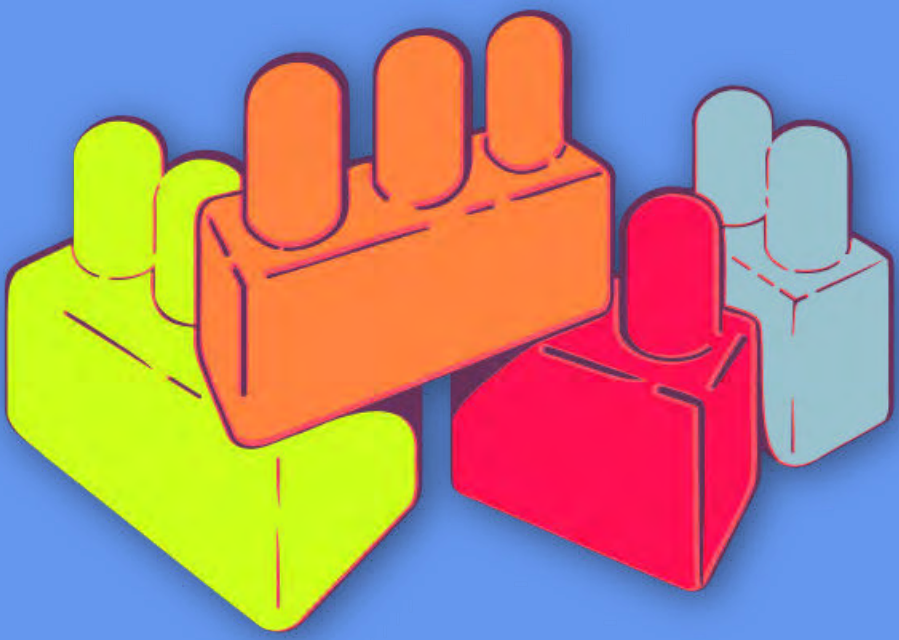
٣. أطلبن من المشاركات مشاركة قصصهن مع التكنولوجيا التي تظهر قوتهن وقدرتهن على المقاومة. يمكنكن البدء بطرح الأسئلة التالية على المجموعة – ماذا تعني التكنولوجيا لكنّ؟ هل هي أمرٌ إيجابيّ أم سلبيّ؟ ومن بعد ذلك، شاركن قصتكن الشخصية أوقصة ملفتة عن التكنولوجيا كمثال – قد يشجع ذلك المشاركات على الشعور بالإرتياح والإنفتاح.

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

٥. بواسطة الملاقط/المشابك الحديدية أو الخشبية ثبتن الصور على الحبل، وأطلبن من المجموعة العمل معًا على ترتيب النساء بالترتيب الزمني الصحيح من أجل إنشاء جدول زمني خاص بقصة أو تاريخ النساء مع التكنولوجيا؛ على سبيل المثال، من الممكن ترتيبها وفقًا لتواريخ ولادتهن أو وفقًا للسنة التي حققن فيها أنجازهن الأوّل في مجال التكنولوجيا – إحرصن أن تكون المعلومات اللازمة متاحة للمجموعة لكي تتمكّن 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 معلقًا 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 معلقًا 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 أومشاركتين 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 ثمّ تقمن بمشاركة قصص كل النساء على الجدول الزمني.



أسس الأمن الرقمي | الجولة الأولى

باب ١١

كيف يعمل الإنترنت؟

- **الأهداف:** إطلاع المشاركات على كيفية فهم تدفق المعلومات عبر الإنترنت والثغرات ونقاط الضعف المختلفة والممارسات الأمنية الجيدّة المناسبة لكل نقطة من نقاط السلسلة.
- **الطول:** 60 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - technology your rights, Your حقوقكن والتكنولوجيا الخاصة بكن
- **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

+ (حاسوب/هاتف محمول) + عدد2 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 توزّع فيها إقتراحات لممارسات الأمن الرقمي
- ورقة تستخدم كلوح – ورقة كبيرة (4 أمتار)، وورقتين أصغر حجمًا (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 تعلمن عنها وأن يشعرن بأنهن يمتلكن الآن المعلومات اللازمة للتحرّك 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 ماريل غارسيا Mariel Garcia من منظمة سوشل تي آي سي SocialTIC وسبيروس موناستيريوتيس Spyros Monastiriotis من منظمة تاكتيكل تكنولوجي كوليكتيف Tactical Technology Collective

إدارة الجلسة

الجزء الأوّل – كيف يعمل الإنترنت – تدفق المعلومات ونقاط الضعف.

١. سيبدأ هذا الجزء من ورشة العمل بلعبة. ستعطى المشاركات أوراق تمثّل جزءًا من السلسلة التي يسلكها تدفق المعلومات على الإنترنت (المودم، الحاسوب مبنى الشركة المقدمة لخدمة الإنترنت... إلخ) وسيطلب منهن ترتيب أنفسهن وفقًا للترتيب الذي يعتبرن أنه يمثّل الترتيب الصحيح للطريق الذي تسلكه رسالة بريد إلكتروني عبر الإنترنت للوصول إلى حاسوب آخر.

٢. بعد أن ترتب المجموعة مواقعها، ستقوم الميسّرات بتصحيح الأخطاء في حال وجودها وستشرحن 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 الميسّرة تغيير رسوم البريد الإكتروني المستخدمة وتغيير النقطة التي يبدأ منها الشرح. على المدربات أيضًا منح الوقت الكافي لتبديد الشكوك المرتبطة بهذه العملية.

٣. يمكنكن أيضًا استخدام فيديو كهذا

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

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

لمساعدة المشاركات على تحديد الأخطاء التي ارتكبنها في الترتيب الذي وضعنه بأنفسهن.

اختياري: لتكييف هذا التمرين لدى إجرائه مع مجموعات أكبر – بدل إعطاء ورقة واحدة لكل شخص، اعطين ورقة واحدة لكل شخصين؛ بالنسبة للمجموعات الأقل عددًا، يمكنهن وضع الأوراق على الأرض ومناقشة الترتيب الصحيح في ما بينهن.

الجزء الثاني – نقاط الضعف

٤. بعد الإنتهاء من العملية السابقة، سيطلب من المشاركات لصق كل ورقة على ورقة كبيرة جدًا ستترك على الأرض. عندها، ستقوم الميسّرات 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 أيضًا إضافة ممارسات أو تهديدات أخرى قابلة للتطبيق في بيئتكن أو لابد من إطلاع المشاركات عليها. يمكن أيضًا تقديم بعض الأمثلة عن الممارسات التي تعتمدها 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 السرّ ورسائل التصيّد، 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 وإقتراح حلول مبتكرة لها. ولجعل ذلك أقلّ صعوبة للمشاركات الأقل خبرة.ستعطى كل مجموعة ورقة عليها حل مقترح لبدء النقاش.

بنهاية التمرين، ستعطى المجموعات مدّة من 30 ثانية إلى دقيقة لتقديم أفكارها (وفي الوقت عينه تقوم إحدى الميسّرات بتدوين الملاحظات وتدخل إضافات إلى ما سبق وتم التحدث عنه). ستتنقل الميسّرات بين المجموعات لتقديم شروحات موجزة والإجابة على الأسئلة، وتحفيز النقاشات بين جميع المشاركات.

مع تقدّم سير النشاط ,لابد 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:

انعدام الأمن المادي: يفضل التخفيف من عرض الأجهزة في منظمتكن للغرباء انعدام 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 اللافتات التي يرد عليها كلمة سرّ شبكة الإنترنت اللاسلكي الخاصة بالمنظمة رصد وسرقة المعلومات عبر إشارة شبكة الإنترنت اللاسلكي WiFi sniffing: تغيير كلمة سرّ شبكة الإنترنت اللاسلكي الخاصة بكن بشكل دوري(يفضل مرة كل أسبوعين) انعدام التشفير: البدء في استخدام أدوات وتقنيات تشفير مأمونة انعدام 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 الرقمية لمعرفة الطرق القانونية التي يمكن من خلالها حماية أنفسكن. طلبات البيانات والبيانات الوصفية من الحكومات المحلية/الوطنية: التعرّف على القوانين النافذة في بلدكن التي تتناول موضوع التدخّل في الاتصالات. المراقبة الدولية: الإنتقال إلى استخدام خدمات آمنة لإجراء عمليات البحث وإرسال الرسائل وإستضافة المواقع والاتصالات بشكلٍ عام. انعدام أمن كلمة السرّ: استخدام كلمات سرّ طويلة ومعقدة! انعدام أمن كلمة السرّ: استخدام خدمة"كي باس" KeePass لعدم نسيان كلمات السرّ المتعددة التي تستخدمنها التصيّد: التفكير قبل الضغط على أي زر (يجب أن تفكرن في المنصات التي تدخلن فيها معلومات تسجيل الدخول الخاصة بكن) استخدام شبكة الإنترنت اللاسلكي الخاصة بالآخرين: تسجيل الدخول على حساباتكن الشخصية دومًا بشكل يدوي بدلا من حفظ كلمات السر الخاصة بكن على هذه الشبكات. كما يجب تذكر تسجيل الخروج من الحسابات الخاصة بكن بعد الانتهاء من استخدامها. استخدام شبكة

الإنترنت اللاسلكي الخاصة بالآخرين: الإنتباه للأمور التي يجب ألا تثرنها أوتبحثن عنها في محركات البحث حين تستخدمن شبكة الإنترنت اللاسلكي الخاص بأشخاص آخرين برمجيات خبيثة: تثبيت برمجيات مكافحة للفيروسات وتشغيلها يدويًا 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 أوبرمجية "سي سي كلينر" CCleaner

الجزء الرابع – الموارد والمسائل العالقة

٦. الهدف من هذا الجزء من الجلسة هوجمع الأسئلة المرتبطة بالأمن الرقمي التي لربما لم تطرح حتى الآن خلال ورشة العمل، بالإضافة إلى مناقشة مواضيع مرتبطة بالمجتمع المحلي الخاص بالمشاركات. هذا وقت مناسب لتوفير الموراد للجميع لتعلّم المزيد والبقاء على إطلاع بالمستجدات في مجال الأمن الرقمي. ستجمع الميسّرات الأسئلة من الحضور وتلمّح إلى الإجابات المحتملة وتذكر المراجع التي يمكن استخدامها لإيجاد الإجابات. 7.

المراجع

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

باب ١٢

بناء كلمات سرّ قويّة

- **الأهداف:** في هذه الجلسة، ستقمن مع المشاركات بمراجعة تداعيات سرقة كلمة سرّ، وكيفية تعرضها للسرقة عادةً، وكيفية إنشاء كلمات سر أقوى، واكتساب عادات أفضل خاصة بكلمات السرّ.
- **الطول:** 45 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - كيف يعمل الإنترنت؟ (أسس الأمن الرقمي،الجولة الأولى)
  - كيفية حماية حاسوبكن (أسس الأمن الرقمي،الجولة الأولى)
- **المواد اللازمة:**
  - جهاز عرض
  - شرائح
  - أوراق

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

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

إدارة الجلسة

الجزء الأوّل - المقدمة

١. إبدأن هذه الجلسة بطرح الأسئلة التالية على المشاركات:

متى كانت المرة الأخيرة التي قمن بها بتغيير أي من كلمات سرّهن؟

هل لديهن كلمات سرّ مختلفة لحساباتهن المختلفة؟

هل كلمات سرّهن مكتوبة على أوراق ملصقة في مكان ما؟

هل قمن 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 المشاركات 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 شخصٌ 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.

غالبًا ما تحتوي هذه الحسابات على معلومات حساسة، ونحن في الغالب نتصرف على سجيتنا 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 علي كلمات سر الأشخاص الآخرين تسمح بإنتحال صفاتهم/ن الشخصية- فأي شخص قادر على الوصول إلى كلمة سرّ حساب ما، يمكنه فعليًا التصرّف على الإنترنت وكأنه صاحب الحساب.

تمنح كلمات السرّ أيضًا إمكانية الوصول إلى عدد من الأمور الأخرى – نقاط التواصل مع شبكة الإنترنت اللاسلكية وفك كلمات سر الأجهزة المحمولة وتسجيل الدخول إلى الحواسيب وفكّ 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 لائحة بكل المنصات التي يتذكرن أنه لديهن حسابات عليها. والآن أطلبن من المشاركات وضع لائحة بما قد يحصل في حال إستحوذ أحدهم على كلمة سرّهن وتمكن من الدخول إلى حساباتهن أو أجهزتهن:

قد تتعرض معلومات أو ملفات مهمة للسرقة (للنسخ) أو للحذف، في حال تعرضها للسرقة، قد لا تلاحظن ذلك مباشرة. وقد تكون المعلومات المسروقة أي شئ مثل مستندات أو ملفات مهمة أو حساسة جدًا أو قائمة جهات اتصال أو رسائل بريدية

إلكترونية.

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

يمكن استخدام حسابات البريد الإلكتروني أومواقع التواصل الاجتماعي لإرسال الرسائل المزعجة أو لانتحال شخصيتكن أو شخصية أصدقائكن أو أفراد عائلتكن أو زملائكن.

قد تصبح إمكانية الدخول إلي حساباتكن محتجزة إلى أن تقمن بدفع شكل من أشكال "الفدية" – قد يتضمن ذلك، دفع المال أو منح إمكانية وصول إلى جهات اتصال أو إلى حسابات أخرى.

قد يستخدم شخص ما كلمة السرّ الموجودة بحوزته للوصول إلى اتصالاتكن ونشاطاتكن ومراقبتها من دون علمكن.

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

الجزء الرابع – كيفية تعرّض كلمات السرّ للسرقة عادةً؟

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

حين تشاركنها مع الآخرين، أو تخزنّها بطريقة سهلة الكشف – من ضمن الأمثلة الشائعة، كتابة كلمة السرّ الخاص بتسجيل الدخول إلى حاسوبكن على ورقة صغير ملصقة على الحاسوب نفسه أو بالقرب منه. حين يرى أحدهم كلمة السرّ أثناء إدخالها على شاشتكن ويكتبها أو يحفظها عن غيب.

في حال استخدام مقدم لخدمة البريد الإلكتروني من دون بروتوكول طبقة المنافذ الآمنة (https) على مدى الجلسة، أو استخدامه 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 يدويًا، أما كلمات السرّ فيمكن الحصول عليها من خلال خاصيتيّ "احفظ كلمة سرّي" "Save My Password" أو "تذكرني" "Remember Me" الموجودتين على مواقع إلكترونية من خلال أي متصفح – يصبح ذلك ممكنًا بشكلٍ خاص في حال لا يتم استخدام تشفير شامل للقرص على أي جهاز. البرمجيات الخبيثة كبرمجيات "كي لوغر" keylogger التي تعمل على توثيق كل نقرة على لوح المفاتيح على جهازٍ ما ومن ثمّ إرسالها لطرف آخر يريد هذه المعلومات. هذه البرمجيات الخبيثة ليست قادرة على كشف كلمات السرّ وحسب بل قد تصل أيضًا إلى معلومات حساسة أو شخصية. من الممكن أيضًا إختراق المنصات أو نقاط الضعف الموجودة في أنظمتها مما يتسبب بكشف معلومات مستخدميها.

الجزء الخامس – كيف يمكننا جعل كلمات سرّنا أقوى؟

٦. إشرحن للمشاركات أنه في حال استخدامنا كلمات السرّ ذاتها لكل الحسابات، وتعرّض إحداها للسرقة، ستصبح كل حساباتنا مكشوفة. شاركن بعض ميزات كلمات السرّ الأكثر أمنًا وقوةً مع المجموعة:

الطول: بكل بساطة، كلما زاد طول كلمة السرّ كلما صارت أفضل! يوصى باستخدام 14 حرفًا كحدٍ أدنى للحصول على كلمات سرّ قوية وفي حال استخدام 20 حرفًا تصبح كلمة السرّ أقوى بكثير.

التعقيد: إستخدمن كلمة سرّ فيها أحرف وأرقام مع أحرف كبيرة وصغيرة مع تشكيلة غنيّة من الأرقام والرموز.

التغيير المستمر: غيّرن كلمات سركن بشكلٍ دوريّ، لا سيما تلك الخاصة بحساباتكن الحساسة، ولابد من تغييرها في حال وصلتكن رسائل بريدية موثوقٍ بها (ليست رسائل تصيّد) تنذركن بأن حسابات المستخدمين آخرين وكلمات السرّ لديهم تعرّضت للسرقة.

استخدام جمل سرّ بدلا عن كلمات السر (تخيلن كلمات سرّ مرتبطة ببعضها ضمن جملة) مثال آخرى عن ممارسة كلمات سرّ قوية – إليكن بعض الأمثلة:

SayNoToSexualHarassmentInMiddleEast ("لا للتحرش الجنسي في الشرق الأوسط")

MyRightToDecentShelter ("حقي في مسكن لائق)

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

٧. أطلبن 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 معيّن 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 معرّضة لأنواع مختلفة من البرمجيات الخبيثة، في سياق المخاطر المحدقة عادةً بالمدافعات عن حقوق الإنسان.
- **الطول:** 30 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - كيف يعمل الإنترنت؟ (أسس الأمن الرقمي،الجولة الأولى)
  - كيفية حماية حاسوبكن (أسس الأمن الرقمي،الجولة الأولى)
  - لنعد إلى خانة الصفر! (أسس الأمن الرقمي،الجولة الثانية)
- **المواد اللازمة:**
  - شرائح (مع االنقاط المفتاحية الواردة أدناه)
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز العرض

- **التوصيات:** يفضل أن تتبع هذه الجلسة، جلسة كيفية حماية حاسوبكن، الموجودة في هذه الوحدة أيضًا.

إدارة الجلسة

الجزء الأوّل – تعريف بالبرمجيات الخبيثة

١. إشرحن للمشاركات ماهية البرمجيات الخبيثة وراجعن معهن بعض أنواع بالبرمجيات الخبيثة الموجودة – كحد أدنى، يوصى بأن تغطى 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 بشكلٍ متزايد؛ في حال كنتن تعملن مع مجموعة من النساء لابد من معالجة هذه البرمجيات بالذات. على نحوٍمماثل، إحرصن بشكلٍ عام على إدراج دراسات حالات وأمثلة عن برمجيات خبيثة تواجهها المشاركات في تدريبكن ضمن بيئتهن.

الجزء الثاني – كيف يمكن أن نتعرضن للإصابة بها؟

٢. فسرن بعض الطرق الشائعة التي قد تصبح أجهزتكن من خلالها مصابة ببرمجية خبيثة، وما هي الممارسات غير الآمنة التي قد تؤدي إلى مثل هذه الإصابات. لابد أيضًا 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 االتصالاتهن.

بعض الأنواع الأخرى تستهدف أفرادًا 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. إختتمن الجلسة بمشاركة بعض الأمثلة عن سيناريوهات إصابة ببرمجيات خبيثة تواجهها عادةً النساء والمدافعات عن حقوق الإنسان، يمكنكن مشاركة دراسات حالات معيّنة 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 بيئتكن أيضًا:

تلقت إمرأة 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 "مشفّرًا" وظهرت رسالة على شاشاتها تطالبها بتسديد مبلغ مالي مقابل أن تستعيد إمكانية الوصول إلى معلوماتها.

باب ١٤

التصفّح الآمن

- **الأهداف:** توفر هذه الجلسة مقدمة حول ممارسات تصفّح الإنترنت الآمنة، بما في ذلك لمحة عامة عن البرامج المضافة والمنافع الأخرى الممكن استخدامها لإنشاء بيئة تصفّح أكثر أمانًا.
- **الطول:** 45 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - كيف يعمل الإنترنت؟ (أسس الأمن الرقمي،الجولة الأولى)
  - كيفية حماية حاسوبكن (أسس الأمن الرقمي،الجولة الأولى)
- **المواد اللازمة:**
  - شرائح (مع النقاط المفتاحية الواردة أدناه)
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز العرض
  - إمكانية اتصال بشبكة إنترنت لاسلكي

إدارة الجلسة

الجزء الأول – اختيار المتصفّح

١. إبدأن الجلسة بسؤال المشاركات عن متصفحات الإنترنت التي يستخدمنها والخيارات الأخرى التي سمعن عنها. قدمن لهن متصفّح فايرفوكس Firefox – إشرحن فوائد استخدامه وناقشن بإيجاز الفرق بينه وبين المتصفحات الشائعة الأخرى من قبيل غوغل كروم Google Chrome أو إنترنت إكسبلورير Internet Explorer.

اختياري: عند العمل مع النساء الناطقات باللغة العربية، قد تجدن هذا الفيدي ومفيدا لبدء النقاش.

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

الجزء الثاني – ممارسات التصفّح الأكثر أمانًا

٢. تتوفر بعض ممارسات التصفّح الأكثر أمانًا التي يمكنكن مناقشتها مع المشاركات – ومع أنكن غير مضطرات للتحدث عنها جميعها معهن، يوصى بأن تشاركن ما يكفي لإعطاء المشاركات خيارات متنوعة (لا تنسين أيضًا أن تحرصن على أن يكون المحتوى مناسبًا ومهماً لبيئة المشاركات).

٣. إشرحن للمجموعة أنكن ستقمن بمراجعة بعض ممارسات التصفّح الآمن معهن، ولكن لن تركزن الآن على أدوات محددة غير المتصفحات بحد ذاتها. بعض المشاركات قد يرغبن منذ هذه اللحظة بتغيير المتصفحات التي يستخدمنها ولكن الأخريات قد لا يكن جاهزات لذلك – لذا قبل مناقشة بعض الأدوات المحددة كالبرامج المضافة إلى المتصفحات، لابد من إبقاء تركيز النقاش على الممارسة في البدايةً.

إليكن بعض الممارسات التي يمكنكن طرحها للنقاش:

البقاء متيقظات تجاه محاولات التصيّد والتصيّد المستهدف.

حجب الإعلانات المضمنة (embedded ads) والإعلانات المفاجئة. (pop-up ads)

معرفة كيفية عمل ملفات تعريف الإرتباط (كوكيز) - إحرصن على التحدث عن مدى تسهيلها للتصفّح ولكن أيضًا عن سلبياتها.

تعطيل ومحو ملفات تعريف الإرتباط من المتصفحات.

محو سجل التصفّح؛

عدم حفظ كلمات السرّ في إعدادات متصفحكن.

التحقق من البرامج المضافة التي قمتن بإضافتها إلى متصفحكن.

تشغيل خيار "عدم التعقّب" (Do Not Track) في متصفحكن.

استخدام بدائل عن محرّك بحث غوغل (مثل دك دك غو Duck Duck Go)

معرفة من يقوم بالتعقّب على الإنترنت ولماذا؟ (كلا الرابطين الموردين أدناه جيدين عن هذه المسألة https://trackography.org/ و https://www.mozilla.org/es-MX/lightbeam/)؛

ناقشن الفرق بين HTTP و HTTPS؛

ما هي الشبكات الافتراضية الخاصة ومتى يجب استخدامها؟

كيف يعمل بالظبط التصفّح المتخفي (Incognito Mode or Private Browsing)، ومتى يجب استخدامه؟

الجزء الثالث - الأدوات والبرامج المضافة من أجل تصفّح أكثر أمانًا

٤. إشرحن، بعد أن عالجتن بعض الممارسات الأساسية للتصفّح الآمن، أنه يمكنكن أيضًا إقتراح أدوات معيّنة - البرامج المضافة بالتحديد - التي قد تساعد أو تسهّل عملية اعتماد

بعض تلك الممارسات تلقائيًا.

٥. قدمن لهن الأدوات التالية، شارحاتٍ لهن كيفية عمل كل واحدة منها، ولا تنسين أيضًا مشاركة الروابط اللازمة لتنزيلها مع المشاركات. لابد أن تفهم المشاركات أهمية وفائدة كل أداة تمت مشاركتها معهنّ؛ ففي حال لم تشرحنها بشكلٍ واضح، قد يؤدي ذلك إلى إتخاذ المشاركات قرارات مبنية على معلومات خاطئة بشأن خصوصيتهن أوإخفاء هويتهن على الإنترنت.

أدوات متصفح سطح المكتب

أداة "نو سكريبت" [١](NoScript)

أداة "آدبلوك بلس" [٢](AdBlock Plus)

أداة "برايفيسي بادجر" [٣](Privacy Badger)

أداة "إيتش تي تي بي إس إفريوير" [٤](HTTPS Everywhere)

أداة "كليك أند كلين" [٥](Click & Clean)

متصفّح "تور" [٦](Tor)

أداة "يوبلوك" [٧](uBlock)

أداة "ديسكونكت" [٨](Disconnect)

---

١ https://noscript.net/
٢ https://adblockplus.org/es/
٣ https://www.eff.org/es/privacybadger
٤ https://www.eff.org/https-everywhere
٥ https://www.hotcleaner.com/
٦ https://www.torproject.org/download/download-easy.html.en
٧ https://www.ublock.org/
٨ https://disconnect.me/

أداة "يومايتركس" [٩](uMatrix)

أدوات متصفحات الهواتف المحمولة

أداة "إيتش تي تي بي إس إفريوير" [١٠](HTTPS Everywhere)

مكافح الفيروسات "أفاست" [١١]Avast

أداة "أورفوكس" [١٢](Orfox)

أداة "أوربوت" [١٣](Orbot)

متصفح "تور" [١٤](Tor) لهاتف آيفون

ممارسات وميزات أخرى

التصفّح المتخفي (Incognito Mode/InPrivate Mode)

غالبًا ما تتسبب هذه الميزة بالإلتباس لأنها غير مفهومة بشكلٍ مناسب – وقد لا يتوفر لدى المشاركات فكرة واضحة عن كيفية عمل التصفّح المتخفي كميزة من ميزات المتصفحات ومتى يكون استخدامها مفيدًا. فسّرن لهن كيفية عمل ميزة التصفّح (والميزات المشابهة)، وقدمن لهن بعض الأمثلة عن الحالات التي قد تكون فيها هذه الميزات مفيدة فعليًا.

الممارسات الآمنة على شبكة الإنترنت اللاسكي

[٩] https://addons.mozilla.org/es/firefox/addon/umatrix/

[١٠] https://www.eff.org/https-everywhere

[١١] https://www.avast.com

[١٢] https://guardianproject.info/apps/orfox/

[١٣] https://www.torproject.org/docs/android.html.en

[١٤] https://mike.tig.as/onionbrowser/

ختامًا، ناقشن لبعض الوقت، وقدمن شرحًا إذا أمكن، لبعض الممارسات الآمنة الأساسية الخاصة بالاتصال بشبكات الإنترنت اللاسكي - يتضمن ذلك ممارسات كتغيير كلمات السرّ المحددة مسبقًا 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 حاسوبكن

- **الأهداف:** تحديد الممارسات السليمة للمحافظة على سلامة حواسيبنا.
- **الطول:** 50 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - كيف يعمل الإنترنت؟ (أسس الأمن الرقمي،الجولة الأولى)
  - التصفّح الآمن (أسس الأمن الرقمي،الجولة الأولى)
  - البرمجيات والفيروسات (أسس الأمن الرقمي،الجولة الأولى)
  - التخزين والتشفير (أسس الأمن الرقمي،الجولة الثانية)
- **المواد اللازمة:**
  - شرائح (مع النقاط المفتاحية الواردة أدناه)
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز العرض
  - نسخ مطبوعة عن نموذج متابعة النسخ الإحتياطي الوارد أدناه

- **التوصيات:** يوصى بأن تقمن بشرح مباشر – بواسطة جهاز عرض متصل بحاسوبكن – عن الأدوات التي تخترن التحدث عنها في هذه الجلسة، لكي تتمكن المشاركات من المتابعة والتدرّب على استخدامها على حواسيبهن الخاصة من خلال استخدام ملفات غير مهمة أنشئت لأغراض هذه الجلسة (وليس ملفات أو بيانات مهمة فعليًا!)

إدارة الجلسة

الجزء الأوّل – 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 يخصصن لصيانة أجهزتهن؟ غالبًا ما يكون الفرق بين مدى تقدير الناس لأجهزتهم وكم الوقت الذي يخصصونه لصيانتها والإعتناء بها كبيرًا جدًا. إشرحن للمجموعة أن هذه الجلسة ستركز على الممارسات الأساسية الخاصة بحماية الأجهزة.

الجزء الثاني – المحيط المادي والصيانة

٣. أخبرن المجموعة أن عددًا 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 التخلّص من الأوساخ أو الرواسب التي قد تتكدس داخل الجهاز، وإجراء عمليات تحقق دورية لتحديد ما إذا كان الجهاز قد تعرّض لأي تعديلات مادية أو محاولات تطفّل ماديّة. في هذا الصدد، يمكنكن التوصية باعتماد ممارسات رقمية أساسية – كاستخدام كلمة سرّ لإقفال الجهاز في حال لم يكنّ في حوذتكن بعد

إغلاقه – بالإضافة إلى أدوات الحماية المادية، كاستخدام حامي لوح المفاتيح (keyboard protector) أو سلك ضد سرقة لوحة المفاتيح (an anti-theft cable chain) لمنع أي سرقة أوإمكانية وصول غير مرغوبٍ بها. إحرصن على أن تشرن هنا إلى أن أهم جانب من جوانب سلامة أجهزتهن المادية هو الوعي. لابد من معرفة مكان وجود جهازٍ ما في أي لحظة – إما بحوزتهن وإما في غرفة أخرى وإما في مكان آمنٍ آخر.

٤. أطلبن من المشاركات إستذكار 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؟ إليكن بعض الجوانب المهمة الأخرى المرتبطة بالوعي – الوعي المادي لا يقتصر فقط على الحرص بألا يصل أي خصم إلى أجهزتهن بل يتضمن أيضًا الضرر المحتمل الذي يتسبب به المكان الذي يتواجد فيه الجهاز.

الجزء الثالث – سلامة البرمجيات

٥. إشرحن للمشاركات مخاطر استخدام برمجيات مقرصنة (من عيوب البرمجيات المقرصنة أنها تؤدي إلي إحتمالية أكبر لتحميل برمجيات خبيثة في أجهزتكن، ولايمكن إجراء عمليات تحديث دورية بالطريقة ذاتها التي تعتمدها البرمجيات المرخّصة... إلخ)؛ إلا أن البرمجيات المرخصة قد تكون باهظة الثمن في معظم الأحيان لذلك يمكنكن عندها مشاركة بعض الموارد مع المجموعة التي قد تساعد في معالجة هذه المشكلة مثل:

أوسلت Osalt[1]

افتحن متصفحًا وإبحثن عن "أوسلت" – هذا موقع إلكتروني يقدّم بدائل مجانية ومفتوحة المصدر لمعظم منصات البرمجيات المهمة المرخّصة (مثلاً استخدام نظام أوبونتو Ubuntu بدل عن نظام ويندوز Windows؛ ليبر أوفيس LibreOffice بدل

[1] http://www.osalt.com

عن برنامج مايكروسوفت وورد Microsoft Office، إنكسكايب InkScape بدل عن أدوبي إلستراتور Adobe Illustrator).

تك سوب TechSoup[٢]

بواسطة "تك سوب"، يصبح المدافعون والمدافعات عن حقوق الإنسان ومنظماتهم مخوّلين 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 المتبرّع بها – الرابط أعلاه يحتوي على قائمة بالشركاء والدول التي يعملون بها.

٦. إشرحن للمشاركات أهمية المحافظة على كافة برمجياتهن محدّثة – 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 المنزّلة مباشرة من أدوبي وليس من مواقع أخرى.

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

استخدام 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.

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

[٢] http://www.techsoupglobal.org/network

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:

استخدام البرنامج المضاف على المتصفحات "يوبلوك" uBlock لتفادي النقر على إعلانات قد تؤدي إلى تنزيل ملفات برمجيات خبيثة على حاسوبهن. التنبه لمحاولات التصيّد، وللروابط أو الملفات المرفقة المشبوهة الموجودة في رسائل بريد إلكتروني بشكلٍ خاص، والتي تبدو أنها أُرسلت من حسابات غير معروفة أو حسابات تبدو وكأنها مشابهة لجهات اتصال موثوقٍ بها. هذه فرصة سانحة جيدة للأتيان على ذكر جدران الحماية Firewalls – حيثُ تقدم جدران الحماية طبقة تلقائية من الحماية على حواسيبهن. شاركن أدوات من قبيل "كومودو فايروول" Comodo Firewall و"زون ألارم" ZoneAlarm و"غلاسوايز" e.Glasswir نسخ أحدث (مرخّصة) لنظاميّ التشغيل ويندوز وماك تتمتع بجدران حماية قوية مثبتة أصلاً.

الجزء الرابع – حماية البيانات والنسخ الاحتياطية

٩. إسألن المشاركات – كم مرة قمن بإنشاء نسخ احتياطية لملفاتهن؟ شاركن أمثلة عن أفضل الممارسات المرتبطة بإنشاء نسخ احتياطية للبيانات، على غرار الإحتفاظ بالنسخ الاحتياطية في مكان آمن منفصل عن حاسوبهن، وإنشاء نسخ احتياطية لمعلوماتهن بشكلٍ دوري ومعتاد – بحسب المعلومات التي أنشئت لها نسخ احتياطية – والتفكير أيضًا في تشفير القرص الصلب أو وسيلة التخزين حيث ستُخزن البيانات.

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

نموذج متابعة النسخ الإحتياطي

نوع المعلومات
الأهمية/القيمة
ما وتيرة إنتاجها أو تغييرها؟
كم مرة في الشهر/السنة يجب إنشاء نسخ احتياطية عنها؟

١١. فسّرن بعد ذلك، أنه على الرغم من توفر أدوات تقوم بنسخ احتياطية بشكلٍ تلقائي (على غرار Duplicati.com أو كوبيان Cobian)، ولكنه يسهل عليهن البدء بإنشاء نسخهن الاحتياطية يدويًا عبر وضع الملفات في وسيلة التخزين الاحتياطية. هذا يعتمد في النهاية على مدى تعقيد أو كمية البيانات التي يتوجب عليهن التعامل معها – بالنسبة للمستخدم العادي غالبًا ما تكون عملية إنشاء النسخ الاحتياطية يدويًا أكثر من كافية.

١٢. لمتابعة النسخ الاحتياطية المحمية للبيانات، راجعن بإيجاز مفهوم تشفير وسائل التخزين. إشرحن للمشاركات ما يعني القيام بذلك، ولماذا يعتبر تشفير أقراصهن الصلبة أو وسيلة التخزين مفيدًا. تعتبر خدمتي "فيراكريبت" VeraCrypt و"ماك كيبر" MacKeeper من الخدمات الشائعة نسبيًا التي يستعان بها لتشفير الملفات أو الأقراص ويمكن ذكرها في هذا السياق كخيارات تستطيع المشاركات اعتمادها.

الجزء الخامس – حذف الملفات إستعادتها

١٣. إقرأن بصوتٍ عالٍ الجملة التالية:

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

إسألن المجموعة عن رأيها بتلك الجملة – هل هذه الجملة منطقيّة؟ كيف يمكن ألا تكون هذه الخاصية موجودة فعلاً؟ ذكرن المشاركات أنهن قادرات على توصيل الملف إلى سلّة المهملات على سطح مكتب حاسوبهن ومن ثمّ إفراغ السلّة، ولكن هذه العملية تقتصر

فقط على إزالة رمز الملف وإزالة أسم الملف من الفهرس المخبّأ الخاص بكل شيء على حاسوبهن ومن ثمّ 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، تمامًا كخزانة ملفات أزيلت فيها كل بطاقات التعريّف 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 أيضًا أدوات يمكن استخدامها لحذف الملفات بشكلٍ دائم (وليس فقط إزالتها من فهرس الملفات إلى أن تُشغل المساحة الشاغرة). إغتنمن هذه الفرصة لتقديم برمجية "سي كلينر" CCleaner، و/أو برمجية "إيرازر" Eraser، و/أو برمجية "بليتش بت" Bleachbit، كأدوات يمكن استخدامها لحذف الملفات وبرمجية "ريكوفا" Recuva كخيار 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-antiviru s-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
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - الخصوصية (الخصوصية)
  - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟ (الخصوصية)
- **المواد اللازمة:**
  - شرائح أوبطاقات عليها أسئلة ترد أدناه
- **التوصيات:** لابد من مشاركة الإرشادات تدريجيًا مع المشاركات مع التقدم في التمرين، 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 الموضوعة من قبل إليس مونروي Elis Monroy من مجموعة "سوبفرسيونس" Subversiones لمشروع "صوت النساء".

إدارة الجلسة

١. أطلبن من المشاركات اختيار شريكة من المجموعة ومن ثمّ أن يجدن مكانًا هادئًا للتحدث معها.

٢. بعد أن تجلس كل مشاركة مع شريكتها، أطلبن منهن مشاركة الإجابات على الأسئلة التالية في ما بينهما:

ما هي الحادثة الأطرف أو الأكثر إحراجًا التي واجهتها في حياتكِ؟ أذكري أمرًا واحدًا تكرهين القيام به.

هل تتمتعين بسماع موسيقى ليست مألوفة بالضرورة؟

هل كان لديك لقبًا عندما كنت طفلة؟

كمدربات، يمكنكن إضافة أو تغيير هذه الأسئلة كما ترونه مناسبًا – الهدف هو طرح أسئلة يرجّح أن تثير معلومات أو قصص قد تكون محرجة أو مضحكة والتحدث عن الخصوصية مع المشاركات. يمكنكن أيضًا الإستعانة بأسئلة شخصية أكثر ولكن يجب أن تنتبهن إلى خياراتكن بحسب البيئة التي تتواجدن فيها، إذ حتمًا لا ترغبن في إشعار المشاركات بالإنزعاج.

٣. بعد أن تنتهي المشاركات من تبادل الإجابات مع بعضهن البعض، أطلبن من كل شريكتين الإنضمام إلى شريكتين جديدتين (يجب أن تتألف كل مجموعة الآن من أربع مشاركات)

٤. أطلبن من المشاركات ضمن المجموعات الجديدة التي شكلنها التعريف بالشريكة التي عملن معها خلال الجولة الأولى، ومشاركة الإجابات على كل الأسئلة مع المشاركات

في مجموعاتهن الجديدة.

٥. بعد أن تنتهي المجموعات المؤلفة من أربع مشاركات من تعريف بعضهن البعض على قصص الأخريات، يمكنكن 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 تشتمل:

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

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

باب ١٧

الخصوصية

- **الأهداف:** تعريف المشاركات بمفهوم الخصوصية والمعلومات المحددة لهويتنا المتوفرة على الإنترنت.
- **الطول:** 50 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - حقوقكن والتكنولوجيا الخاصة بكنّ (إعادة النظر بعلاقتنا بالتكنولوجيا)
  - إطرحي عليي ما تريدينه من أسئلة! (الخصوصية)
  - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟ (الخصوصية)
  - الجمهور الشبكي (الخصوصية)
  - الاستقصاء عن المعلومات الشخصية الخاصة بالمتصيد (العنف ضد المرأة على الإنترنت)
- **المواد اللازمة:**
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض

- شرائح (عليها النقاط المفتاحية الواردة أدناه)

• **التوصيات:** بعض المشاركات قد يشعرن 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 يجدنها. 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 "تاكتيكل تكنولوجي" Tactical Technology "الهدوء وفن جعل التكنولوجيا تعمل لصالحك"

إدارة الجلسة

الجزء الأوّل – هل نتمتع فعلاً بالخصوصية؟

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

٢. أطلبن من المشاركات مشاركة بعض الأمثلة عن عوامل قد تؤثر على قدرتهن على التحكّم ببياناتهن ومعلوماتهن الشخصية وعناصر أخرى. قد تكون تلك العوامل ممارسات شخصية أو منصات يضعن معلوماتهن بعهدتها أوالمعرفة التي يتمتعن بها بشأن الأدوات والأجهزة التي يستخدمنها أو ما يقوم به الآخرون في شبكاتهم.

الجزء الثاني – "الاستقصاء عن الذات" Self Doxxing

٣. إشرحن للمشاركات معنى الاستقصاء عن المعلومات الشخصية Doxxing- بشكلٍ أساسي، هو القيام بجمع كميات كبيرة من المعلومات الشخصية عن شخص ما ومن ثمّ نشرها للعموم (عادةً على الإنترنت). يجب أن تفسرن أيضًا كيفية استخدام الاستقصاء هذا ضد بعض الأشخاص كتكتيك إنتقامي 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 سيتدربن على عملية "الاستقصاء عن الذات" كطريقة لإكتشاف كم ونوع المعلومات التي يمكن إيجادها عن أنفسهن على الإنترنت. إشرحن لهن أن هذا تدبير 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 متصفحًا لا يستخدمنه عادةً – وذلك لكي لا يُسجّل دخولهن تلقائيًا إلى حساباتهن المختلفة.

٦. أطلبن من المشاركات، قبل أن يبدأن بذلك، وضع قائمة بكل الحسابات العامة وصفحات وسائل التواصل الاجتماعي الخاصة بهن؛ ومن ثمّ أطلبن منهن وضع لائحة بالكلمات أو الجمل الرئيسية التي قد تكون مرتبطة بهن، والتي قد تتضمن معلومات من قبيل: المدينة التي ولدن فيها المدينة التي يقطنّ فيها عنوان منزلهن المنظمة التي يعملن فيها (أو المنظمات التي يعملن لديها بشكلٍ دوريّ) 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)، وثانيًا تسجيل ملاحظات بالمعلومات التي استطعن

إيجادهاعن أنفسهن فيها.

٨. بعد ذلك، على المشاركات البحث عن أسمائهن وعن كلمات رئيسية أخرى من القائمة التي وضعنها، بواسطة محرّك غوغل وداك داك غو وفايسبوك وتويتر وأي منصات أخرى – إليكن 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 معيّنة على الإنترنت – خاصة بمدن أو حكومات أو غير ذلك – حيث قد تُعرض معلوماتٍ عنهن، عليهن البحث فيها أيضًا. في حال كان لديهن موقعًا إلكترونيًا خاصًا بهن، عليهن البحث عن عنوان المجال على :https //whois-search.com للإطلاع على المعلومات الموجودة عنهن في سجلّ 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 سجّلنها، ومن ثمّ تفكير في الخطوة التالية التي يجب أن يتخذنها للإمساك أكثر بزمام الأمور بشأن ما قد يجده الآخرون عنهن على الإنترنت. أطلبن منهن وضع لائحة بالخطوات التي يتوجب عليهن القيام بها، وقد تتضمن إقفال بعض الحسابات وتعديل بعض المعلومات و/أو إعدادات الخصوصية على صفحات وسائل التواصل الاجتماعي، وتشغيل خاصية حجب معلومات التسجيل علي نطاق إستضافة موقعهن، إلخ.

١١. أثناء قيام المشاركات بوضع لوائح بالخطوات التي يتوجب عليهن إتخاذها، شاركن معهن بعض الموارد المفيدة لهن أثناء تطبيق بعض تلك الخطوات – قد يجدن ما يساعدهن

أيضًا 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 أوصفحات 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، ذكّرن 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. شددن للمجموعة على أن التمتع بمستوى خصوصية أفضل ممكن من خلال استخدام كلمات سرّ أقوى وممارسة عادات تصفّح أكثر أمانًا والإستفادة 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
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - إطرحي عليي ما تريدينه من أسئلة! (الخصوصية)
  - الخصوصية (الخصوصية)
  - الاستقصاء عن المعلومات الشخصية الخاصة بالمتصيد (العنف ضد المرأة على الإنترنت)
  - ماذا يمكن لبياناتكن الوصفية أن تفصح عنكن؟ (المناصرة الآمنة على الإنترنت)
- **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. إبدأن الجلسة بالشرح أنها ستركّز على فهم أوضح لما يحدث حين تصبح التكنولوجيا مكونًا حيويًا وأساسيًا أكثر فأكثر في المجتمع وتأثير ذلك على الهوية والخصوصية.

٢. إشرحن أنه من أجل توضيح ذلك، ستتطرقن 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 المتصوّر الذي ينشأ نتيجةً 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:

تشكّل 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: إحتمالية 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 الخفيّة: 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 صعباً. 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 يستخدمنها عادةً – سيساعدهن ذلك في تحديد أنواع المعلومات المشاركة مع هذه المنصات وفي وضع تكتيكات لاستخدامها بشكلٍ آمنٍ في نشاطاتهن الشخصية وعملهن على الإنترنت.
- **الطول:** 120 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أوتدريب مسبق
  - وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)
  - كيف يعمل الإنترنت؟ (أسس الأمن الرقمي،الجولة الأولى)
- **جلسات/تمارين ذات علاقة:**

- إطرحي عليي ما تريدينه من أسئلة! (الخصوصية)
- الخصوصية (الخصوصية)
- الجمهور الشبكي (الخصوصية)
- الحملات الآمنة على الإنترنت (المناصرة الآمنة على الإنترنت)

• **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 أوجهاز 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 بشكلٍ أفضل (راجعن قسم المراجع للإطلاع على الروابط).

إدارة الجلسة

الجزء الأوّل – 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 مطوّر كل تطبيق.

٢. إعطين المشاركات مهلة 15 دقيقة للقيام بما ورد أعلاه. بعد إنتهاء هذه المهلة، أطلبن 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 الفعليّة؛
- شروط خدمة غير واضحة أو مكتوبة بشكلٍ مبهم؛
- سياسات خصوصية تسمح للشركات ببيع بيانات المستخدمين للغير.

٣. شاركن أمثلة عن التطبيقات التي تتابع الدورة الشهرية على سبيل المثال تطبيق My Calender والتطبيقات الأخرى الخاصة بمتابعة الصحة الشخصية مع المجموعة. فسرن لهن كيف يتم ذلك وأنه وفقًا 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 أيضًا؟

٤. قسمن المشاركات إلى مجموعات من 3 إلى 4 مشاركات كحد أقصى وأطلبن من كل مجموعة وضع لائحة بما يعرفنه عن فايسبوك وغوغل – لتقديم مثال، يمكنكن الطلب منهن البدء بالإجابة على هذه الأسئلة:

- هل هذين الكيانين 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؟

أمهلن المشاركات 15 دقيقة للإنتهاء من وضع القائمة بكل المعلومات التي يعرفنها.

٥. ما أن ينتهي الوقت المخصص، أطلبن من كل مجموعة وضع لائحة بما قد تعرفه شركتا فايسبوك وغوغل 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 أيضًا للمساعدة في هذا الجزء من الجلسة. أمهلن 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 معًا (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 أزالها موقع فايسبوك أو فيديوهات محظورة على موقع يوتيوب أو أمثلة أخرى عن حسابات أغلقت على منصات التواصل الاجتماعي؟ شركات كشركة فايسبوك وغوغل تربطها علاقات وطيدة مع حكوماتنا ويعرف عنها أنها تتبادل معلومات المستخدمين معها (https://govtrequests.facebook.com) ما تداعيات ذلك علينا؟ هل نعرف بأي حالات عنف ضد النساء على الإنترنت بشكلٍ عام؟ وبشكلٍ خاص، أي حالات تلقت فيها مدافعات عن حقوق الإنسان تهديدات على الإنترنت أونشرت صور لهن وهنّ عاريات أو أنشأت حسابات على مواقع التواصل الاجتماعي للتشهير بهن أو"للترويج"

لخدماتهن الجنسية؟ على أي منصات حصلت هذه الحوادث وكيف تعاملت المنصة مع ذلك؟

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

٧. معًا كمجموعة، فكرن خلال 5 إلى 10 دقائق في كيفية استخدام هذه المنصات أيضًا 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 نسى أن المشاركات قد يرغبن بالاستمرار في استخدامها 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 الاستمرار في استخدام التطبيقات والمنصات ومواقع التواصل الاجتماعي هذه للاستخدام الشخصي أولجهود المناصرة ولكن بطريقة أكثر أمانًا.

٩. مع إبقاء المشاركات في المجموعات ذاتها من التمارين السابقة، أطلبن منهن التركيز الآن على طرق إبداعية في التفكير بشكلٍ جماعي لإستعادة خصوصيتهن. أعطين كل مجموعة رزمة أوراق صغيرة لاصقة بالإضافة إلى أقلام خطاطة وأقلام عادية. ومن ثمّ أطلبن منهن تقديم أكبر قدر ممكن من الأفكار خلال 10 إلى 15 دقيقة. يمكنكن تقديم أمثلة عن بعض التكتيكات ليتمكنّ من البدء بالتفكير، على سبيل المثال:

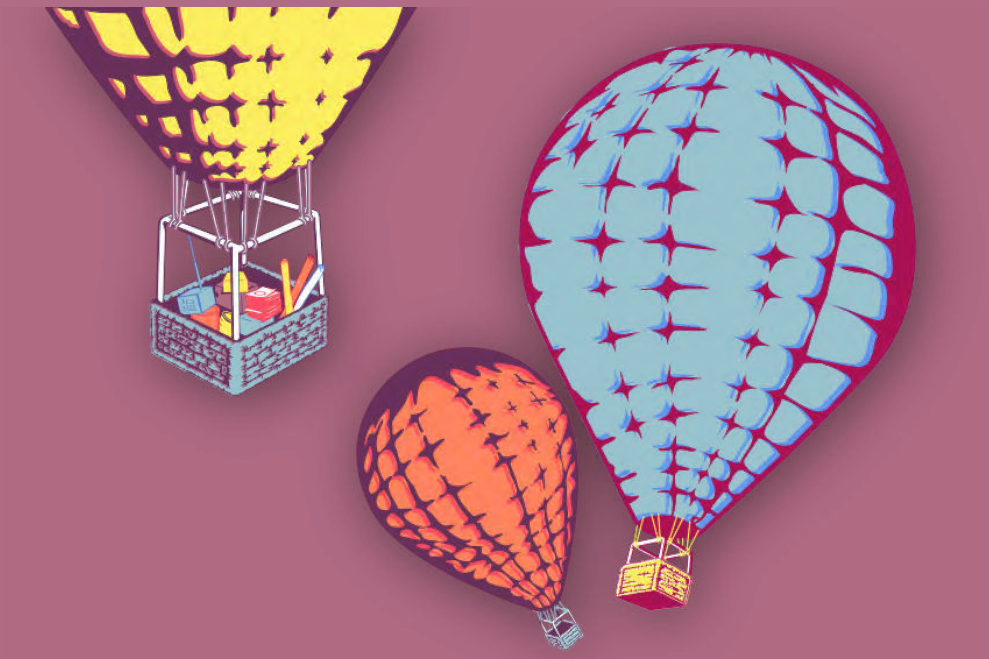
- إرباك الخوارزميات (algorithms) التي تستعين بها المنصات لأغراض الإعلان أو تحسين المحتوى؛

- مراجعة سياسات الخصوصية ومستجدات إعدادات الخصوصية بشكلٍ دوري؛
- التنبه للأذونات المعطاة للتطبيقات على أجهزتهن، لا سيما تلك المرتبطة بإعدادات تحديد الموقع الجغرافي وتحديد الموقع الجغرافي للصور والمنشورات؛
- استخدام منصات بديلة ملتزمة إلى حدٍ 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 مكانٍ ظاهر في غرفة التدريب لكي تتمكن المشاركات من العودة إليها مع تقدمهن في التدريب. هذه الأفكار ستكون مفيدة لكنّ أيضًا عند تعديلكن محتوى تدريبكن، لا سيما إذا أرادت المشاركات التركيز بشكلٍ أكبر على تحسين مستوى استخدامهن الآمن لشبكات التواصل الاجتماعي 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_manual



المناصرة الآمنة على الإنترنت

باب ٢٠

مواقع إلكترونية أكثر أمانًا

- **الأهداف:** في هذه الجلسة، ستساعدن المدافعات عن حقوق الإنسان في تحديد الممارسات الآمنة الواجب تطبيقها عند إدارة وحماية مواقعهن الإلكترونية – قد تكون المواقع هذه مواقعًا شخصية يستخدمنها في نشاطهن على الإنترنت أومواقع إلكترونية خاصة بمنظماتهن/جماعاتهن/حركاتهن.
- **الطول:** 50 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** متقدم
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أوتدريب مسبق
  - معرفة سابقة بكيفية إدارة المواقع الإكترونية
  - بمن تثقن؟ (تمارين بناء الثقة)
- **جلسات/تمارين ذات علاقة:**
  - بمن تثقن؟ (تمارين بناء الثقة)
  - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟ (الخصوصية)
  - الحملات الآمنة على الإنترنت (المناصرة الآمنة على الإنترنت)

- **المواد اللازمة:**
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
  - شرائح (عليها النقاط المفتاحية الواردة أدناه)
- **التوصيات:** هذه الجلسة تناسب مجموعات معينة أكثر من غيرها – ضعن هذه الجلسة على رأس سلّم الأولويات لا سيما للناشطات أو الجماعات التي لديها موقع إلكتروني.

من المفيد تحضير بعض الأمثلة قبل هذه الجلسة (من تقارير إخبارية أومنشوات على مدونات أومنشورات على وسائل التواصل الاجتماعي أو تجارب شخصية) عن الهجمات الإلكترونية ضد المدافعات عن حقوق الإنسان و/أو منظمات الدفاع عن حقوق الإنسان أوإختراقات المواقع الإلكترونية أو عمليات تدمير المواقع بشكلٍ 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 مباشرةً على عمليات إدارة مواقعهن، تقدم هذه الجلسة مع ذلك أساسًا صلبًا يمكنهن بواسطته البدء بالتفكير في التغييرات التي قد يقترحنها (أو تولي سيطرة أكبر في مسألة إدارة مواقعهن).

إدارة الجلسة

الجزء الأوّل – ما الأشكال الممكنة للهجمات الإلكترونية؟

١. إبدأن الجلسة بمراجعة بعض الإجابات المقدمة خلال جلسة "بمن نثقن؟" (تمارين بناء الثقة) – وأذكرن بشكلٍ خاص بعض الخصوم المحتملين بحسب المشاركات أنفسهن. سيوفر لكنّ ذلك أساسًا مفيدًا لتناول مسألة سلامة المواقع الإلكترونية بشكلٍ عام والمساحات الإلكترونية الخاصة بالناشطات بشكلٍ خاص.

٢. إسألن المشاركات – ما الذي يعتبرنه هجومًا 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 منظمتها/جماعتها. يمكنكن أيضًا تقديم بعض دراسات الحالات المعدّة مسبقًا من قبلكن في حال لا تتوفر لدى المشاركات أمثلة يمكنهن مشاركتها.

٣. إطرحن أسئلة متابعة بشأن الحالات التي تمت مشاركتها. هل شُن الهجوم ضمن سياق معيّن قبيل مظاهرة أو عرض تقرير ما أو نوع آخر من التجمعات العامة؟ ما كان شكل تعامل المدافعات عن حقوق الإنسان مع الهجوم؟ هل وُثّق الهجوم؟

الجزء الثاني – حماية المواقع الإلكترونية

٤. 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:

اختياري: 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 ونُظم إدارة المحتويات (Content management system CMS).

حماية موقعكن

- إستخدمن كلمات سرّ قوية لإدارة الموقع لتفادي تعرّض الموقع للإختراق – إستغلال الخصوم كلمات السرّ الضعيفة للوصول إلى الجهة الخلفية لأحد المواقع يعتبر من الطرق

الشائعة التي تتعرض بها المواقع للإختراق. في حال كان ذلك ممكنًا، فعّلن خاصية التحقق بخطوتين في حساب الموقع وخدمة الإستضافة وأي بوابات وصول أخرى.

- عند تسجيل أسم مجالٍ ما، غالبًا ما يتطلب الأمر من الشخص الذي يقوم بالتسجيل تقديم معلومات من قبيل أسمه/ها وعنوانه/ها وبريده/ها الإلكتروني. تحققن لمعرفة ماهية المعلومات المتوفرة في ملف تسجيل مجال معيّن وفكّرن 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؟ لابد 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 بياناتكن، والسؤال الأهم، هل يمكن الوثوق بأن خدمة الإستضافة لن تسلّم بياناتكن بناءً على طلب الحكومة؟ هل قد تحاول حكومة تلك الدولة التدخّل بموقعكن أو تحاول تدميره؟
  - فكرن في مدى فائدة شراء خدمات الإستضافة من خلال بائع ثاني، ففي بعض الهجمات قد تحتجن لفريق دعم جيّد قادر على مساعدتكن، 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 موقعٌ ما حاليًا – هذا النوع من البرامج شائع بشكلٍ خاص على المواقع التي تستعين بمنصات كوورد برس Wordpress كنظام إدارة معلومات. إحرصن على استخدام البرامج المضافة الضرورية فقط، وتحققن من أن أي برنامج إضافي مستخدم حاليًا مصنوع من مصدر موثوق به.
- فكرن في تثبيت برامج خدمات من قبيل برنامج "جت باك" Jetpack من شركة أوتوماتيك Automattic على منصة وورد برس لا سيما للخدمات مثل العناصر التفاعلية (widgets) الخاصة بالتواصل الاجتماعي والتعليقات ونماذج الاتصال. تتوفر أيضًا

برامج مضافة خاصة بأمن المواقع الأساسي من قبيل "بيتر دبليو بي سيكيوريتي" Better WP Security، بالإضافة البرامج المضافة الخاصة بالنسخ الاحتياطية الآلية للبيانات من قبيل "فولت برس" VaultPress أو "باك أب بودي" Backup Buddy.

- إحرصن على إجراء تحديثات على الخوادم المستضيفة للموقع بشكلٍ دوريّ (في حال لم تكن هذه التحديثات مدارة تلقائيًا 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 مواقعكن

- يوصى بشكلٍ كبير أن تقدم المواقع للمستخدمين والمستخدمات صلات مزودة ببروتوكول نقل النص الفائق الأمن (HTTPS) بشكلٍ تلقائي (وليس فقط كخيار) – 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 الأمن مجانًا.
- تعمل جماعات كثيرة حول العالم على دعم جهود الناشطين في مجال التكنولوجيا وتتخصص في العمل مع منظمات الناشطين مثل: "فرونتلاين ديفندرز" Frontline Defenders، "إلكترونيك فرونتيرز فاونديشن" EFF، لجنة حماية الصحفيين CPJ، "أيفكس" ifex، " منظمة تاكتيكل تكنولوجي كوليكتيف Tactical Technology Collective، منظمة تبادل الإعلام الاجتماعي SMEX، "آي ركس" IREX، و"إنترنيوز" Internews.
- سبق أن تعرضت منظمات أو مواقع إلكترونية لهجمات حجب الخدمة الموزّعة في الماضي، فكرن في الإستعانة بخدمات الحماية من هذه الهجمات المقدمة من مبادرات كثيرة منها "ديفلكت" Deflect أو "بروجكت شيلد" Project Shield. مبادرة "ديلفكت" التي تديرها منظمة "إيكواليتي. آي إي" Equalit.ie من مونتريال، كندا، هي عبارة عن خدمة مجانية بالكامل وموثوق بها بشكلٍ كبير في مجتمع الأمن الرقمي.

اختياري: فكرن في مشاركة الموارد بشأن التعامل مع هجمات حجب الخدمة الموزّعة، 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_manual/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
- **المستوى المهاري:** متوسط
- **المعرفة المطلوبة:**
  - بمن تثقن؟ (تمارين بناء الثقة)
- **جلسات/تمارين ذات علاقة:**
  - بمن تثقن؟ (تمارين بناء الثقة)
  - نموذج المخاطر القائمة على الجندر (تحديد الحلّ الأفضل)
  - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟ (الخصوصية)
  - المواقع الإلكترونية الأكثر أمانًا (المناصرة الآمنة على الإنترنت)
  - بناء كلمات سرّ قوية (أسس الأمن الرقمي،الجولة الأولى)
  - البرمجيات الخبيثة والفيروسات (أسس الأمن الرقمي،الجولة الأولى)
  - كيفية حماية حاسوبكن (أسس الأمن الرقمي،الجولة الأولى)

- **المواد اللازمة:**
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
  - شرائح (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 أمانًا؛ 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 كورنيليو Indira Cornelio لصالح "سوشل تي آي سي" SocialTIC

إدارة الجلسة

الجزء الأوّل -المقدمة والتخطيط الوقائي

١. إشرحن للمشاركات أن هدف الجلسة هو تحديد الحلول في مجال الأمن الرقمي، التي يمكنهن تطبيقها من أجل نشاطات حملات على الإنترنت أكثر أمانًا. لن يتوجب عليهن تطبيقها مباشرة خلال الجلسة. ولكن الهدف هو أن يبدأن بعملية إستكشاف من أجل تحديد تلك الحلول المناسبة لبيئتهن الفردية وحملاتهن.

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؟

٣. ذكرن 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 جدًا، لابد لهن من التنبه جيّدا لمن قد يراقبهن أو من قد يشكّل تهديدًا 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 أوالمسألة؟ 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 بشكلٍ إستراتيجي أكثر – التأكيد على المجموعة أنه يمكنهن حتى إعداد رسائل مسبقًا ردًا على السيناريوهات الممكنة الناتجة عن الردود على هذه الأسئلة. إضافة إلى ذلك، ذكرن المشاركات أن وضع تصوّر لأفضل سيناريو ممكن للحملة قد يساعدهن في التخطيط للتدابير الإحترازية – على سبيل المثال، كيف يمكن أن يحضرن لإحتمال ألّا يتمكن موقعهن من تحمّل الإرتفاع المفاجئ لعدد زوار الموقع وأن ينهار على أثر ذلك، في حال لاقت الحملة نجاحًا ورواجًا كبيرًا؟

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 كنّ يستخدمن أجهزتهن الشخصية لتنفيذ الحملة (مقابل جهاز "العمل") – ما كمية المعلومات المرتبطة بالحملة التي تخزّن على هذه الأجهزة؟ هل هي متصلة أيضًا بعنوان البريد الإلكتروني وحسابات مواقع التواصل الاجتماعي؟

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

حماية حواسيبهن وهواتفهن المحمولة بواسطة كلمة سرّ؛

تثبيت برمجيات مكافحة للفيروسات على كل من حواسيبهن وهواتفهن المحمولة؛

إجراء عمليات نسخ احتياطية بشكلٍ دوريّ 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 OSX FileVault[١] وبرمجية "ويندوز بيتلوكر" (Windows BitLocker[٢]) من أكثر الخيارات الشائعة المتاحة لتشفير الأقراص تشفيراً شاملاً؛

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

الجزء الثالث – إدارة إمكانية الوصول في الحسابات

٩. غالبًا ما تتطلب الحملات على الإنترنت أن يعمل عليها مستخدمون ومستخدمات عدّيدين من أجل التمكن من الوصول إلى الحسابات ذاتها (أو الأجهزة، في بعض الحالات). تؤدي إمكانية الوصول إلى جهاز أو حساب من قبل عدّة مستخدمين أو مستخدمات بواسطة بيانات الدخول ذاتها إلى إرتفاع حاد للخطر؛ ولكن، من خلال إتخاذ بعض

[١] https://en.wikipedia.org/wiki/FileVault
[٢] https://en.wikipedia.org/wiki/BitLocker

التدابير الإحترازية، تستطيع المشاركات تقليص إحتمالية أن تتحوّل هذه المخاطر إلى تهديدات مباشرة بشكلٍ ملحوظ. علي سبيل المثال يمكن عمل الآتي:

بالنسبة لكل الحسابات على الإنترنت والأجهزة المشتركة، يعتبر تحديد لائحة بأقل عدد ممكن من الأشخاص المخولين بالوصول من التدابير الأولى الأهم الواجب تطبيقها؛ ومن التدابير الأخرى، الحرص على الإلتزام ببروتوكولات أوإجراءات معيّنة بشكلٍ منتظم (لا سيما في ما يخص التوصيات التالية) : بالنسبة للمنصات على الإنترنت بشكلٍ خاص، يجب أن تحرص كل عضوات الفريق اللواتي مُنحن إمكانية الوصول على التحقق بشكلٍ دوري من سجل الاستخدام والنشاط على الحسابات المشتركة – على سبيل المثال، يمكنهن على حسابات "جي مايل"/غوغل، التحقق من سجّل عمليات تسجيل الدخول الحديثة (وإعداد إنذارات للنشاطات المشبوهة) ضمن "نشاط الحساب الأخير" (Last Account Activity)؛ وعلى نحوممائل، 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"/KeePass" "كي باس إكس" KeePassX[٣] بإنشاء ملفات قواعد بيانات فردية لكلمات سرّ الحسابات، التي تكون محمية بدورها بواسطة كلمة سرّ رئيسية؛ على نحو ممائل، بالنسبة للحسابات على غوغل وفايسبوك وتويتر يوصى بتفعيل خاصية التحقق بخطوتين التي توفر مستوى إضافي من القدرة على التحكّم؛ في حال كان لابد من مشاركة كلمة سرّ ما مع أعضاء الفريق، وفي حال لم يكن القيام بذلك وجهًا لوجه ممكنًا، يعتبر خيار إرسال كلمات السرّ عبر البريد الإلكتروني المشفّر – بواسطة برمجية جي بي جي GPG أوبواسطة خدمة مثل خدمة توتانوتا Tutanota[٤] أو عبر الرسائل المشفّرة (بواسطة تطبيق سيجنال على هاتف محمول) من الخيارات الأكثر أمانًا – في حال استخدام تطبيق سيجنال، احرصن على تحديد بروتوكول مع أعضاء الفريق حول عملية حذف الرسائل المزوّدة

[٣] http://keepass.info/
[٤] https://tutanota.com/

بكلمات السرّ من أجهزتهن ما إن تصلهن.

الجزء الرابع – اختيار التطبيقات للحملات

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 ستُستخدم، لابد أن تأخذ المشاركات بعين الإعتبار بعض المسائل التي قد تساعدهن بشكلٍ أساسي على تفادي مشاركة معلوماتهن بواسطة بعض الأدوات غير الآمنة أو الأدوات التي لم تعد مدعومة من المطوّرين:

هل ما زال التطبيق فاعلاً، أي هل يتابع المطورون/ات توفير تحديثات على الأمن 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 مؤخرًا؟

الجزء الخامس – بناء المجتمعات من خلال فايسبوك

١١. غالبًا ما يستخدم فايسبوك في الحملات على الإنترنت من أجل تنظيم المجتمعات ونشر الرسائل المهمة وأي اتصالات أخرى بسرعة. ولكن لابد تسليط الضوء على بعض نقاط الضعف المحتملة عند استخدام هذه المنصات كجزء من البنية التنظيمية الأساسية للحملة:

يجب أن تدرك المشاركات أن لاستخدام فايسبوك (أوأي منصة تواصل إجتماعي كبيرة أخرى) تداعيات محتملة على هوياتهن الشخصية على الإنترنت – للتخفيف من مدى تعرّضهن، يمكنهن إنشاء صفحات مخصصة لإدارة صفحات الحملة عوضًا عن استخدام صفحاتهن الشخصية؛

تجدر الإشارة هنا أنه من الممكن الآن تلقي إشعارات من فايسبوك تكون مشفّرة بواسطة مفتاح جي بي جي العام مرتبط بحساب بريد إلكتروني – قد يكون ذلك مفيدًا للمدافعات عن حقوق الإنسان اللواتي يرغبن في إتخاذ تدابير إضافية لفصل عملهن عن هويتهن الشخصية على الإنترنت أثناء إدارة الحملات؛ يجب أن تخطط المسؤولات عن إدارة الحملات على الإنترنت بشكلٍ مدروس لأنواع المعلومات والاتصالات التي يشاركنها على منصات إلكترونية كمنصة فايسبوك – فالأمثلة السابقة كثيرة عن إختراق صفحات حملات على فايسبوك من قبل الخصوم، وهذا ما فرض على مديري الصفحات إغلاقها (أوأدى ذلك إلى تدمير الصفحة بالقوّة من قبل المنصة بسبب تبليغ الخصوم عنها) قد يشكّل ذلك تراجعًا ملحوظًا بالنسبة للحملة وعملية تقدّم بناء المجتمع، لذا شددن للمشاركات على أهمية توفر قنوات اتصال وتنظيم بديلة – قد تتضمن هذه القنوات:

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

تستطيع المستخدمات أيضًا تنزيل المعلومات الموجودة على صفحة الفايسبوك لإنشاء نسخ احتياطية خارج الإنترنت، وهذه إستراتيجية جيّدة؛

استخدام خدمة لخدمة قوائم "رايز أب" Riseup[٥] لإنشاء مجموعات بريد إلكتروني لإرسال نشرات إخبارية أوأي رسائل أخرى؛

تنظيم إجتماعات وجهًا لوجه إن أمكن؛ ولكن، بالنسبة للحملات التي تتناول قضايا معيّنة ودول معيّنة، لابد من الانتباه إلى أن ذلك قد يشكّل خطرًا كبيرًا لذا يوصى بعدم عقد مثل هذه اللقاءات؛

[٥] https://www.lists.riseup.net

الجزء السادس – الموافقة عن دراية

١٢. ناقشن أهمية الموافقة عن دراية مع المجموعة – لابد من ذلك بشكلٍ عام في حملات التوعية بشأن قضايا حقوق الإنسان، ولا سيما عند الإستعانة بصور أوشهادات 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 صريح وواضح على ذلك مسبقًا؛ وعلى نحو مماثل، يجب أن يوافقوا أيضًا بشكلٍ صريح وواضح أن تُشارك أي مادة من هذه المواد مع عموم الناس – يجب أن تشرحن لهم بشكلٍ واضح 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 لبياناتكن الوصفية (Metadata) أن تفصح عنكن؟

- **الأهداف:** في هذه الجلسة، ستقدّمن مفهوم البيانات الوصفية وأهمية التنبه للبيانات الوصفية الموجودة في أنواع مختلفة من المحتويات – لا سيما عند إجراء عمل حساس مرتبط بحقوق الإنسان.
- **الطول:** 90 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - الحملات الآمنة على الإنترنت (المناصرة الآمنة على الإنترنت)
  - الجمهور الشبكي (الخصوصية)
- **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 المعقّدة التي يمكن تقديمها في العملية التدريبية
- إحرصن على تخصيص الوقت الكافي لتقديم هذه الجلسة بالتفصيل، فهي مهمة جداً لبيئات عمل المدافعات عن حقوق الإنسان والناشطات الحقوقيات

إدارة الجلسة

الجزء الأوّل – ما هي البيانات الوصفية؟ Metadata

١. إبدأن الجلسة بمشاركة بعض النقاط الرئيسية مع المشاركات – أهمها يتضمن ما يلي:

إشرحن 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 يمكنكن 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 المعقّدة التي يمكن تقديمها في العملية التدريبية، لذا إحرصن على سؤال المشاركات إن كان المفهوم واضحاً بالنسبة لهن – في حال لم يكن كذلك، خصصن الوقت اللازم للإجابة عن أسئلتهن بشكلٍ مفصّل

إستنادًا إلى خبرتكن.

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

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

١. تكشف البيانات الوصفية معلومات كثيرة عنكن أطلبن من المشاركات إلتقاط 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 مخصصًا لمجموعة من المبتدئات. والآن، أطلبن من المشاركات إعادة التمرين ولكن هذه المرة مع تعطيل خدمات تحديد الموقع الجغرافي على هواتفهن. قسمن المشاركات إلى مجموعات من 3 إلى 4 مشاركات كحدٍ أقصى لمناقشة أفكارهن حول مدى فائدة البيانات الوصفية وكيف برأيهن قد تؤدي إلى تعريض أمنهن للخطر عند القيام بعمل في مجال حقوق الإنسان. خلال نقاشهن، لابد من المحافظة على التركيز على العمل في مجال حقوق الإنسان، ولابد للمشاركات أيضًا 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 مشفّر وإنشاء نسخ منفصلة لغايات التنقيح والتعديل أو التخزين على حواسيبهن.

٢. تنشأ البيانات الوصفية ولكن من الممكن إزالتها أيضًا. أطلعن 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 أيضًا 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/

هواتف محمولة أكثر أمانًا

باب ٢٣

ماركو بولو

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

[١] https://cyber-women.com/ar/الخصوصية/

[٢] https://cyber-women.com/ar/الجمهور-الشبكي/

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

إدارة الجلسة

١. إخترن إحدى المشاركات في المجموعة للعب دور "الهاتف المحمول" – من بعد تحديد المتطوّعة، أطلبن منها مغادرة الغرفة.

٢. في المساحة المتوفرة لديكن في مكان التدريب، قسّمن بقية المجموعة إلى "مبانٍ" و"هوائيات لاسلكية" وزعهن في كافة أرجاء الغرفة. إحرصن أن تتوزع الهوائيات بشكلٍ متساوٍ، بحيث تستطيع كل واحدة تحديد "نطاقٍ" خاص بها في الغرفة.يمكن لكل مشاركة وضع دائرة علي الأرض لتحديد نطاقها الخاص إذا كانت مساحة التدريب تسمح بذلك.

٣. 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.

٤. 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:

تشغّل شركات الاتصالات هوائيات في مناطق مختلفة، توفر كل واحدةٍ منها التغطية لمنطقة (أو نطاق) معيّن؛

تتلقى الهواتف المحمولة التغطية عبر إرسال طلبات إلى الهوائيات الجديدة التي تلتقي بها ("ماركو") أثناء تنقلها من مكانٍ لآخر، وترد الهوائيات بـ ("بولو") على الطلبات عبر تقديم التغطية.

باب ٢٤

الهواتف المحمولة،الجزء الأوّل

- **الأهداف:** تقدم هذه الجلسة للمشاركات لمحة عامة تعريفية حول كيفية عمل الهواتف المحمولة من خلال شبكات الاتصالات الهاتفية.
- **الطول:** 60 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - ماركو بولو (هواتف محمولة أكثر أمانًا)
  - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟ (الخصوصية)
- **المواد اللازمة:**
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
  - أوراق
  - شرائح (عليها النقاط المفتاحية الواردة أدناه)
- **التوصيات:** هذه الجلسة لها فعالية قصوى في حال قدّمت مباشرة من بعد تمرين ماركو

بولو من هذه الوحدة، ولكن يمكن تقديمها وحدها أيضًا.

هذه الجلسة نسخة معدّلة 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

إبدأن الجلسة بشرح المكونات الرئيسية للهواتف المحمولة للمشاركين. يمكنكن عرض صور لكل مكوّن منها ثناء الشرح.

الجزء الأوّل – ما هي مكونات الهاتف؟

١. على الرغم من أن بعض الهواتف، لا سيما الهواتف الذكية منها، تتمتع بقدرات متطوّرة، تتشارك كل الهواتف مكوّنات أساسية عدّة منها الآتي:

الهوائي

الهوائيات اللاسلكية، التي تسمح بالتواصل بين الهاتف المحمول والشبكات الخارجية، قد تكون ظاهرة في الأجهزة الأقدم – حيث في بعض الأجهزة القديمة جدًا كان من الضروري إخراجها يدويًا للتمكن من استخدامها. معظم الهواتف الحديثة العهد مزودة بهوائيات ضمن الجهاز مباشرةً، لذا لم تعد "ظاهرة". عدا عن الهوائي المسؤول عن التواصل مع شبكة الهواتف، قد تكون هذه الهواتف الحديثة مزوّدة 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 ولاحقًا هواتف سامسونغ غالاكسي إس)، لم تُصمم البطاريات بشكلٍ 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 اتصالات الهاتف، بما في ذلك الاتصالات والأوامر التي يصدرها المستخدم للهاتف، ومن الهاتف من وإلى شبكة الهواتف. يعتبر النطاق الأساسي في أي هاتف عادةً "ملكية" مهمة من قبل المصنعين وقد يعتبر "الصندوق الأسود" (لا يمكن الوصول إليه ويصعب التلاعب به) من حيث بروتوكولات اتصالاته وكيفية التحكّم 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 هاتفكن محدودة، ويمكن لبعض المستخدمين إتخاذ القرار بشأن حفظ بيانات معيّنة على شريحة هاتفهم أو في الذاكرة الداخلية للهاتف أو على وسائط قابلة للإزالة من عدمه. لا تنسين ذكر أن بعض الهواتف مصممة لتحمّل 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، غالبًا ما تكون هذه الوسائط شرائح الذاكرة أو شرائح

الذاكرة المصغّرة. بعض الهواتف مزوّدة أيضًا 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 مزوّدٌ أيضًا بآلات تصوير في كل من الجهة الأمامية والجهة الخلفية من الجهاز، وغالبًا ما تستخدم آلتي التصوير هذه في تطبيقات اتصالات الفيديو من قبيل فايسبوك مسنجر أوسكايب.

الجزء الثاني – الممارسة التطبيقية

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

٣. ما إن تنتهي كل مجموعة من العمل، أطلبن 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 الإفتراضية الخاصة التحقق من إعدادات ضبط التطبيقات كلمات سرّ قوية النسخ الاحتياطية للبيانات عدم شحن هواتفكن بواسطة منفذ مفتاح اليواس 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
- **المستوى المهاري:** متوسط
- **المعرفة المطلوبة:**
  - ماركو بولو (هواتف محمولة أكثر أمانًا)
  - الهواتف المحمولة،الجزء الأوّل (هواتف محمولة أكثر أمانًا)
  - تعريف بمسألة التشفير (التشفير)
  - كيفية حماية حاسوبكن (أسس الأمن الرقمي،الجولة الأولى)
- **جلسات/تمارين ذات علاقة:**
  - ماركو بولو (هواتف محمولة أكثر أمانًا)
  - الهواتف المحمولة،الجزء الأوّل (هواتف محمولة أكثر أمانًا)
  - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟ (الخصوصية)
  - كيفية حماية حاسوبكن (أسس الأمن الرقمي،الجولة الأولى)

- **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 سؤالٌ 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، ذكّرن المشاركات ببعض ممارسات الأمن الرقمي الأساسية التي يمكن تطبيقها في الهواتف المحمولة من قبيل: تحميل برمجيات مكافحة الفيروسات على الهواتف المحمولة، والشبكات الإفتراضية 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 سيتخدمن أجهزتهن الخاصة في هذه الجلسة، لابد أن يقمن بعملية نسخ احتياطي لبياناتهن من باب الإحتياط.

إدارة الجلسة

الجزء الأوّل – التشفير في الهواتف المحمولة

١. ذكّرن المشاركات بالجلسات السابقة التي تناولت مفهوم التشفير، لا سيما جلسة التعريف بمسألة التشفير – ولعلكن أيضًا ناقشتن سابقًا التشفير من حيث تشفير الأقراص بشكلٍ شامل خلال جلسة كيفية حماية حاسوبكن. أذكّرن للمشاركات أن النسخ الأحدث من أنظمة آي أو أس وأندرويد (أيار/مايو 2017) مزوّدة بتشفير مفعّل تلقائيًا.

الجزء الثاني – استخدام برمجية جي بي جي على الهواتف المحمولة

٢. في حال كانت المشاركات تعرفن التشفير بواسطة برمجية جي بي جي GPG، قدمن لهن خدمة البريد الإلكتروني "كاي 9" K-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 نقّاط الضعف الخاصة بالهواتف المحمولة) – المقصود هنا هوالتشديد 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.

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

الجزء الثالث – هل يقوم هاتفكن بتعقبكن؟

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 أيضًا بتعقّب المحتوى فحسب بل تتعقّب جهات الاتصال الخاصة بنا – فكل حديث مرتبط بفرد معيّن.

٤. قد ترغبن أيضًا في مناقشة كيف يمكن أن يعتبر نوع التعقّب الذي يجريه الهاتف نوعًا من أنواع المراقبة، وكيف أن المراقبة قادرة على الحدوث من خلال طرق كثيرة أخرى غير الطرق الإعتيادية المتوقعة. إسألن المجموعة عن أنواع المخاطر أو التهديدات التي يشعرن أنها محدقة 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

المحافظة على سريّة الهوية

باب ٢٦

الصديقة السريّة

- **الأهداف:** في هذه الجلسة، ستشرحن مفهوم المحافظة على سريّة الهوية وستوجّهن المشاركات في عملية ممارسة تطبيقية ستُشعرهن بأهميته.
- **الطول:** 30 دقيقة
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - المحافظة على سريّة الهوية (المحافظة على سريّة الهوية)
  - المزيد من الهويات الإلكترونية! (المحافظة على سريّة الهوية)
- **المواد اللازمة:**
  - أقلام وأوراق لكتابة الرسائل ومغلفات
  - كراسي
  - وعاء أوإناء
  - قصاصات صغيرة من الورق الأبيض

- عصبة للعينين أوأي شيء آخر لتغطية العينين

• **التوصيات:** يوصى بإعلام المشاركات بهذا التمرين قبل موعده 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 سينشأنها وبالتالي يمكنهن المجيء جاهزات وقد فكّرن في كل هذه التفاصيل.

إدارة الجلسة

الجزء الأوّل – المقدمة

١. خلال هذا التمرين، ستشارك كل مشاركة هوية جديدة بالكامل لها. يفترض أن تحضر المشاركات هذه الهوية مسبقًا، و يجب ألّا تستند على شخص فعلي وأن تكون من نسج الخيال.

٢. إشرحن لهن أنه عند بناء هذه الهوية الجديدة، يمكنهن التمتع بالحريّة الكاملة، أي يمكنهن أن يكن نساءًا أو رجالاً ,أوحتى مكانًا، أوأ ي شيء يخطر في بالهن. الفكرة الأساسية من هذا التمرين هي أن يختلقن هوية جديدة لهن بكل ما للكلمة من معنى – وهذا يعني إختلاق اسمٍ جديد لهن ومكان سكن جديد ومكان عمل جديد وعائلة جديدة وحتى هوايات جديدة.

الجزء الثاني – حان وقت اللعب!

٣. من بعد التعريف بالتمرين، إبدأن المرحلة التالية بالتعريف بشكلٍ موجز بمفهوم المحافظة على سريّة الهوية. إسألن المشاركات لماذا يعتبرن مسألة المحافظة على سريّة الهوية مسألةً لابد منها في عملهن وفي حياتهن الشخصية وعلاقاتهن على حدٍ سواء.

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

٤. يجب أن تجّهز كل مشاركة قبل المجيء إلى التمرين مفهومًا واضحًا لهويتها الجديدة - على أن يشمل ذلك اسمها ومكان ولادتها ومكان عملها وعائلتها وحتى هواياتها، ... إلخ. قبل البدء بالتمرين، أطلبن من كل مشاركة الإفصاح عن أسم هويتها الجديد معكن وليس للمجموعة لكي تتمكنّ كمدربات من المتابعة (هذا عنصر مهم من التمرين).

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

٦. 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 السرّية.

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

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

٩. تجولن في الغرفة وإجمعن كل المغلفات. إستنادًا إلى لائحتكن التي تحدد الهوية الجديدة المرتبطة بكل مشاركة، وزعن الرسائل على المتلقيات المقصودات (هذه المرة أيضًا، إحرصن ألّا ترى المشاركات الأسماء المكتوبة على المغلفات، بإستثناء تلك المخصصة لهن).

١٠. واحدة تلو الأخرى، أطلبن 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 السرّية الجلوس في كرسي آخر وضع إلى جانب المتطوعة.

١٢. بعد أن تنتهي كل مشاركة من وصف رسالتها، أطلبن منها محاولة تخمين مَن من المشاركات الأخريات هي صديقتها السرّية. وبعد أن تحاول ذلك، أزلن العصبة عن عينيها وأطلبن منها أن تنظر إلى الشخص الجالس إلى جانبها لمعرفة ما إذا كان تخمينها صحيحًا.

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

الجزء الثالث – الحلقة الختامية

١٤. بعد الإنتهاء من التمرين، إسألن المجموعة – هل كانت تخميناتهن صحيحة بشأن هوية صديقاتهن السريات؟ كيف تمكنّ من معرفتها، أوما هي العملية الذهنية التي إستعنّ بها في تخميناتهن؟ ما كان مدى صعوبة ذلك عليهن؟

١٥. إختتمن التمرين بالتفكير في أهمية المحافظة على سريّة الهوية والتمكن من حماية هوية شخص ما بالكامل، ومن ناحية أخرى مدى سهولة إخفاء الآخرين لهوياتهم الحقيقية أحيانًا (ولنيّاتهم أيضًا).

باب ٢٧

المحافظة على سريّة الهوية

- **الأهداف:** في هذه الجلسة، ستقدمن للمشاركات مفهوم المحافظة على سريّة الهوية على الإنترنت، بالإضافة إلى الأدوات والممارسات المرتبطة بهذا المفهوم، والتي قد تساعد في حماية الهوية وعدم الكشف عنها.
- **الطول:** 40 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** متوسط
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أوتدريب مسبق
- **جلسات/تمارين ذات علاقة:**
  - الصديقة السريّة (المحافظة على سريّة الهوية)
  - ماذا يمكن لبياناتكن الوصفية أن تفصح عنكن؟ (المناصرة الآمنة على الإنترنت)
  - التصفح الآمن (أسس الأمن الرقمي،الجولة الأولى)
  - المزيد من الهويات الإلكترونية! (المحافظة على سريّة الهوية)
- **المواد اللازمة:**
  - شرائح (فيها النقاط المفتاحية الواردة أدناه)

- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض

إدارة الجلسة

الجزء الأوّل – تعريف بالمحافظة على سريّة الهوية على الإنترنت

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

- إشرحن فوائد معرفة المزيد عن ماهية المحافظة على سريّة 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 سريّة الهوية على مستويات أو طبقات مختلفة، شارحاتٍ للمشاركات أنهن قادرات على المحافظة على سريّة الهوية في نشاط معيّن أو اتصال معين أو صفحة بأكملها أو جلسة استخدام

الجزء الثاني – البيانات المحددة للهوية والمحافظة على سرّية 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 معيّن 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 الإفتراضية من دون الكشف عن الهوية)؛
- بغية تبيان بعض تداعيات عناوين بروتوكول الإنترنت على المحافظة على سريّة الهوية للمجموعة، أطلبن منهن استخدام موقع إلكتروني من قبيل https://what ismyipaddress.com/ للتعرف على عنوان بروتوكول الإنترنت الخاص بهن كأفراد، وكيف أنها تكشف عن أنواع أخرى من المعلومات التي قد تكون حساسة أوقادرة على تحديد هوية شخصٍ ما.

٣. والآن، ستقدمن الأدوات التالية للمشاركات وستشرحن أهمية كل واحدةٍ منها في المحافظة على سريّة الهوية على الإنترنت – أشرن إلى أن كل واحدة منها تقدّم إمكانية المحافظة على سريّة الهوية بطرقٍ مختلفة أوبمستويات مختلفة:

- متصفح تور
- الشبكات الإفتراضية الخاصة (Virtual Private NetworksVPN's)
- نظام "تايلز" Tails (The Amnesiac Incognito Live System)
- برنامج "إيتش تي تي بي إس إفري وير" HTTPS Everywhere

لابد 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. أطلبن 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

فرقًا في عناوين بروتوكول الإنترنت أو في أمرٍ آخر؟

٥. هذه فرصة جيّدة لتناول نقطة أخرى تربك المستخدمين/ات: التصفّح المتخفي (Incog-nito Mode). ففي معظم الأحيان، يظنّ المستخدمون أنهم يتصفحون الإنترنت من دون الكشف عن هويتهم أثناء استخدام التصفّح المتخفي فقط (أو ما يعادله، بحسب المتصفّح المستخدم). ما الذي تلاحظنه 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
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
  - المحافظة على سريّة الهوية (المحافظة على سريّة الهوية)
  - ماذا يمكن لبياناتكن الوصفية أن تفصح عنكن؟ (المناصرة الآمنة على الإنترنت)
  - التصفح الآمن (أسس الأمن الرقمي،الجولة الأولى)
- **جلسات/تمارين ذات علاقة:**
  - المحافظة على سريّة الهوية (المحافظة على سريّة الهوية)
  - الصديقة السريّة (المحافظة على سريّة الهوية)
  - ماذا يمكن لبياناتكن الوصفية أن تفصح عنكن؟ (المناصرة الآمنة على الإنترنت)

- التصفح الآمن (أسس الأمن الرقمي،الجولة الأولى)

• **المواد اللازمة:**
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
- لوح ورقيّ (ورقة أو ورقتين لكل مشاركة)
- أقلام خطاطة أو أقلام

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

إدارة الجلسة

الجزء الأوّل – الهويات الإلكترونية المتصلة

١. إبدأن التمرين بالطلب من المشاركات وضع لائحة بأي من الهويات الإلكترونية التي يمتلكنها؛ يمكن أيضًا سؤالهن بكل بساطة عما إذا كانت إحداهن 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. إستنادًا 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، إلّا أنهن لا يرغبن في استخدام صفحاتهن الشخصية أوهويتهن لإدارة صفحة الحملة؛ المدافعات اللواتي يجرين عمليات بحث حساسة على الإنترنت، ويرغبن في ترك أقل قدر ممكن من الآثار الرقمية التي تسمح بتعقّب أثرهن؛

المدافعات اللواتي كنّ يوثق حالات إنتهاك الحكومات لحقوق الإنسان، واللواتي يخططن

لفضح هذه المعلومات عبر نشر تقرير مهم أو بيان عام.

٣. والآن أطلبن من المشاركات تشكيل مجموعات من شخصين وتحديد الظروف الأخرى التي يفضل أن ينشئن فيها هوية جديدة غير مرتبطة بهويتهن الشخصية. أطلبن منهن التفكير في مدى مزجهن لهوياتهن الشخصية وعملهن كناشطات:

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

ما مدى إرتباط حياتهن الرقمية الشخصية بحياتهن كناشطات؟

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

طلب معلومات من وكالات حكومية؛

زيارة المواقع الإلكترونية الحكومية لجمع معلومات سينشرنها على الإنترنت؛ إدارة حسابات مواقع التواصل الاجتماعي الخاصة بمنظمتهن أوجماعتهن)؛

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 مزيّفة 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 مزيّفة 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 أيضًا البدء بعدد صفر متابعين/ات على صفحات التواصل الاجتماعي؛

فصل الصفحات الشخصية عن الصفحات المهنية: يتطلب ذلك فقط من المستخدمات تغيير إعدادات الخصوصية الخاصة بحساباتهن، إما من أجل الحد من المعلومات المتوفرة للعموم وإما لإدارة مستوى المعلومات المتاحة لأصدقاء ومتابعين وجهات اتصال معيّنين؛ 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 لهويتهن الشخصية أو المهنية) ترك هوياتهن كما هي الآن: يتطلب ذلك على الأرجح من المستخدمات تغيير إعدادات الخصوصية الخاصة بحساباتهن، إما من أجل الحد من كمية المعلومات المتوفرة للعموم وإما لإدارة مستوى المعلومات المتاحة لأصدقاء ومتابعين/ات وجهات اتصال معينة.

٦. والآن، أطلبن من المشاركات مناقشة ضمن المجموعات ذاتها في المرحلة الثالثة، بعض إيجابيات وسلبيات كل خيار من هذه الخيارات، إما بالمعنى العام أو خصيصًا بالنسبة لهن ولبيئة عملهن. ومن ضمن المشاكل التي قد تنشأ خلال هذه النقاشات، هي المشاكل المرتبطة بالجانب العملي والمصداقية – كنّ جاهزات للتحدث عن هذه المسائل تحديدًا حين تقمن المشاركات بمشاركة بعض خلاصات نقاشهن مع المجموعة.

الجزء الثالث – الممارسة التطبيقية والتوصيات

٥. إشرحن للمشاركات أنه يمكنهن الاختيار 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 هويتهن الجديدة – تتضمن بعض الإعتبارات المحددة التي يتوجب عليهن التفكير فيها ما يلي:

ما هو الاسم الذي قد يستخدمنه؟ (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 هواياتهن وإهتماماتهن المحتملة؟ أين ولدن وأي يعشن؟ 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 تساعدهن في تفادي إنكشاف هوياتهن الحقيقية. إذكرن أن بعض تلك التوصيات سبق أو وردت في جلسات سابقة (المحافظة على سريّة 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 المستخدمات 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 المستخدمات على تفادي الأخطاء التي تعرّض هويتهن الجديدة لخطر الإنكشاف. تستطيع المشاركات القيام بذلك عبر استخدام أجهزة حاسوب أو هواتف منفصلة، وإعداد آلة افتراضية منفصلة على حاسوبهن، أو عبر استخدام نظام تشغيلي بديل كنظام تايلز (راجعن جلسة لنعد إلى خانة الصفر! للمزيد من المعلومات)؛ عند إعداد صفحة جديدة، يفضل أن تفكر المشاركات عند تسجيل الدخول في الحسابات المرتبطة في استخدام متصفح منفصل مختلف عن الذي يستخدمنه بشكلٍ رئيسي للوصول إلى صفحاتهن الحالية – سيساعدهن ذلك في تفادي ربطها بالحسابات، أوتسجيل دخولهن إلى إحداها في المتصفح الآخرعن طريق الخطأ ومشاركة المعلومات التي قد تفضح الفصل بين هوياتهن؛ راجعن عادات التصفّح الآمن العامة مع المشاركات – يمكنكن استخدام هذه المراجعة كأساس

للتحدّث عن مفهوم "بصمات" المتصفح، وأثر ذلك المحتمل على الفصل بين هوياتهن https://panopticlick.eff.org/static/browser-uniqueness.pdf؛

إضافة إلى ذلك، يمكنكن مراجعة كيفية تعتيم عناوين بروتوكول الإنترنت التي قد تفضح تفاصيل موقعكن الجغرافي؛

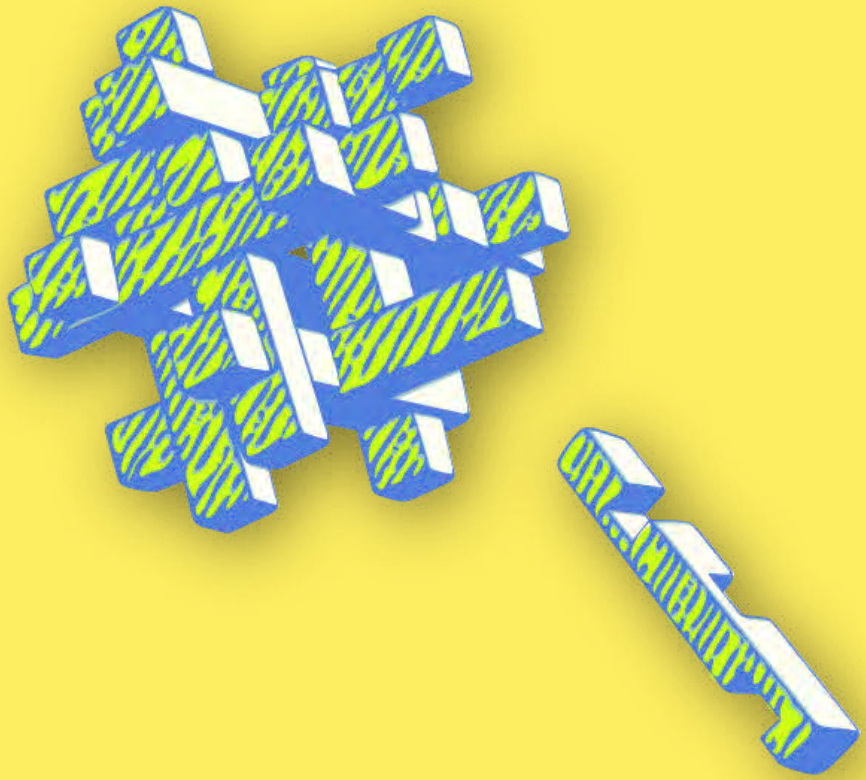
يجب ألا نتبع المشاركات أي أصدقاء أو أعضاء من عوائلهن أو منظمتهن بواسطة هوياتهن الجديدة – فقد يسمح ذلك بسرعة لأي شخص يبحث بدقة علي إكتشاف الرابط بين الهوية تلك والهوية الحقيقية؛

ذكرن المشاركات أن يتنبهن 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 لهوياتهن الإلكترونية الجديدة!

المراجع

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



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
- **المستوى المهاري:** متوسط
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أوتدريب مسبق
- **جلسات/تمارين ذات علاقة:**
  - الخصوصية (الخصوصية)
  - الحملات الآمنة على الإنترنت (المناصرة الآمنة على الإنترنت)
  - الاتصالات المشفّرة (التشفير)
  - التخزين والتشفير (أسس الأمن الرقمي الجولة الثانية)
- **المواد اللازمة:**
  - شرائح (فيها النقاط المفتاحية الواردة أدناه)
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض

- أمثلة عن تقنيات التشفير (مطبوعة)

إدارة الجلسة

الجزء الأوّل – هل سبق لكن أن إستخدمتن التشفير؟

١. إشرحن لهن أن هذه الجلسة جلسة ستعرّفهن على التشفير كمفهوم، لذا لن نتعمّقن كثيرًا 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)

٢. قسمن المشاركات إلى مجموعات من شخصين ومن ثمّ إبدأن الجلسة عبر عرض بعض الأمثلة عن تقنيات التشفير. إليكن بعض الأمثلة التي يمكنكن تحضيرها مسبقًا لمشاركتها مع المجموعة:

شيفرة كلمة "بلوبرينتس" 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 يستعين 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 "يُفك التشفير".

يمكنكن أيضًا 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 LNPUB (وهذه ليست كلمة) حين "يُفك التشفير"، ولكن مثلا يمكنكن الآن "فكّ تشفير" التسلسل 43206 للتوصل إلى كلمة RINSE.

الرسائل القصيرة القديمة الطراز

إستخدمن صورة للوح 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 استخدامهن للوح المفاتيح هذا لكتابة كلمات متنوعة – أحد الأمثلة على ذلك التي يمكنكن الاستعانة بها قد تكون الطلب من كل مشاركة شرح كيفية استخدامها للوح المفاتيح لكتابة اسمها. على سبيل المثال، لكتابة اسم إحدى المشاركات: لينا

Lina، نكتب تسلسل الأرقام التالي 2 66 444 555.

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 يستخدمها الكثير من الناس في حياتهم اليومية هي "إيتش تي 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 الأوّل، عليكن الآن التوسّع وشرح المزيد من الأسس والممارسات للمجموعة:

طرق التشفير: خصصن الوقت الكافي لشرح كيفية عمل التشفير إستناداً إلى الأمثلة من الجزء الأوّل بالإضافة إلى عرض بعض الأمثلة عن صور ملتقطة عن شاشات لشكل البريد الإلكتروني المشفّر بواسطة "جي بي جي". شددن على بعض حالات تنفيذ التشفير الشائعة – وبشكلٍ 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 المفتاحين العام والخاص. إستعدن الأمثلة عن التطبيقات المذكورة آنفًا (إيتش تي بي إس، التشفير الكامل وجي بي جي/بي جي بي) وإشرحن أنه لكل واحدة من هذه التطبيقات مفاتيح خاصة مخزّنة و/أوظاهرة للمستخدم.

ممارسات التشفير: ألقين 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، يمكنكن مناقشة فوائد ومساوئ توقيع وتوزيع المفاتيح المتاحة للعموم. والوقت مناسب أيضًا لمناقشة المراسلات المشفرة تشفيرًا كاملاً في تطبيقات المحادثة كتطبيق سيجنال وواتساب وتليغرام- ذكرن المشاركات أن التشفير الكامل ليس دائمًا مفعّلًا بشكلٍ تلقائي على بعض هذه الخدمات.

النسخ الاحتياطية المشفّرة: إستنادًا إلى مثال التشفير بواسطة جي بي جي/بي جي بي المذكور أعلاه، إسألن المشاركات إذا كنّ يعتقدن أن القيام بنسخة احتياطية 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

الاتصالات المشفّرة

- **الأهداف:** تستند هذه الجلسة إلى محتويات التدريب السابقة المرتبطة بالتشفير، ناقلةً إلى المشاركات أهمية تشفير الاتصالات وفائدتها وتقديم الأدوات المهمة لذلك
- **الطول:** 50 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** متوسط
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أوتدريب مسبق
  - تعريف بمسألة التشفير (التشفير)
- **جلسات/تمارين ذات علاقة:**
  - تعريف بمسألة التشفير (التشفير)
  - الخصوصية (الخصوصية)
  - الحملات الآمنة على الإنترنت (المناصرة الآمنة على الإنترنت)
- **المواد اللازمة:**
  - شرائح (فيها النقاط المفتاحية الواردة أدناه)
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض

إدارة الجلسة

١. إبدأن الجلسة بمشاركة بعض الأمثلة المهمة عن حالات يكون فيها تشفير الاتصالات مفيدًا، 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.

٢. إحصرن النقاش الآن بالتحديد على الأدوات التي تسمح بتشفير الاتصالات: تطبيق سيجنال للاتصالات والرسائل، وتطبيق "ميت.جيتسي" https://meet.jitsi لاتصالات الفيديو وتوتانوتا أو جي بي جي و"ثندر بيرد" Thunderbird لرسائل البريد الإلكتروني. كلها أمثلة مفيدة لابد من مشاركتها.

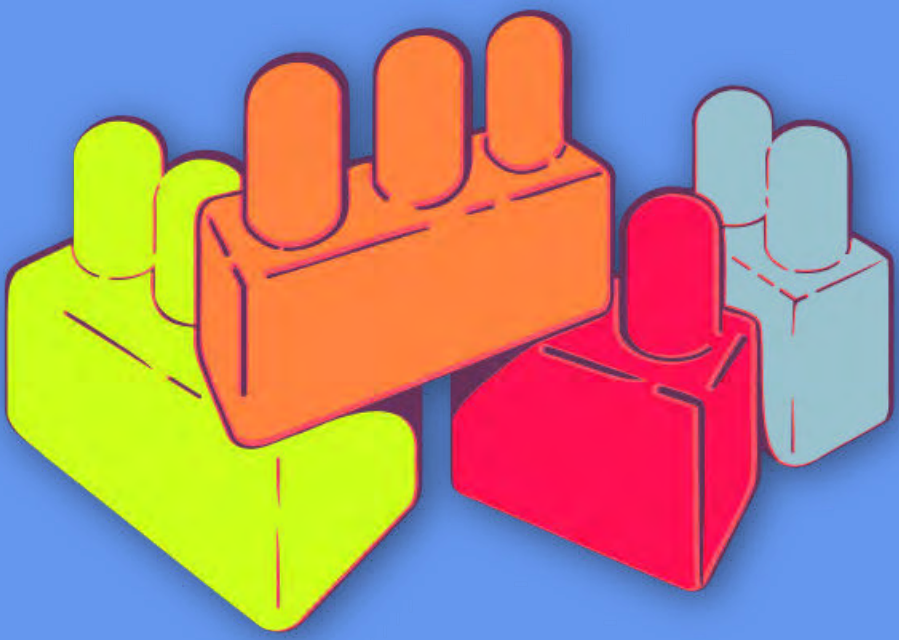
٣. إشرحن الفوائد الأمنية لهذه الأدوات للمجموعة، وبشكلٍ أساسي كيف تمكّن المستخدمين من الحد من إمكانية وصول الآخرين إلى اتصالاتهن؛ ومن ثمّ ناقشن الحالات التي قد يتعرض فيها أمن بيانات المستخدم لخطر الإنكشاف، حتى مع استخدام الاتصالات المشفّرة. إسألن المشاركات – كيف يمكن أن تتعرض محتويات بريد إلكتروني مشفّر بواسطة جي بي جي لخطر الإنكشاف بسبب تسجيل المفاتيح (keylogging) أوبرمجيات الخبيثة لإلتقاط صور الشاشة (screen-apturing malware) ؟ ما الذي قد يحدث في حال تمكن أحد الخصوم من الوصول إلى مفتاح جي بي جي خاص بمستخدم/ة – كيف يمكن للخصوم استخدامه للوصول إلى بياناتهن؟

٤. في حال كان الوقت المتوفر يسمح بذلك، لابد من توفير فرصة الممارسة التطبيقية للمشاركات على الأقلّ على واحدة من الأدوات المذكورة آنفًا في المرحلة الثانية. ومع أن الوقت قد لا يكون متاحًا لتعليم المجموعة كيفية إعداد تقنية جي بي جي/بي جي بي للبريد الإلكتروني، يمكنكن اختيار عرض اتصال فيديومحمي بتقنية إيتش تي تي بي إس عبر تطبيق "ميت.جيتسي"، أوأطلبن من المشاركات تثبيت تطبيق سيجنال على

هواتفهن للتدرّب على إرسال الرسائل المشفّرة إلى بعضهن البعض، أوتبادل الاتصالات الهاتفية المشفّرة.

المراجع

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



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 المشاركات.
- **الطول:** 90 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** متوسط
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أوتدريب مسبق
  - تعريف بمسألة التشفير (التشفير)
  - كيفية حماية حاسوبكن (أسس الأمن الرقمي،الجولة الأولى)
- **جلسات/تمارين ذات علاقة:**
  - الخصوصية (الخصوصية)
  - الحملات الآمنة على الإنترنت (المناصرة الآمنة على الإنترنت)
  - تعريف بمسألة التشفير (التشفير)
  - كيفية حماية حاسوبكن (أسس الأمن الرقمي،الجولة الأولى)

- **المواد اللازمة:**
  - شرائح (فيها النقاط المفتاحية الواردة أدناه)
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
  - نسخ مطبوعة عن نموذج النسخ الإحتياطي (أدناه)
  - مفاتيح يو إس بي أو نوع آخر من وسائط التخزين (لكل مشاركة)
- **التوصيات:** المشاركات في هذه الجلسة ستستخدمن إما برمجية "فيراكريبت" veracrypt أو "ماك كيبر" mackeeper (بحسب النظام التشغيلي الخاص بهن) للتدرّب على تشفير النسخ الاحتياطية للبيانات ووسائط التخزين – لتوفير الوقت، فكرن في الطلب من المشاركات تنزيل أي من هذه البرمجيات مسبقًا. بشكلٍ عام، ولا سيما للمبتدئات، لا ينصح بإجراء المشاركات لعملية تشفير شاملة للقرص الصلب على حاسوبهن الآن – عوضًا عن ذلك، يتوجب عليهن إختبار برمجيتي "فيراكريبت" أو "ماك كيبر" على وسيط تخزين خارجي (من قبيل مفتاح يو إس بي) باستخدام ملفات مزيّفة حضّرنها خصيصًا لهذه الجلسة. إذ حتمًا لا ترغبن في التعرّض لخطر فقدان إحدى المشاركات لإمكانية الوصول إلى أي بيانات خلال التدريب عن طريق الخطأ!

إدارة الجلسة

الجزء الأوّل – 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 أيضًا في تشفير القرص الصلب أووسيط التخزين حيث سيقمن بتخزين البيانات.

٢. شاركن مع المشاركات نموذج تنظيم النسخ الإحتياطي الوارد أدناه، وأطلبن منهن

البدء بملئه 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 تخزينهن للبيانات وعدد المرّات التي يجب فيها إنشاء نسخ احتياطية للبيانات.

نموذج تنظيم النسخ الإحتياطي

- نوع المعلومات
- الأهمية/القيمة
- ما وتيرة إنتاجها أوتغييرها؟
- 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 لائحتهن مجددًا – أثناء قيامهن بذلك، أطلبن منهن التفكير في ما قد يحدث في حال وصلت هذه المعلومات إلى أحد خصومهن، أوفي حال فقدن هذه المعلومات كلها. ما أثر ذلك عليهن شخصيًا وعلى منظمتهن؟

٤. والآن، قدّمن مفهوم التشفير للمجموعة – إشرحن لهن أنهن على الأرجح يجدن التشفير مرات عدّة 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 المنتقلة من النقطة "أ" إلى النقطة "ب") في حين أنهن في هذه الجلسة، ستناقشن تشفير البيانات "الثابتة" (أي البيانات المخزّنة في مكان واحد).

٥. كرن المشاركات بأنه طلب منهن تنزيل إما برمجية "فيراكريبت" أو برمجية "ماك كيبر" على حواسيبهن. إمنحن المشاركات الوقت اللازم لتثبيت هذه الأدوات وإختبارها،

بواسطة وسيط تخزين خارجي (من قبيل مفاتيح يو إس بي) وملفات مزيّفة حضّرنها خصيصًا لهذه الجلسة. لا ينصح بإجراء عملية تشفير شاملة لقرص الحاسوب الصلب الآن، لا سيما للمشاركات المبتدئات - إذ حتمًا لا ترغبن 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
- **المستوى المهاري:** متوسط
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أوتدريب مسبق
  - تعريف بمسألة التشفير (التشفير)
  - التخزين والتشفير (أسس الأمن الرقمي،الجولة الثانية)
- **جلسات/تمارين ذات علاقة:**
  - وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)
  - البرمجيات الخبيثة والفيروسات (أسس الأمن الرقمي،الجولة الأولى)
  - الخصوصية (الخصوصية)
  - المزيد من الهويات الإلكترونية! (عدم الكشف عن الهوية)

- التخزين والتشفير (أسس الأمن الرقمي،الجولة الثانية)

• **المواد اللازمة:**

- شرائح (فيها النقاط المفتاحية الواردة أدناه)
- مفاتيح يو إس بي مجهّزة بنظامي تايلز وأوبونتو Ubuntu القابلين لإعادة التشغيل.

• **التوصيات:** فكرن في جلب مفاتيح يو إس بي مجهّزة بنظام تشغيل لكل مشاركة على أن يحتفظن بها؛ وإلّا جهزن حاسوبًا لتتدرب المشاركات عليه (أو إثنين في حال عرضتن نظامي تايلز وأوبونتو التشغيليين) - وحتى لو كان الهدف من النشاط تشغيل نظامي تايلز أو أوبونتو من مفتاح يو إس بي مجهّز بنظام تشغيل، عوضًا عن تثبيته، قد لا تشعر بعض المشاركات بالإرتياح لاستعمال حاسوبهن الخاص لإختباره. من الممكن أيضًا تغيير ذلك بحيث يسهل إدخاله إلى أي جلسة مخصصة لناشطات لا يخفن من شيء في ورشتكن التدريبية، يرغبن في تغيير الأنظمة التشغيلية بالكامل من ماك أو ويندوز إلى نظام كنظام أوبونتو من شركة لينوكس linux.

إدارة الجلسة

الجزء الأوّل - تبديد الخرافات

الجزء الأوّل - 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 مستخدميها. في حال قدمتن جلسة وجهات النظر الشخصية حيال الأمن للمشاركات، يمكنكن تذكيرهن بما يلي من التأكيدات الختامية:

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

الجزء الثاني – ما الذي نعنيه فعليا بإعادة الضبط؟

٢. كررن للمجموعة هذا التأكيد من المرحلة السابقة، وشددن على الجملة الأخيرة منه "يمكننا دومًا إعادة ضبطها" – ماذا يعني ذلك؟ إشرحن لهن ذلك عبر تقديم السيناريو التالي:

لعلكن في إحدى محطات مسيرتكن مع الأمن الرقمي، شعرتن أنكن تقمن بكل شيء بالطريقة الخاطئة.

تنظرن إلى حاسوبكن – هو مليء بالبرمجيات المقرصنة والأفلام والبرامج التلفزيونية المنزّلة عبر منصة "تورينت" والملفات الأخرى المبعثرة التي لا تتذكرن حتى أنكن نزّلتنها.

إستخدمتن مفاتيح اليو إس بي من دون تمييز – على حاسوبكن المحمول، وعلى حواسيب وآلات طباعة في مقاهي إنترنت، وربما لا تقمن دائمًا بإخراجها بالطريقة الصحيحة حين تنتهين من استخدامها.

ربما إنفصلتن مؤخرًا عن شخصٍ ما تعرفن جيّدًا أنه/ها كان يفتح حاسوبكن في غيابكن – وربما قام/ت بتخمين كلمة السرّ أو حتى أعطيتنه/ها إياها بأنفسكن.

والآن، تشعرن بأنكن فقدتن السيطرة – من يعرف ما نوع الفيروسات الموجودة على قرصكن الصلب، أو من يا ترى له القدرة على الوصول إلى معلوماتكن؟

ولكن على فكرة، ذلك ليس مشكلة كبيرة! لم يفت الأوان بعد لفتح صفحة جديدة. هل ترغبن في فتح صفحة جديدة؟ هذه الجلسة معدّة خصيصًا لكنّ إذًا!

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

لا تنسين 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 جدًا عن عملية إعادة الضبط في حال لم تكن المشاركات جاهزات لها، أو في حال لم يقمن بإجراء نسخ احتياطية لبياناتهن مؤخرًا – وقد يحتجن لحواسيبهن المحمولة بما أنهن يرغبن حاليًا 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 يشكّل محطة تحضيرية مهمة في حال قررن إجراء عملية إعادة ضبط لاحقًا.

الجزء الثالث – التحقق: هل تحتجن لإنشاء نسخ احتياطية؟

٤. يفضّل أن تكنّ قد قدمتن قبل الآن جلسة التخزين والتشفير للمشاركات بما أنها تتناول نقاطًا 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.

اختياري: كتذكير سريع بجلسة التخزين والتشفير، إسألن المشاركات - كم مرّة في السنة يقمن بنسخ إحتياطي 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 المعلومات التي يُنشأ لها نسخ احتياطية، والتفكير أيضًا 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، لابد من تناول مسألة مهمة هي العلاقة بين إعادة التشغيل وإعادة الضبط فربما استخدم هذان المصطلحان من دون تمييز بينهما طوال هذه الجلسة:

يدلّ هذان المصطلحان إلى عمليتين تشبه بعضهما إلى حدٍ 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 أيضًا يجب فهمها من أجل الممارسة التطبيقية لأنظمة التشغيل البديلة التي ستجرى في الجزء التالي من الجلسة.

٦. لمزيد من التوضيح للفكرة الواردة أعلاه، قدمن أنظمة تشغيل تايلز وأوبونتوإلى 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 ووينـدوز – في هذه الجلسة، سيركز الجزء الخاص بالممارسة التطبيقية على تشغيل هذين النظامين التشغيليين من مفتاح يو إس بي.

الجزء الخامس – الأنظمة التشغيلية الحيّة

٧. قد يطرح عليكن سؤالاً من قبيل: كيف يمكننا استخدام النظام التشغيلي الجديد على حواسيبنا المحمولة من دون التخلّص من الذي نستخدمه الآن؟ ماذا سيحدث لبياناتنا؟ عليكن 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 الحيّة؛ ومن الممكن إعداد أوبونتوللعمل 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 ديبيان Debian، هو إحدى النسخ الأكثر شعبية وهو يشكّل 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 الدي في 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 تشغلها معظم الحواسيب حيت يتم تشغيلها. يستخدم هذا النظام لإجراء عمليات إختبار ذاتية على الأنظمة والأجهزة لضمان عملها بشكلٍ 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 وفقه تحميل المعلومات من هذه الأجهزة. عادةً القرص الصلب في الحاسوب هو الجهاز الأوّل في تسلسل التشغيل، ومنه يتم تحميل نظام التشغيل. ولكن من الممكن تغيير تسلسل التشغيل ليُحمّل معلومات من أجهزة خارجية قابلة للإزالة أوّلاً كأقراص الدي في دي أو مفاتيح اليو إس بي.

الجزء السادس – الممارسة التطبيقية

٨. للبدء بالجزء المخصص للممارسة التطبيقية من هذه الجلسة، قسمن المشاركات إلى مجموعتين على الأقل. قدمن لكل مجموعة حاسوبًا ليجربن عليه تشغيل نظام أوبونتو أو تايلز من مفتاح يو إس بي معدّ مسبقًا، أو، في حال توفر لديكن العدد الكافي من مفاتيح اليو إس بي المعدّة مسبقًا لكل المشاركات، عندها سيتمكنّ من التدرّب كل واحدةٍ 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 المشاركات 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 تفهم 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 خيارًا لفتح "صفحة جديدة" على حواسيب المشاركات في حال التعرّض لهجوم برمجيات خبيثة أو أي فقدان آخر للسيطرة، ولكن إحرصن أيضًا 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

العنف على الإنترنت ضد النساء

باب ٣٣

طيف الآراء

- **الأهداف:** يوفر هذا التمرين طريقة مفيدة للمشاركات للتعرّف على أفكار بعضهن البعض بشأن مسائل محددة، عبر إنشاء "طيف من الآراء" في مكان التدريب.
- **الطول:** 90 دقيقة
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - إنترنت نسوي (العنف ضد المرأة على الإنترنت)
- **المواد اللازمة:**
  - غرفة كبيرة أومساحة في الهواء الطلق
  - أنفسكن!

محتوى هذا التمرين وضعته ماريل غارسيا Mariel Garcia من منظمة سوشل تي آي سي SocialTIC وسبيروس موناستيريوتيس Spyros Monastiriotis من منظمة تاكتيكل تكنولوجي كوليكتيف Tactical Technology Collective

إدارة التمرين

١. إبدأن الجلسة بإرشاد المجموعة إلى مكان طرفي الطيف – في حال استخدام مكان داخلي، يمكن استخدام الجهتين المعاكستين من الغرفة لهذا الغرض؛ أما بالنسبة للمساحات في الهواء الطلق، يمكن الإستعانة بشجرتين أو حائطين أوأي معالم آخرى.

٢. إشرحن لهن أن كل طرفٍ منهما يدلّ على رأي عام - حددن أن إحدى الجهتين ستمثّل الرأي "الموافق جدًا" والجهة الأخرى ستمثّل الرأي "المعارض بشدّة".

٣. والآن، إشرحن لهن سير التمرين – ستقرأن عبارات بصوتٍ عالٍ (لابد من تسميتها بالعبارات وليس بالأسئلة)، ومن ثمّ تكرارها؛ ومن بعدها، تقمن المشاركات بترتيب مواقعهن وفقًا لطيف الآراء من "موافق جدًا" إلى "معارض بشدّة" بحيث تعبرن عن مدى أهمية العبارة الذي تمت قراءتها.

٤. ذكرن المشاركات أنهن لسن مضطرات لاختيار الجهة القصوى المعينة من طيف الآراء أو الجهة الثانية؛ يمكنهن أيضًا الوقوف في منتصف المساحة في حال لم يكوّنّ رأيًا في موضوعٍ ما، أو يمكنهن الوقوف في أي موقع آخر يشير إلى مدى موافقتهن أو رفضهن للعبارة

٥. ي طيف الآراء هذا، ستقرأن بصوتٍ عالٍ عبارات عدّة مرتبطة بالأمن الرقمي وتجارب النساء على الإنترنت – إليكن في ما يلي بعض الأمثلة على العبارات التي يمكنكنّ استخدامها:

- لا يوجد سبب وجيه لمشاركة أي شخص لكلمة سرّ بريده الإلكتروني/حساب وسائل التواصل الاجتماعي.
- أحيانًا،لابد لنا كنساء أن نتفادى مشاركة بعض الآراء على الإنترنت .
- الناشطات والناشطون يواجهون نوع العنف ذاته الذي يؤدي إلى نوع من أنواع العنف والتهديدات على الإنترنت.
- يصبح عملي مستحيلًا في حال عدم توفر إمكانية وصول آمنة إلى المساحات

الإلكترونية.

٦. بعد أن تنتهي المشاركات من ترتيب تمركزهن من بعد الإدلاء بعبارة ما، أطلبن من مجموعات من إثنتين إلى ثلاث مشاركات عن سبب اختيارهن لمكان وقوفهن فقد يحوّل ذلك النقاشات إلى نقاشات مثيرة للاهتمام.

٧. يمكنكن أيضًا 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
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - قصتها مع التكنولوجيا (إعادة النظر بعلاقتنا بالتكنولوجيا)
  - العنف الرمزيّ (العنف ضد المرأة على الإنترنت)
- **المواد اللازمة:**
  - أوراق لوح ورقي
  - أقلام خطاطة ملونة
  - نسخ عن مستند مبادئ الإنترنت النسوي للمشاركات

إدارة التمرين

الجزء الأوّل - التوعية

١. إبدأن 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 معًا ببعض العوائق التي تواجهها النساء في أغلب الأحيان حين يحاولن الوصول إلى التكنولوجيا واستخدامها، أو المشاركة بشكلٍ فاعل في مساحات الإنترنت. يمكنهن القيام بذلك ضمن مجموعة واحدة أو ضمن مجموعات صغيرة – الخيار يعود لكن. سجّلن العوائق التي تذكرها المجموعة على ورقة كبيرة من أوراق اللوح الورقيّ.

٣. من بعد الإنتهاء من عملية التفكير والمناقشة، شاركن بعض الإحصائيات العالمية التالية مع المشاركات – وإن أمكن، حاولن أيضًا ذكر إحصائيات خاصة ببلد معيّن أو منطقة معيّنة مرتبطة ببيئة المشاركات:

- نسب الاستخدام و الوصول 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 بما لا يقل عن 28 في المئة من الرواتب التي يحصل عليها الرجال من المستوى العلمي 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 مجانًا لاستخدام الجميع؟

الجزء الثاني – المبادئ النسوية للإنترنت

٥. والآن قدمن 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 والجندرية ليتمكنّ من التمتع 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/reports_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:** 45-30 دقيقة
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - طيف الآراء (العنف ضد المرأة على الإنترنت)
  - إنترنت نسوي (العنف ضد المرأة على الإنترنت)
- **المواد اللازمة:**
  - شريط لاصق
  - ألواح ورقية
  - أقلام أو أقلام رصاص
  - أوراق ملوّنة

- قصاصات لاصقة

إدارة التمرين

الجزء الأوّل - ما هو العنف الرمزي؟

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

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

وهذا يعني أننا كنساء نُحمّل مسؤولية أي عنف نواجهه، فيولّد بدوره الخوف أو حتى الهلع - ينتج هذا الخوف أو الهلع "خارطة ذهنية بالأماكن الممنوعة" 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 خطى وراءنا؛ ممارسة الرقابة الذاتية لا شعوريًا 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 أبدًا في الوقت عينه إستراتيجيات وموارد لمعالجة ذلك العنف (عدا ردود الفعل المشروطة المذكورة أعلاه)، ولا إستراتيجيات وموارد للتمتع والسيطرة على المساحات المتاحة أو للتحرّك والتعبير عن أنفسنا وعن جسدنا وجنسانيتنا بحريّة، إلخ.

ينتج عن العنف الرمزي مساحات وحالات ممنوعة على النساء، مما يمنعنا عن حقنا الأساسي في الأمن والتحرّك بحرية، وما يزيد من الطين بلة هو الحصانة المعطاة غالبًا للمعتدين، ففي أغلب الأحيان، لا يخضعون للتحقيق أو المساءلة بل يصنفون "كمجانين" أو كغير قادرين على التحكّم أو تحمّل مسؤولية أفعالهم.

وقد يتوجب عليكن هنا مناقشة صور عن حالات عنف ضد النساء (إن كان رمزيًا أو غير ذلك) توزّع و تطبّع 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 عدّلنها بسبب العنف الرمزي الذي يختبرنه كنساء في مساحات الواقع والفضاء الرقمي على حد سواء. من بعد الإنتهاء من ذلك، إجمعن القصاصات اللاصقة وإقرأن بعض الأمثلة المدوّنة بصوتٍ عالٍ – ناقشنها معًا كمجموعة، وعلّقن على المحفزات المحتملة لتغيير هذه السلوكيات والمخاوف 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 أومقبولة إلى حدٍ ما.

- **"العجز الملقّن"**: 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، تتكيّف الحالة النفسية مع ذلك، مضحية بالتالي بقدرتها على التحكّم بتلك النتيجة (فتتقبّله وتعتبره طبيعيًا عوضًا 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.
- الإعتراف 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 أبدًا 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

- **الأهداف:** في هذه الجلسة، ستقدمن للمشاركات بعض النصائح حول العنف على الإنترنت في منصات التواصل الاجتماعي مثل فايسبوك وتويتر.
- **الطول:** 40 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - الحملات الآمنة على الإنترنت (المناصرة الآمنة على الإنترنت)
  - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟ (الخصوصية)
  - لنبدأ بتوثيق الحالات! (العنف ضد المرأة على الإنترنت)
- **المواد اللازمة:**
  - جهاز عرض وشرائح عرض
  - قصاصات ورقية لاصقة
  - حاسوب لكل مشاركتين (إن أمكن)

• **التوصيات:** يوصى بهذه الجلسة لمجموعات النساء اللواتي تعرّضن للتحرّش على الإنترنت أو المشاركات في حملات على الإنترنت.

منصات التواصل الاجتماعي

إدارة الجلسة

١. إبدأن الجلسة بطرح الأسئلة التالية على المشاركات:

• هل يعرفن بأي جماعات نسائية أو ناشطات تعرّضن للتحرّش على الإنترنت؟
• في حال كنّ يعرفن أيًا منها، على أي منصات حصلت حالات التحرّش؟

أطلبن منهن تقديم أمثلة عن تكتيكات شهدن على استخدامها، من قبل تلك المجموعات أوالأفراد لمعالجة أو مكافحة التحرّش على الإنترنت، أو التكتيكات التي إستعنّ بها هنّ. أطلبن 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 التحرّش:

• يوصي موقع فايسبوك بالإشارة إلى التعليق أو المنشورالمحدد (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
• حجب المتحرشين سيمنعهم من إرسال طلبات الصداقة أو المتابعة، ومن بدء الأحاديث أو إرسال الرسائل والإطلاع على المستجدات المنشورة على حائط المستخدم/ة. لا يُبلغ المستخدمين بحجبهم، ولكن يمكنهم أن يلاحظوا حصول ذلك، في حال لم يعودوا قادرين فجأة على التواصل مع ضحيتهم. إلتقطن صور للشاشة قبل حجب المتحرشين على المنصات للحصول على أدلة توثق التحرّش –

فما إن يتم حجبهم، يصبح من الصعب جدًا جمع الأدلة الداعمة، التي يُطلب من المستخدمين عادةً تقديمها خلال التحقيق في الحادث (قد يتوجب عليكن تعليم المشاركات كيفية إلتقاط 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 المتحرّش. ومن الممكن على تويتر التبليغ عن تغريدة واحدة أو صفحة شخصية كاملة.

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

٣. خلال هذا الجزء من الجلسة، يتوجب عليكن أيضًا تعليم المشاركات كيفية حجب المستخدمين والتبليغ عن الصفحات الشخصية أو المنشورات على فايسبوك وتويتر، إلى جانب أي منصة تواصل إجتماعي أخرى يستخدمنها كثيرًا. إحرصن على البحث عن هذه التفاصيل قبل التدريب من أجل أن تعرفن المستجدات، فلسوء الحظ تتغيّر هذه الإجراءات كثيرًا (تمامًا 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 أوالمزعجين – على سبيل المثال، عليهن محاولة توثيق أي منشورات أوصفحات شخصية على فايسبوك، تُرتكب من خلالها حالات التحرّش ومن ثمّ تقديم التقارير عبر الآلية المحددة.

المراجع

- https://karisma.org.co/descargar/manualseguridadtw

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
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - التبليغ عن الإساءات على منصات التواصل الاجتماعي (العنف ضد المرأة على الإنترنت)
  - الاستقصاء عن المعلومات الشخصية الخاصة بالمتصيد (العنف ضد المرأة على الإنترنت)
- **المواد اللازمة:**
  - شرائح (فيها النقاط المفتاحية الواردة أدناه)
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
  - نسخ مطبوعة عن نماذج سجّل التوثيق (أدناه)

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

إدارة الجلسة

الجزء الأوّل – ما أهمية التوثيق؟

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

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

ما هو الحادث؟ الحادث هوأي تطوّر يطرأ إما على الإنترنت أو في الواقع قد يشكّل إساءةً أو تحرشًا – تصنيف التطوّر على أنه حادث أم لا، يعتمد كثيرًا على البيئة والظروف التي طرأ فيها وشدّة أثره بهذه العوامل. على سبيل المثال، في حال تلقيتن بريدًا إلكترونيًا يبدو وكأنه محاولة تصيّد – وأنتن معتادات على تلقيها غالبًا – قد لا يكون ذلك مهمًا بما فيه الكفاية لإعتباره حادثًا، ولكن في حال كانت منظمتكن تستعد لإطلاق حملة مهمة وبدأتن بتلقي أعدادًا كبيرة جدًا غير معتادة منها، قد يشكّل ذلك حادثًا ولابد من توثيقه. مثال آخر على ذلك، في حال كانت منظمتكن تستعد لإطلاق حملة مهمة وبدأتن بتلقي عدد هائل من طلبات الصداقة على فايسبوك من غرباء.

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

ما الذي يجعل عملية التوثيق بهذه الأهمية؟ التوثيق مفيد كمرجع يستخدم لاحقًا حين تحاولن فهم الوضع بأكمله وربط حوادث مختلفة ببعضها البعض طرأت خلال إطار زمني محدد أوطالت عددًا من الأشخاص من المنظمة نفسها.

قد يكشف التوثيق أنماطاً معيّنة من الإساءة أوالهجمات الأخرى على الإنترنت، ربما لم تكنّ لتلاحظنها لولاه،وعبر تقديم مجموعة من الأدلة المترابطة. إكتشاف هذه الأنماط يساعدنا في تحديد هوية الخصوم، أو في فهم مجريات الأمور والعلاقة بين أنواع معيّنة من الحوادث، وأنواع معينة من الأعمال التي تقمن بها أنتن أو منظمتكن. 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.

الجزء الثاني – كيفية توثيق الحوادث؟

٢. بعد الإنتهاء من مراجعة الفقرات الواردة أعلاه عن التوثيق ومعرفة أسباب التوثيق وأهميته، يمكنكن توزيع نسخ مطبوعة من نماذج سجّل التوثيق أدناه على المشاركات.

٣. أذكرن للمشاركات أن هذه النماذج توفر مثالًا واحدًا فقط عن أنواع المعلومات المهمة التي لابد من جمعها في عملية توثيق الحوادث. ولهن الحريّة في إضافة أو إزالة أي خانة وفقًا لتقديرهن حين يقمن بوضع نماذج خاصة ببيئة عملهن في المستقبل. 4. في ما يلي نموذجان، الأوّل مخصص لتوثيق الحوادث على الإنترنت، والثاني مخصص للحوادث في الواقع خارج الإنترنت:

نموذج سجل التوثيق (على الإنترنت)

التاريخ
التوقيت
ملخص مجريات الحادث

المنصة
الرابط (URL)
صورة الشاشة (اسم الملف أو نسخ/لصق)
توصيف محتوى صورة الشاشة
مستوى الخطر
إجراءات المتابعة
ملاحظات

نموذج سجل التوثيق (في الواقع)

التاريخ
التوقيت
المكان
ملخص مجريات الحادث
الأشخاص المعنيين/ات
مستوى الخطر
إجراءات المتابعة
ملاحظات

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

٥. إحرصن على التركيز على خانة مستوى الخطر، فهذه الخانة ذاتية بامتياز وأقل وضوحًا من الخانات الأخرى. وكيفية تعريف المشاركات و/أوالمنظمات لمستويات الخطر مرتبط إلى حدٍ 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 معًا) عند التعريف بالخطر في هذه البيئة.

اختياري: إما قبل أو مباشرة بعد هذه الجلسة، قمن بتمرين نماذج المخاطر القائمة على النوع الاجتماعي مع المشاركات. خلال ذلك التمرين، ستتسنى فرصة أفضل للمجموعة للتعريف بمستويات الخطر في بيئتهن الخاصة – ويمكنهن تطبيق هذه التعريفات للمخاطر في سجلات التوثيق الخاصة بهن.

٦. وختامًا، لابد من التشديد أيضًا على خانة إجراءات المتابعة خلال هذا الجزء من الجلسة. فإجراءات المتابعة في هي فعليًا الخطوة التالية المتخذة لمعالجة الحادث الحالي (مثلا تقديم تقرير تبليغ على فايسبوك)، أو إجراء سينفذ لمنع أي حادث مماثل في المستقبل أو التقليص من أثره.

اختياري: إما قبل أو مباشرة بعد هذه الجلسة، قمن بجلسة الخطط والبروتوكولات الأمنية الخاصة بالمنظمة مع المشاركات. خلال هذا التمرين، ، ستتسنى فرصة أفضل للمجموعة لتحديد الخطط والبروتوكولات الأمنية الخاصة بالتعامل مع مخاطر معروفة أو محتملة معيّنة – لابد من خطوات مشابهة عند التخطيط لإجراءات متابعة الحوادث.

الجزء الثالث – وضع سجلات التوثيق

٧. أطلبن من المشاركات البدء بملء نماذج سجلهن بشكلٍ فرديّ – بمنحهن من 10 إلى 15 دقائق لملء أكبر قدر ممكن من الخانات. يمكنهن ملئ الخانات بمعلومات مفصّلة عن الحوادث الفعلية التي تعرضن لها في حال رغبن في ذلك، ويمكنهن أيضًا استخدام أمثلة إفتراضية للتدرّب على ملء النماذج.

٨. من بعد أن ينتهين من وضع المسودة الأولى للسجل، أطلبن منهن تشكيل مجموعات من شخصين ومشاركة الحوادث التي سجلنها مع شريكاتهن – في هذه المرحلة، يفضّل 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 أتحن لهن إمكانية العمل وحدهن إن أردن ذلك.

الجزء الرابع – ممارسات ونصائح عن كيفية الحفاظ على سجلات التوثيق

٩. ذكرن 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 ستوكل مهمة جمع المعلومات للسجّل 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 تولي شخص آخر مهمة توثيق الحادث.

١٠. شجعن المشاركات على إختبار سبل عمل مختلفة لجعل عملية تحديث سجلات التوثيق الخاصة بهن أكثر كفاءة وفعالية – قد تتوفر طرق لجعل بعض الإجراءات تتم بشكل أتوماتيكي، 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 عِبر أساسية من النقاش أو أفكار، بشأن كيفية المحافظة على السجل وجعل عملية تحديثه أكثر سهولة.

باب ٣٨

الاستقصاء عن المعلومات الشخصية الخاصة بالمتصيد

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

- ماذا يمكن لبياناتكن الوصفية أن تفصح عنكن؟ (المناصرة الآمنة على الإنترنت)
- لنبدأ بتوثيق الحالات! (العنف ضد المرأة على الإنترنت)

• **المواد اللازمة:**
- شرائح (فيها النقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
- نسخ مطبوعة عن نموذج سجّل التوثيق (على الإنترنت)

• **التوصيات:** يوصى بهذا التمرين لمجموعات المدافعات عن حقوق الإنسان اللواتي يتعرضن حالياً لحالات تحرّش/ تهديد على الإنترنت، أو اللواتي تعرضن مؤخراً لها. مع أن هذا ليس مطلوباً ، ولكن يفضل إجراء هذا التمرين من بعد جلسة "لنبدأ بتوثيق الحالات!" يفضل إجراء هذا التمرين والمشاركات معهن أجهزتهن الخاصة أو حواسيبهن. قد يتوجب عليكن تقسيم هذا التمرين إلى جزئين، فهو تمرين طويل ومكثّف. كما يمكنكن تنفيذه من دون تقسيمه ولكن مع تخصيص إستراحة أطول من العادة عند منتصفه.

هذا التمرين مستقى من نشاط وضعه كل من إنديرا كورنيليو Indira Cornelio (من سوشل تي آي سي SocialTIC) وفي ريكويم Phi Requiem (#سيغورياداديخيتال SeguridadDigital) بالتعاون مع مشروع "تايك باك ذا تيك"(لنسترد التكنولوجيا) للجمعية التقدمية للاتصالات

إدارة التمرين

الجزء الأوّل – الاستقصاء ما هو؟

١. إشرحن للمشاركات ماهية الاستقصاء – 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 الاستقصاء يستخدم أحياناً ضد أشخاص للإنتقام منهم، وغالباً ما يستخدم لمضايقة 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 الاستقصاء كممارسة فضلى (أو عدم التوصية باستخدام وسائل غير قانونية أومريبة للقيام بذلك) – الاستقصاء هذا يعني نشر معلومات شخصية للعلن، لذا لابد من التشديد على أن "نشر" هوية أومعلومات شخص ما غير ضروري. هدف هذا التمرين هو تعليم المشاركات كيفية جمع هذا النوع من المعلومات لمساعدتهن على إتخاذ قرارات بشأن كيفية التعامل مع حالات الإساءة أو التحرّش.

٣. ختامًا، إشرحن أيضًا أنه لابد للمشاركات من تذكّر ما يعرفنه 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 عددًا من الدوافع الممكنة قبل أن تبدأ المشاركات بالتمرين:

- هل ذلك لمعرفة هويتهم الحقيقية؟
- لفهم دوافع تحرشهم بهن؟
- لمعرفة إن كانوا يتحرشون بمدافعات أخريات عن حقوق الإنسان أيضًا؟
- لمعرفة إن كان وراء التحرش شخص واحد أوعدّة 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 وضحن 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 وللتبليغ عن التحرّش. في حال لم تخضع المجموعة بعد للجلسة المذكورة آنفًا، إشرحن لهن أنكن ستطلعنهن خلال هذا التمرين على طريقة لمتابعة حوادث التحرّش.

الجزء الثالث – أنواع مختلفة من الأشخاص ودوافع مختلفة

٦. شاركن بعض قصص وتجارب ناشطات أوصحافيات مع التحرّش على الإنترنت. حاولن إيجاد حالات ذات صلة ببيئة المشاركات وتظهر أنواع مختلفة من المتحرشين ودوافع مختلفة لأفعالهم.

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

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

الجزء الرابع – توثيق الحوادث والتهديدات

٩. 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 يمكنكن الإنتقال إلى الجزء الخامس – التحضير للعمل.

١٠. في حال لم تخضع المشاركات بعد لجلسة لنبدأ بتوثيق الحالات!، إبدأن أولاً بشرح النقاط التالية، التي تركّز على أهمية ممارسة التوثيق في معالجة مشكلة التحرّش على الإنترنت:

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

ما هو الحادث؟ الحادث هوأي تطوّر يطرأ إما على الإنترنت أوفي الواقع قد يشكّل إساءةً أو تحرشًا – تصنيف التطوّر على أنه حادث أم لا، يعتمد كثيرًا على البيئة والظروف التي طرأ فيها وشدّة تأثره بهذه العوامل. على سبيل المثال، في حال تلقيتن بريدًا إلكترونيًا يبدو وكأنه محاولة تصيّد – وأنتن معتادات على تلقيها غالبًا – قد لا يكون ذلك مهمًا بما فيه الكفاية لإعتباره حادثًا، ولكن في حال كانت منظمتكن تستعد لإطلاق حملة مهمة وبدأتن بتلقي أعداد كبيرة جدًا غير معتادة منها، قد يشكّل ذلك حادثًا ولابد من توثيقه. مثال آخر على ذلك، في حال كانت منظمتكن 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 الإحتفاظ بسجل بكل الحوادث التي تطرأ، بطريقة منظمة ستساعدكن على الإحتفاظ بمعلومات وأدلة مهمة عن كل حادث، يمكن استخدامها لاحقًا أو اعتمادها كمراجع.

ما الذي يجعل عملية التوثيق بهذه الأهمية؟ التوثيق مفيد كمرجع يستخدم لاحقًا حين تحاولن فهم الوضع بأكمله وربط حوادث مختلفة ببعضها البعض طرأت خلال إطار زمني محدد أو طالت عددًا من الأشخاص من المنظمة نفسها. قد يكشف التوثيق أنماط معيّنة من الإساءة أو الهجمات الأخرى على الإنترنت، ربما لم تكنّ لتلاحظنها لولاه، عبر تقديم مجموعة من الأدلة المترابطة. إكتشاف هذه الأنماط يساعدنا في تحديد هوية الخصوم أو في فهم مجريات الأمور والعلاقة بين أنواع معيّنة من الحوادث وأنواع معينة من الأعمال التي تقمن بها أنتن أو منظمتكن. 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، يمكنكن تعريف المشاركات بسجل التوثيق – في هذا التمرين، يمكنكن الإكتفاء باستخدام النسخة المخصصة للإنترنت، التي يفترض أنكن حضرتن نسخ مطبوعة منها للمجموعة – راجعن النموذج أدناه:

نموذج سجل التوثيق (على الإنترنت)

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

١٢. أذكرن للمشاركات أن هذا النموذج يوفر مثالًا واحدًا فقط عن أنواع المعلومات المهمة التي لابد من جمعها في عملية جمع المعلومات حول المتحرشين. ولهن الحريّة في إضافة أو إزالة أي خانة وفقًا 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 واحدةٍ منها (أي ما يجب أن تتابعه المشاركات لملء كل واحدة منها).

١٤. إحرصن على التركيز على خانة مستوى الخطر، فهذه الخانة ذاتية بامتياز وأقل وضوحًا من الخانات الأخرى. وكيفية تعريف المشاركات و/أو المنظمات لمستويات الخطر مرتبط إلى حدٍ 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 معًا) عند تعريف بالخطر في هذه البيئة.

١٥. أطلبن من المشاركات البدء بملء نماذج سجلهن بشكلٍ فرديّ – إمنحنهن من 10 إلى 15 دقائق لملء أكبر قدر ممكن من الخانات. يمكنهن ملء الخانات بمعلومات مفصّلة عن الحوادث الفعلية التي تعرضن لها في حال رغبن في ذلك، ويمكنهن أيضًا 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 أويجدنه أثناء الاستقصاء عن المتحرّش – فقد تكون هذه محاولات تصيّد (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 حاليًا للتحرّش على الإنترنت، يفضل أن يتفادين لفت أي إنتباه غير ضروري إلى أنفسهن قد يؤدي إلى تحرّش لاحقًا.

١٧. وجهّن 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 سجلّ التوثيق)؛
- بعد ذلك، عليهن اختيار المتصفّح الذي سيستخدمنه في تحقيقهن – وعلى هذا المتصفّح، عليهن تسجيل خروجهن من كل حساباتهن، وحذف سجّل تصفحهن وملفات تعريف الإرتباط عليه. يمكنهن أيضًا التفكير في استخدام متصفح تور لهذا النشاط، في حال

سبق لكن أن عرفتهن به؛

- يمكنهن أيضًا التفكير في إنشاء هويات إلكترونية أو صفحات شخصية جديدة لإجراء هذا النشاط (حسابات بأسماء مستعارة على فايسبوك أو تويتر، أو حساب جي مايل مزيّف) – ذكرنهن بضرورة الإنتباه إلى عدم استخدام أي معلومات في هذه الحسابات قد تستخدم لربطها بهوياتهن الحقيقية!
- شددن على أهمية تسجيل الملاحظات خلال هذه العملية – ذكرن المجموعة بما ناقشتنّه عن تناولكن أهمية ممارسات التوثيق.
- أطلبن من المشاركات إنشاء ملف مخصص على حواسيبهن لجمع وتخزين المعلومات والأدلة التي يجمعنها – قد تشتمل تلك على صور رمزية أو صور شاشات أو أسماء مستخدمين أو حسابات بريد إلكتروني أو حسابات على مواقع التواصل الاجتماعي أو تعليقات على منتديات أو أي ذكر لأمكان تواجدهم الممكنة أو جهات اتصال معروفة أخرى.

الجزء السابع – الأدوات المفيدة

١٨. والآن يمكنكن 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، أومستند يرد فيه لائحة 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[١] Duck Duck Go;

[١] https://duckduckgo.com

- بحث متقدم على تويتر[٢] Advanced search on Twitter;
- الإطلاع على موقع Whois.net في حال تمكّن من إيجاد معلومات ناشئة عن موقع للتأكد من توفر أي معلومات عن الشخص المالك للمجال
- [٣] Google reverse image search: محرّك البحث عن الصور من غوغل في حال تلقيهن صورًا أورسومات يمكنهن البحث من خلال الصور هذه
- أدوات خاصة بالبيانات الوصفية في حال تلقيهن صورًا أو رسومات، يمكنهن التحقق من توفر بيانات وصفية:
  - ميتاشيلد[٤] MetaShield
  - ميتابيكس[٥] MetaPicz
  - سوشل منشن[٦] Social Mention;
  - فولوور وونك[٧] Follower Wonk;
  - نايم تشيك[٨] NameCheck;

٢٠. إشرحن أيضًا أنه من الممكن للمشاركات بناء أنظمة مراقبة مصغّرة لتعقّب المعلومات على الإنترنت: هذا مفيد جدًا في تعقّب صفحات شخصية أو أسماء مستخدمين أو هاشتاغات معيّنة:

- موقع آي إف تي تي[٩] IFTTT – بالنسبة لهذا الموقع، إشرحن كيف أنه يسمح للمستخدمين بربط تويتر بغوغل درايف من أجل التمكن من تعقّب التغريدات وحالات الذكر المرتبطة بإسم مستخدم أو هاشتاغ معيّن.
- خدمة التنبيه غوغل أليرتس[١٠] Google Alerts خدمة تويتديك

[٢] https://twitter.com/search-advanced
[٣] https://images.google.com/
[٤] https://www.elevenpaths.com/technology/metashield/index.html
[٥] http://metapicz.com/
[٦] http://socialmention.com
[٧] https://moz.com/followerwonk/
[٨] https://namechk.com
[٩] https://ifttt.com
[١٠] https://www.google.com/alerts

- Tweetdeck[١١]

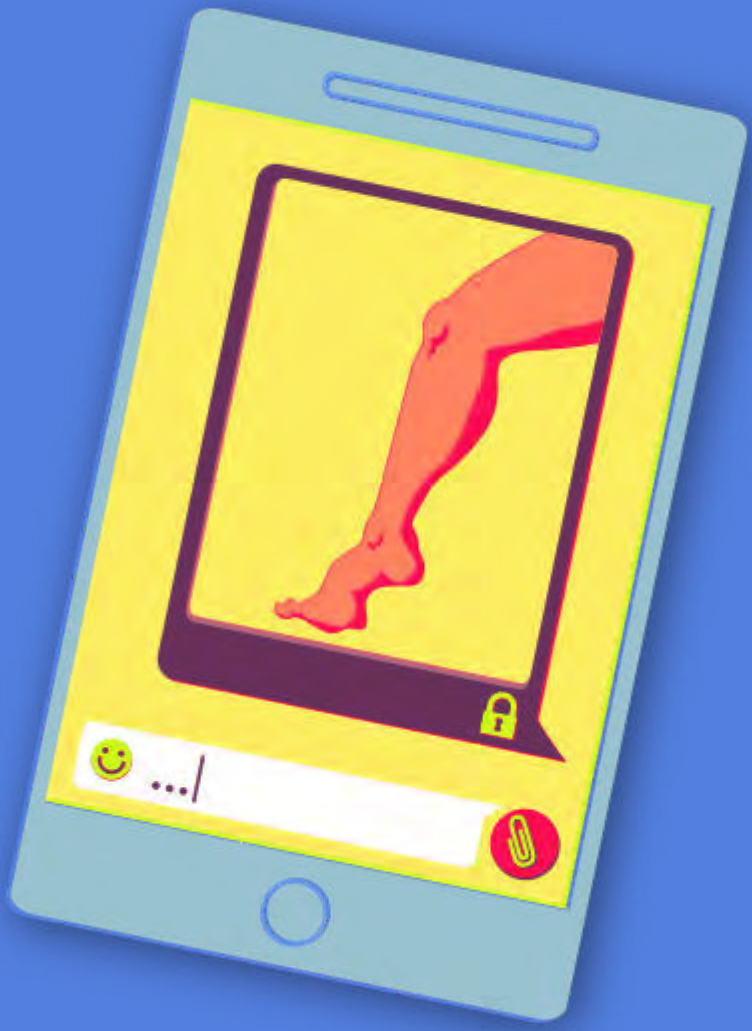
٢١. وفقًا للوقت المتوفر لكن، يمكن للمشاركات إما إجراء تحقيقاتهن الآن أثناء ورشة العمل، أو يمكنهن القيام به "كفرض منزليّ" يُقدّم في اليوم التالي من التدريب. في كلا الحالتين، ذكّرن المجموعة أنه من المفيد، بعد الإنتهاء من جمع المعلومات، التوقف قليلاً ومن ثم الإطلاع على إجمالي المعلومات التي جمعنها:

- هل لاحظن أنماطًا معيّنة؟
- 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/

[١١] https://tweetdeck.twitter.com



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 عنفًا إن حدث على الإنترنت أو في الواقع.
- **الطول:** 15 دقيقة
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - None
- **المواد اللازمة:**
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
  - مكبرات صوت (للفيديو)

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 شاهدنه – ما رأيهن بالحالة؟ ما الذي يمكنهن القيام به؟

باب ٤٠

التحادث الجنسي

- **الأهداف:** هذه الجلسة تتابع النقاش عن التحادث الجنسي من منظور جندري الذي بدأ في الجلسة السابقة من هذه الوحدة (حان وقت المراقبة!)، وتستند إليها للبدء بإقتراح ممارسات وأدوات والتوصية بها لتحادث أكثر أمانًا.
- **الطول:** 40 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** 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 علاقة:**
  - حقوقكن والتكنولوجيا الخاصة بكنّ (إعادة النظر بعلاقتنا بالتكنولوجيا)
  - حان وقت المراقبة! (التحادث الجنسي)
  - ماذا يمكن لبياناتكن الوصفية أن تفصح عنكن؟ (المناصرة الآمنة على الإنترنت)

- عدم الكشف عن الهوية (عدم الكشف عن الهوية)
- تعريف بمسألة التشفير (التشفير)

• **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 الأوّل – وصف مشكلة إجتماعية -

١. إبدأن الجلسة بعرض بعض الأمثلة عن المقالات التي تتناول 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:

• إلتقاط الصور الشخصية (Selfies) وصور عريّ وإرسالها هو ممارسة لحريّة شخصية.

- قد يكون التحادث الجنسي أيضًا فعل من أفعال المقاومة الممتعة ضد العنصرية والتمييز، على أساس الجنس وإستبداد الرجل والمحافظة والمعايير المفروضة على أساس تطبيع المغايرة الجنسية.
- في النهاية، إن كنتن تشاركن صورًا عنكن من هذا النوع أم لا، يجب أن يكون ذلك خيارًا محصورًا بكن، ويجب أن يكون ممارسة واعية لحقكن في التعبير عن أنفسكن، وحقكن بالخصوصية في الوقت ذاته.

الجزء الثالث – تحادث جنسي أكثر أمانًا؟

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

لابد لكن هنا أن تتحضرن لكل الإحتمالات – قدمن النصائح أوالتوصيات بشأن الأمن الرقمي، إستنادًا إلى أولويات أو شكوك المشاركات وبواسطة بعض الإقتراحات التالية على سبيل المثال:

- إبقين آمنات – إحذفن صور العريّ أو الصور الذاتية التي ترسلنها إلى الآخرين من جهازكن مباشرةً بعد إرسالها. وعند إرسال الصور، إعتمدن القنوات الأكثر أمانًا (مثل تطبيق سيجنال – إطّلعن على المزيد من التفاصيل أدناه في المرحلة الخامسة).
- حددن قواعد أو اتفاقات 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 للتحادث الجنسي – مع أن الطلب من شريك/ة التحادث الجنسي تنزيل تطبيق جديد أو اتباع إجراء معيّن 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 أمانًا 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 غالبًا ما توفر معلومات محددة لهوية المستخدمين، وهذا أمر لابد 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 بديهي (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 لتحادث جنسي أكثر أمانًا مع شركائهن:

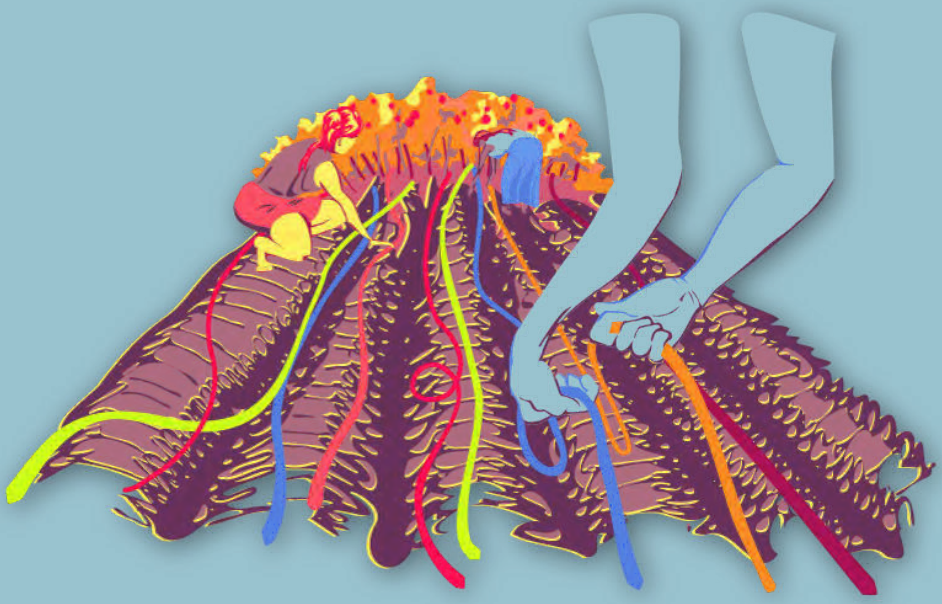
ObscuraCam أبسكورا كام: هذا التطبيق المخصص للهواتف وهو من إنتاج مشروع غارديان Guardian Project يتيح للمستخدمين "تنظيف" (إزالة) تفاصيل بيانات وصفية محددة من صورهم.

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

يجنال أو تليغرام: هذان التطبيقان المخصصان للمراسلة عبر الهواتف يقدمان مستويات متفاوتة من الحماية المشفّرة (للبيانات المتنقلة بين المستخدمين) بالإضافة لخاصية التحقق من المستخدم، يتيح تطبيق سيجنال للمستخدمين تحديد "تاريخ إنتهاء" للرسائل أوالمحتويات الأخرى المرسلة (على سبيل المثال، يمكن ضبط التطبيق بحيث تختفي صورة مرسلة بعد خمس دقائق من مشاهدتها من قبل المتلقي 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/obscuracam
- https://meet.jit.si
- https://signal.org
- https://telegram.org
- https://acoso.online



تحديد الحل الأفضل

باب ٤١

نموذج المخاطر القائمة على النوع الاجتماعي

- **الأهداف:** في هذه الجلسة، ستوجهن المشاركات في عملية من مراحل عدّة، أوّلها تحديد المخاطر المحدقة بهن، كنساء وكمدافعات عن حقوق الإنسان، وثانيها وضع إستراتيجية أمنية فرديّة للتعامل مع هذه المخاطر.
- **الطول:** من 40 إلى 5 دقيقة
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - متفاوتة (راجعن التوصيات أدناه)
- **جلسات/تمارين ذات علاقة:**
  - لنبدأ بتوثيق الحالات! (العنف ضد المرأة على الإنترنت)
  - الخطط والبروتوكولات الأمنية الخاصة بالمنظمة (التخطيط المسبق)
- **المواد اللازمة:**
  - أقلام خطاطة ملوّنة

- أقلام وأقلام رصاص
- ألواح ورقية أو لوح أبيض/أسود

• **التوصيات:** من الممكن تقديم هذه الجلسة بطرق مختلفة: قدمن الجلسة كاملة في بداية التدريب، ومن الجزء الثالث حتى النهاية بعد أن تقدّمن أدوات وممارسات محددة أكثر في جلسات سابقة؛ (a) وجّهن المشاركات في الجزئين الأوّل والثاني من هذه الجلسة عند بداية التدريب، ومن ثمّ قدّمن من الجزء الثالث حتى النهاية بعد أن تقدّمن أدوات وممارسات محددة أكثر في جلسات سابقة؛ (b) قسمن الجلسة إلى ثلاث جلسات صغيرة فردية إبتداءً من الجزء الأوّل عند بداية التدريب، والجزء الثاني في منتصفه بعد أن تتسنى للمشاركات فرصة مناقشة الأمن الرقمي في بيئاتهن الشخصية، والجزء الثالث عند النهاية بعد أن تقدّمن 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 يقدّم التدريب لأعضاء جماعة أو منظمة مدافعات عن حقوق الإنسان.

من الممكن تقديم هذه الجلسة بطرق مختلفة: قدمن الجلسة كاملة في بداية التدريب، ومن الجزء الثالث حتى النهاية بعد أن تقدّمن أدوات وممارسات محددة أكثر في جلسات سابقة؛ (a) وجّهن المشاركات في الجزئين الأوّل والثاني من هذه الجلسة عند بداية التدريب، ومن ثمّ قدّمن من الجزء الثالث حتى النهاية بعد أن تقدّمن أدوات وممارسات محددة أكثر في جلسات سابقة؛ (b) قسمن الجلسة إلى ثلاث جلسات صغيرة فردية إبتداءً من الجزء الأوّل عند بداية التدريب، والجزء الثاني في منتصفه بعد أن تتسنى للمشاركات فرصة مناقشة الأمن الرقمي في بيئاتهن الشخصية، والجزء الثالث عند النهاية بعد أن تقدّمن 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 يقدّم 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 جدًا لكن كمدربات أن تقمن بإدارة

مستوى الإجهاد في الغرفة. 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 إخافتهن، حيث تتوفر نشاطات كثيرة يمكنهن اعتمادها لمكافحة العنف على الإنترنت.

هذه الجلسة مُعدّة إستنادًا إلى جلسة وضعتها جينيفر شولتي Jennifer Schulte في معكسر 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 الأوّل – تحديد المخاطر والإحتمالات

١. إبدأن الجلسة بنقاش جماعي حول المخاطر المحددة التي تواجهها أو قد تواجهها المدافعات عن حقوق الإنسان – ذكّرن 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 تتبدّل وفقًا 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 نصيّة من قبل الخصوم عند استخدام تطبيق إرسال الرسائل النصية القصيرة الإعتيادي، ولكنه يخفض في حال أرسلت مشفّرة عبر تطبيق كتطبيق سيجنال؛

وعلى نحو مماثل، في حال كان شخص ما ناشطًا مستهدفًا في دولته، خطر إعتراض رسالة يرتفع بشكلٍ ملحوظ في حال أُرسلت بواسطة تطبيق الرسائل النصية القصيرة على هاتف

متصل بشبكة اتصالات دولته، ولكن منسوب هذا الخطر يخفض بشكلٍ ملحوظ، في حال أُرسلت بواسطة تطبيق كتطبيق سيجنال من على شبكة اتصالات في دولة أجنبية؛

ما يرد أعلاه مجرّد مثال بسيط عن كيفية تأثير العوامل التقنية الخارجية على إحتمالية 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. إرسمن جدولاً شبيهًا 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 خاليًا 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 إحتمالية 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 إفتراضي كمثال في هذه الجلسة.

٥. يمكنكن تحديد مقياس لقياس إحتماليات حدوث هذه المخاطر. على سبيل المثال، يمكنكن استخدام مقياس بسيط من 1 إلى 5، حيث الدرجة الخامسة تدل إلى أن إحتمالية تحوّل الخطر إلى حقيقة "عالية جدًا" وحيث الدرجة الأولى تدل إلى أن إحتمالية تحوّل الخطر إلى حقيقة "منخفضة جدًا". ما الدرجة التي يمكن إعطاؤها لكل خطر؟ يمكنكن البدء بملء الجدول للمجموعة أثناء مناقشة كل خطر على حدة، ليبدوكما يلي:

الخطر الرقمي // إحتمالية الحدوث

النقر على رابط في بريد إلكتروني فيه برمجية خبيثة عن طريق الخطأ! = 4 تتعرض مكاتبنا للمداهمة من قبل الشرطة لمصادرة أقراصنا الصلبة أو أجهزةأخرى! = 2

1 = منخفضة جدًا 5 = مرتفعة جدًا

الجزء الثاني – تحديد مدى التأثير

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

٧. إشرحن أن آثار المخاطر، تمامًا كالمخاطر نفسها، متقلبة هي الأخرى. تعتمد طبيعة التأثير وحدّته أيضًا على عدد من العوامل الخارجية. هل ستطال تداعيات أثار 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 كمّي مشابه للذي أستخدم لقياس إحتمالية الحدوث، أو قد يستخدم كأداة قياس نوعي يصف طبيعة وتفاصيل التأثير بدقّة. 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 مجرّد مفاهيم نظرية (لأغراض هذه الجلسة، سنستعين بمقياس كمّي).

٩. إشرحن للمجموعة أن إستباق رد فعلكن الممكن مع آثار المخاطر جزء مهمٌ من فهم المخاطر وقياسها – إسألن المشاركات عن تفاعلهن المحتمل على الصعيد الشخصي تجاه خطر معيّن؟ ومن ثمّ ناقشن كيف – تمامًا كالإحتمالية والتأثير – ستضعن مقياسًا

لقياس رد الفعل الذي قد يكون هوالآخر كمّيًا أو نوعيًا (ولكن لأغراض هذه الجلسة سنستعين بمقياس كمّي).

إستنادًا إلى ما بدأتن بشرحه في المرحلة الخامسة، سيشبه جدولكن الآن الجدول المبيّن أدناه كمثال:

- **الخطر الرقمي**: النقر على رابط في بريد إلكتروني فيه برمجية خبيثة عن طريق الخطأ!
- **إحتمالية الحدوث**: 4
- **الأثر**: 3
- **رد الفعل**: 2
- **الخطر الرقمي**: تتعرض مكاتبنا للمداهمة من قبل الشرطة لمصادرة أقراصنا الصلبة أوأجهزة أخرى!
- **إحتمالية الحدوث**: 2
- **الأثر**: 5
- **رد الفعل**: 5
- **إحتمالية الحدوث**: 1= منخفضة جدًا 5= مرتفعة جدًا
- **الأثر**: 1= خطورة منخفضة 5= خطورة مرتفعة
- **رد الفعل**: 1 = هادئ، تحت السيطرة 5 = حالة ذعر وتوتر شديد

الجزء الثالث – وضع إستراتيجيات للحلول

١٠. كما سبق وذكرنا في التوصيات، تتضمن هذه الجلسة نقاشًا مفصّلاً عن المخاطر الشخصية من منظور بيئة المدافعات عن حقوق الإنسان – قد تبدأ معالم القلق أوالإجهاد 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 هوعدم إخافتهن، حيث تتوفر نشاطات كثيرة يمكنهن اعتمادها 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 المعطاة من قبل المجموعة ستختلف وتتبدّل وفقًا للمرحلة التي ستقدمن فيها هذه الجلسة خلال عملية التدريب – في حال قدمتن هذه الجلسة في بداية التدريب، قد لا تتوفر لديهن إجابات مفصّلة جدًا، ولكن إن قدمتن هذه الجلسة عند نهاية التدريب عندها ستصبح إجاباتهن أكثر إرتباطًا بشأن بعض الأدوات والممارسات.

١٢. إستكمالاً للجدول الذي بدأتن 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**: النقر على رابط في بريد إلكتروني فيه برمجية خبيثة عن طريق الخطأ!
- **إحتمالية الحدوث**: 3
- **الأثر**: 4
- **رد الفعل**: 3
- **ماذا يمكنني أن أفعل؟**: تنزيل برمجية مكافحة فيروسات وتثبيتها؛ تنبيه الآخرين في شبكتي/منظمتي في حال ظهر لديهم الرابط ذاته

- **الخطر الرقمي**: تتعرض مكاتبنا للمداهمة من قبل الشرطة لمصادرة أقراصنا الصلبة أوأجهزة أخرى!
- **إحتمالية الحدوث**: 4
- **الأثر**: 5
- **رد الفعل**: 5
- **ماذا يمكنني أن أفعل؟**: القيام بنسخ احتياطية عن بياناتنا بشكلٍ دوري، وتخزينها في مكان آمن خارج مكاتبنا، وتنبيه الآخرين في شبكتنا إذا ما تعرضت معلومات خاصة بهم للكشف
- **إحتمالية الحدوث**: 1= منخفضة جدًا 5= مرتفعة جدًا
- **الأثر**: 1= خطورة منخفضة 5= خطورة مرتفعة
- **رد الفعل**: 1 = هادئ، تحت السيطرة 5 = حالة ذعر وتوتر شديد

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 هوتعريف النساء بعملية التفكير الإستراتيجي النقدي المستخدمة في صنع القرارات الواعية بشأن تنفيذ وتطبيق ممارسات وأدوات الأمن الرقمي، وتحديد الموارد التي ستساعدهن في متابعة المستجدات بعد هذا التدريب.
- **الطول:** 90 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** متوسط
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
- **جلسات/تمارين ذات علاقة:**
  - وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)
  - بمن نثقن؟ (تمارين بناء الثقة)
  - كيف يعمل الإنترنت؟ (أسس الأمن الرقمي،الجولة الأولى)
  - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟ (الخصوصية)
- **المواد اللازمة:**
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض

- شرائح بالنقاط المفتاحية الواردة أدناه
- نسخ عن الرسوم البيانية الخاصة بحالات المدافعات عن حقوق الإنسان (راجعن الملاحق)

• **التوصيات:** بما أن هذه الجلسة تستوجب حد أدنى من المعرفة الأساسية بمفاهيم الأمن الرقمي، يفضل تقديمها في تدريب على عدّة أيّام أو كجزء من ورشة عمل قصيرة المدّة، تركّز أكثر على تصميم البروتوكولات الأمنية الفردية.

إدارة الجلسة

الجزء الأوّل – المقدمة

١. إبدأن بسؤال المشاركات عن عدد المرات التي طرحن فيها على مدربة أو خبيرة أخرى سؤالاً عن الأمن الرقمي، فتلقين إجابات مختلفة في كل مرة بحسب الشخص الذي طرح عليه السؤال – هذا أمرٌ محيّر، أليس كذلك؟ أحيانًا حين نطلب نصائح عن الأمن الرقمي، قد لا يشرح الأشخاص الذين يقدمون لنا المساعدة سير العملية، بل يكتفون "بحلّ المشكلة" على أجهزتنا من دون أن يشرحوا ما قاموا به - ألا تفضلن معرفة ماهية الحلّ المناسب لكي تتمكّن من تطبيقه مرة أخرى في حال واجهتن المشكلة مرّة أخرى؟

٢. إشرحن لهن أن الهدف من هذه الجلسة هو تعريف المجموعة بعملية التفكير النقدي الإستراتيجي المستخدمة في صنع القرارات الواعية بشأن تطبيق وتنفيد ممارسات وأدوات الأمن الرقمي، وتحديد الموارد التي من شأنها مساعدتهن على متابعة المستجدات بعد التدريب. ناقشن فكرة أن الأمن الرقمي ليس محصوراً فقط بتنزيل تطبيقات جديدة، بل تشمل أيضًا معرفة ممارساتكن جيّدًا وإتخاذ قرارات واعية لبناء بيئة أكثر أمانًا لكنّ.

الجزء الثاني – كيف تم بناء البرمجيات التي تستخدمنها؟

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

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

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

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

الجزء الثالث – التفكير في المستخدمين؟

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

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

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

الجزء الرابع – التفكير في الأدوات

٨. الأسئلة التالية هي أسئلة لابد من طرحها عند التفكير في استخدام منصة أو أداة جديدة – إشرحن ذلك للمشاركات. لا حاجة لشرحها والإجابة عنها كلها (فهي أسئلة محددة جدًا)، ولكن إحرصن على قراءتها بصوتٍ عالٍ وإشرحن بإيجاز سبب أهمية كل واحد منها:

هل البرمجية مجانية ومفتوحة المصدر؟

هل تعرفن من برمج الأداة، أو من موّل المشروع؟

هل هي متوفرة بلغتكن؟

إبحثن عن منشورات مدونات أو أي موقع يأتي على ذكر الأداة على الإنترنت، ماذا

وجدتن؟ متى أُدخل التحديث الأخير على الأداة؟ هل النسخة المتوفرة نسخة ثابتة من الأداة؟ هل توفر جهة ما الدعم التقني للأداة أم هي مدعومة من متطوعين/ات؟ ما مدى سهولة إعدادها؟ هل خضعت الأداة للإختبار أو التدقيق؟ هل الأداة متوفرة لنظام التشغيل الذي تستخدمنه على أجهزتكن؟ تحققن من شروط الخدمة الخاصة بالأداة – هل توافقن عليها أم تبدو لكن مريبة؟ في حال كانت الأداة أو المنصة تستعين بخوادم عن بعد، هل تعرفن أين تتواجد هذه الخوادم؟ هل قام مطورها في يوم من الأيام بتسليم بيانات أي مستخدم إستجابة لطلب حكومةٍ ما؟ كيف تُخزن المعلومات على خوادمها؟ هل هي مشفّرة، وإن كان الأمر كذلك هل يمتلك المشروع طريقة لفك التشفير والوصول إليها؟ في حال ساورتكن أي شكوك، إبحثن عن طريقة للتواصل مباشرة مع المطورين والتحدث معهم.

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

١٠. وضحن للمجموعة أن عددًا كبيرًا من برمجيات الأمن الرقمي تتضمن تشفيرًا بدرجات متفاوتة – فسّرن للمشاركات أنه في حال كان التشفير خاصية مهمة بالنسبة لهن، يوصى إذًا باستخدام البرمجيات المفتوحة المصدر. فالبرمجيات المفتوحة المصدر قابلة للتدقيق من قبل المجتمع من أجل ضمان عدم وجود أي أبواب خلفية؛ في حال لا تشمل أداة برمجية ما خاصية التشفير، ولم يكن التشفير عاملاً مهمًا في عملية صنع القرار، قد يكون استخدام البرمجيات المفتوحة المصدر أقل أهمية (مع أنه أبخس ثمنًا حتمًا).

١١. أكملن هذا الجزء من الجلسة عبر تقسيم المشاركات إلى مجموعات من 3 إلى 4 أشخاص كحدٍ أقصى – وضمن مجموعاتهن الصغيرة، أطلبن منهن وضع لائحة ببعض أدوات الأمن

الرقمي التي يعرفنها، والإجابة عن الأسئلة الورادة أعلاه عن كل أداة. أثناء قيامهن بذلك، يتوجب على كل مجموعة مناقشة الإيجابيات والسلبيات التي يجدنها في كل أداة م

الجزء الخامس – التدرب على التفكير في الحلول

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

الجزء السادس – الموارد اللازمة للتمكن من متابعة المستجدات

١٣. لابد للمشاركات في تدريبكن أن تتوفر لديهن إمكانية الوصول إلى المزيد من الموارد بعد إنتهاء التدريب، التي يمكنهن العودة إليها للمحافظة على تدريبهن والتمكن من متابعة المستجدات بشأن الأدوات أو الممارسات الجديدة التي تنتج عن مجتمع الأمن الرقمي.

إليكن بعض الموارد المقترحة التي يمكن تقديمها للمشاركات:

- الهدوء وفن جعل التنكولوجيا تعمل لصالحك // Tactical Technology Collective (تاكتيكل تكنولوجي)[١]
- موقع "سيكيوريتي إن آي بوكس Security in a Box (فرونتلاين ديفندرز Frontline Defenders وجماعة تاكتيكل تكنولوجي)[٢]
- مشروع "سورفايلنس سلف ديفينس" Surveillance Self-Defense (مؤسسة إلكترونيك فرونتير)[٣]

[١] https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual
[٢] https://securityinabox.org
[٣] https://ssd.eff.org/en/module/choosing-your-tools

اختياري: يمكنكن ايضًا وضع لائحة بمنظمات مختلفة تستطيع المشاركات متابعتها (على الإنترنت عمومًا وعلى تويتر،.إلخ) للوصول إلى المزيد من المعلومات عن الأمن الرقمي في بلدانهن.

باب ٤٣

أنا صاحبة القرار

- **الأهداف:** الهدف من هذه الجلسة هوتوجيه المشاركات في عملية التفكير النقدي الإستراتيجية لإتخاذ القرارات بشأن أدوات أو ممارسات محددة في مجال الأمن الرقمي سيقمن بتطبيقها لأنفسهن.
- **الطول:** 15 دقيقة
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - ممارسة التطبيقية بواسطة أدوات وممارسات الأمن الرقمي من التدريب السابق
  - القرارات المرتبطة بالأمن الرقمي (تحديد الحلّ الأفضل)
- **جلسات/تمارين ذات علاقة:**
  - وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)
  - بمن نثقن؟ (تمارين بناء الثقة)
  - كيف يعمل الإنترنت؟ (أسس الأمن الرقمي،الجولة الأولى)
  - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟ (الخصوصية)

- القرارات المرتبطة بالأمن الرقمي (تحديد الحلّ الأفضل)

• **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:** كمدربات، غالبًا ما نفرض منظورنا الخاص عن ممارسة الأمن الرقمي على المشاركات، إما عن قصد إنطلاقًا من نوايا حسنة، وإما عن غير قصد. ولكن، لابد لنا أن نتذكر – بصفتنا مدربات وخبيرات – أن المشاركات غير مجبرات على استخدام الأدوات التي نعلمهن عنها، أو التكييف مع الممارسات التي نعتبرها "الأكثر أمانًا".

إدارة التمرين

١. إفتتحن الجلسة بشرح كيف أن بناء ممارسة في مجال الأمن الرقمي عبارة عن عملية متكررة وغالبًا ما تكون صعبة على أي شخصٍ كان. تستند هذه الجلسة على العمل الذي بدأتنه خلال جلسة القرارات المرتبطة بالأمن الرقمي من هذه الوحدة التي بدأت المشاركات خلالها تحديد الأدوات الممارسات الخاصة بهن.

٢. ضعن 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 تعرّفن على عدد من الأدوات المعروضة على الطاولة قبل هذه الجلسة – من قبيل مفاتيح بي جي بي PGP أو تطبيق سيجنال أو أوبسكورا كام أو إيتش تي تي بي إس إيفريوير. ذكرن المجموعة أنه كما سبق أن ذكرتن في مراحل سابقة من التدريب، هنّ من سيتوجب عليهن اختيار الأدوات المناسبة لهن ولحاجاتهن وليس أنتن كمدربات أو متخصصات تقنياً أو أي شخص آخر.

٤. أطلبن من المشاركات التقدم نحو الطاولة واختيار من بين رسومات الأدوات الموجودة

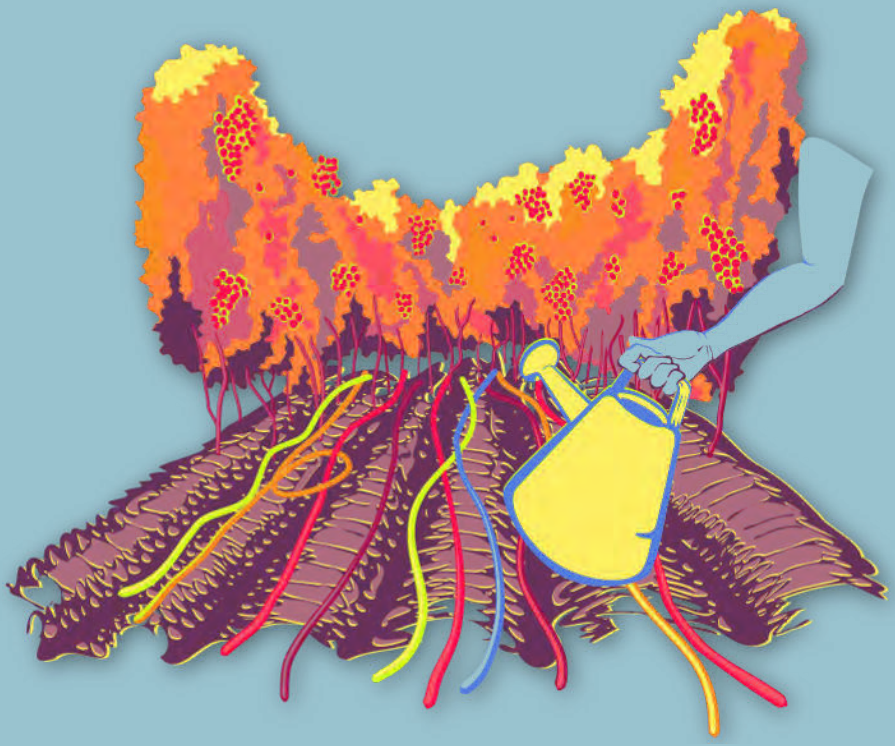
هناك، تلك التي يعتبرنها مهمة لهنّ ولحاجاتهن الفردية، وتلك التي سيستمرن في التدرّب على استخدامها والاستمرار في استخدامها بعد إنتهاء التدريب بأكمله.

٥. بعد أن تختار كل المشاركات أدواتهن، أطلبن من كل واحدة منهن شرح سبب اختيارهن للأدوات التي إخترنها – عليهن الوقوف أو الجلوس في حلقة حول الطاولة، ومن ثمّ، يعرضن واحدة تلو الأخرى خياراتهن وأسبابها إلى أن تقمن جميعًا بذلك. لابد لهن أيضًا من ذكر إن وجدن أي أداة أردن اختيارها ولكن اخترنها الأخريات 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) أطلبن منهن التعبير عن أي مخاوف ما زالت تساورهن إذ لا تعالجها كما يجب أي أداة من الأدوات التي توفرت لديهن.

٧. إختتمن الجلسة بالتفكير جماعيًا حول كيفية مشاركة المعرفة، وأنه على اللواتي إخترن أداةً أردنها مشاركات أخريات أيضًا (ولكن لم يستطعن لعدم توفر ما يكفي منها) مشاركتها وتبادلها لكي نتمكن جميعًا من "التعلّم" من بعضنا البعض.

النساء فى فضاء الإنترنت



التخطيط المسبق

باب ٤٤

الخطط والبروتوكولات الأمنية الخاصة بالمنظمة

- **الأهداف:** في هذه الجلسة، ستقمن بتسيير عملية ستنفذها المشاركات لوضع خطة أمنية والبروتوكولات المرتبطة بها التي يمكنهن استخدامها لتطبيق إجراءات الأمن الرقمي في منظماتهن.
- **الطول:** 90 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** 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 علاقة:**
  - وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)
  - بمن تثقن؟ (تمارين بناء الثقة)

- كيف يعمل الإنترنت؟ (أسس الأمن الرقمي،الجولة الأولى)
- نموذج المخاطر القائمة على النوع الاجتماعي (تحديد الحلّ الأفضل)
- الخطط والبروتوكولات الأمنية الخاصة بالمنظمة (التخطيط المسبق)

• **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 القادمات من المنظمة أو الجماعة ذاتها، بما أن النشاطات الواردة أدناه تركّز على وضع خطة أمنية على مستوى المنظمة – وعملية تصميم كل هذا سيساعدنا في تعزيز ممارستها وتنفيذها بشكلٍ مستمر من قبل النساء المشاركات. لابد 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 معيّنة أو طريقة تنفيذهن لها 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 عالجنها، ولن يرتحن لمشاركة بعض الصعوبات الفعلية عند نشوئها.

إدارة الجلسة

الجزء الأوّل – عودة إلى نموذج المخاطر

١. إبدأن الجلسة بالتشديد على أهمية بناء نموذج مخاطر قبل وضع مسودة خطة وبروتوكولات. ذكّرن 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 ستتضمن:

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

الجزء الثاني – الخطط في مواجهة البروتوكولات

٢. إشرحن للمشاركات الفرق بين خطة أمن رقمي وبروتوكول أمن رقمي. الفكرة الرئيسية الي 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 واحدةٍ منها مرتبطة بنشاط أو عملية معيّنة ضمن المنظمة أو الجماعة. البروتوكولات فعلياً عبارة عن ممارسات دائمًا تبقى فاعلة عندما يكتمل تطبيق خطة أمن رقمي معيّنة، وتتطوّر مع الوقت إستجابةً للتغييرات في بيئات المخاطر والتهديدات.

قدمن أمثلة عن الخطط والبروتوكولات للمشاركات – على سبيل المثال، الأنشطة كالسفر أو المشاركة في مظاهرات عامة يخصص لكل نشاط منها بروتوكل أمن رقمي خاص؛ البنود الواردة في خطة أمن رقمي قد تتضمن خضوع الموقع الإلكتروني الخاص بالمنظمة للتدقيق، والتحقق من توفر برنامج مكافحة للفيروسات مثبّت 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 لجزء من المشاركات، يمكن عندها للواتي لا ينتمين لأي منظمة أو مجموعة العمل على وضع خططهن وبروتوكولاتهن الشخصية.

٤. أطلبن من المشاركات مراجعة نموذج المخاطر من تمرين نموذج المخاطر القائمة على النوع الاجتماعي، بالإضافة إلى ملاحظاتهن من تمرين بمن نثقن؟. أطلبن منهن القيام بوضع مسودة بخطتهن الأمنية – الجدول التالي قد يكون مفيدًا. إشرحن للمشاركات كل قسم من الأقسام (يجب إضافة سطر جديد لكل خطر أو تهديد نحدده):

- **التهديدات والمخاطر**: ما هي التهديدات والمخاطر المحدقة بنا حاليًا؟ وما هي تلك التي قد نواجهها في المستقبل؟
- **نقاط الضعف المحددة**: ما هي الممارسات أو الظروف التي قد تعرضنا كأفراد وكمنظمات للأذي؟
- **نقاط القوة والقدرات**: ما هي نقاط القوة التي نتمتع بها كمنظمة فتعطينا القدرة على التعامل مع التهديدات والمخاطر التي حددناها؟
- **إجراءات التخفيف**: ما هي الإجراءات المطلوبة للتخفيف من المخاطر التي حددناها؟ ولنكون جاهزاتٍ بشكلٍ أفضل عند مواجهة التهديدات التي حددناها؟

- **الموارد المطلوبة**: ما هي الموارد (الإقتصادية، البشرية، إلخ.) المطلوبة لتنفيذ هذه الإجراءات؟
- **من هي العناصر المطلوبة**: ما هي القطاعات أو من هم الأشخاص داخل منظمتنا الواجب إشراكهم في عملية التنفيذ؟ هل سنحتاج لأي تواقيع أو أي أذونات أخرى؟

٥. ذكرن المشاركات أنه على الرغم من التركيز في هذا التدريب على الأمن الرقمي، علينا التذكر دائمًا أن نأخذ الإجراءات الشاملة بعين الإعتبار. أطلبن 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، أطلبن 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. يعدّ ذلك فرصة قيّمة 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؟

٨. اقشن خطوات المتابعة مع المشاركات – سيحتجن لتنظيم إجتماع خاص ضمن منظمتهن لتشارك المعلومات الأساسية والخلاصات الرئيسية من هذه الجلسة، بالإضافة إلى تمرين

نموذج المخاطر القائمة على النوع الاجتماعي 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 أيضًا تذكر أن عضوات أخريات في منظمتهن سيحتجن لتدريب على ممارسات و/أو أدوات معيّنة في مجال الأمن الرقمي من أجل أن يصبح التنفيذ الكامل ممكنًا.

باب ٤٥

خطط وبروتوكولات الأمن الرقمي: إعادة تنفيذها بعد التدريب

- **الأهداف:** في هذه الجلسة، ستستند المشاركات إلى جلسة الخطط والبروتوكولات الأمنية الخاصة بالمنظمة. ستقمن هنا بعرض مجموعة توصيات تساعد المشاركات في تسهيل عملية إعادة تنفيذ الخطط والبروتوكولات بعد التدريب ضمن منظماتهن.
- **الطول:** 40 دقيقة
- **الشكل:** جلسة
- **المستوى المهاري:** 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 الحلّ الأفضل)
  - الخطط والبروتوكولات الأمنية الخاصة بالمنظمة (التخطيط المسبق)
- **جلسات/تمارين ذات علاقة:**
  - وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)

- بمن نثقن؟ (تمارين بناء الثقة)
- كيف يعمل الإنترنت؟ (أسس الأمن الرقمي،الجولة الأولى)
- نموذج المخاطر القائمة على النوع الاجتماعي (تحديد الحلّ الأفضل)
- الخطط والبروتوكولات الأمنية الخاصة بالمنظمة (التخطيط المسبق)

• **المواد اللازمة:**
- شرائح (فيها النقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض

إدارة الجلسة

الجزء الأوّل – وضع خارطة بالهيكليات والعوائق التنظيمية

١. ضمن مجموعات من شخصين، أطلبن من المشاركات وصف منظماتهن:
   • كم عدد الأشخاص المشاركين/ات فيها؟
   • كم مرة يلتقون في الأسبوع/السنة؟

٢. ضمن الثنائيات من الخطوة السابقة، أطلبن من المشاركات الآن تشارك مع بعضهن البعض، بعض العوائق أوالتحديات التي يتوقعن مواجهتها ضمن منظماتهن عند تقديم خططهن الأمنية والتعبير عن الحاجة للبدء بعملية التنفيذ.

الجزء الثاني – تسيير تنفيذ المنظمة

٣. بعد أن تنتهي المجموعات من مناقشة النقاط المذكورة أعلاه، شاركن بعض الأفكار 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 وإختبارها الكثير من الوقت، وستمر المنظمة في مرحلة تكيّف إلى أن يعتاد أفرادها على هذه التغييرات. ومع ذلك، يجب أن يحرصن على التشديد أن التفكير بشكلٍ نقديّ أكثر بشأن الأمن التنظيمي خطوة في الطريق الصحيح.
- حذرن المشاركات أنهن سيتلقين بعض الرفض بسبب مصطلح "بروتوكول" بما أن معناه أصبح تقنيًا ومشحونًا أكثر من اللازم؛ يجب أن يذكّرن الأخريات في منظمتهن أن البروتوكولات ليست إلا إتفاق بشأن المخاطر والتهديدات المحدقة بهن، والإلتزام بحلّها معًا 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 ثمّ مشاركة نتائج هذا التقييم والخطوات اللاحقة مع بقية زميلاتهن. شددن أيضًا على أن يحرصن المشاركات على إفساح المجال للأخريات في منظمتهن من أجل تقديم الملاحظات بشأن الخطط والبروتوكولات الأمنية – بما أن مهام أشخاص مختلفين ستتأثر بطرق مختلفة بهذه التدابير الجديدة، لابد لهن من تفادي إضافة أعباء جديدة على مهام أي شخصٍ كان.
- أطلبن من المشاركات التفكير في طرق أخرى لإشراك فرق مختلفة من المنظمة بشكلٍ جماعي – إحدى تلك المقاربات الممكنة هي أن يقترحن "هيئة أمن رقمي" تشمل ممثلات (لديهن ما يلزم من معرفة لإتخاذ قرارات) عن كل فريق أومجال عمل، مهمتها الإشراف على تنفيذ الخطة الأمنية. ومن ثمّ يمكنهن تنفيذ هذه العملية بشكلٍ تدريجي، فيركزن أولاً على الموظفات ذوات المستوى الأعلى أوالبدء مع فرق معيّنة ومن ثمّ توسيع رقعة المشاركة. المقاربة الفضلى ستختلف كثيرًا من منظمة لأخرى.
- في الختام – أطلبن من المشاركات مشاركة بعض الأفكار التي لديهن والتي قد تساعد في تسيير عملية التنفيذ في منظماتهن.

الجزء الثالث – طرح المسألة

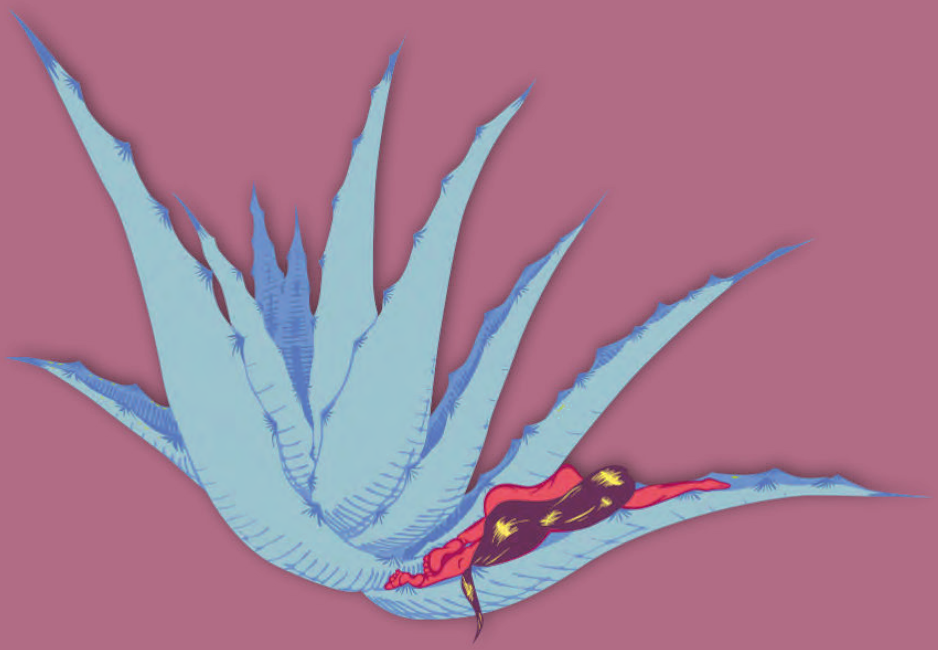
٤. أطلعن المشاركات على هيكلية أساسية لطرح هذه المسألة المهمة لمناقشتها ضمن منظماتهن – قد يكون ذلك عبارة عن مجموعة أسئلة، أو خطة تدريب ممكنة خاصة بهن تتضمن جلسات وتمارين معينة مرتبطة ببيئة المخاطر التنظيمية.

٥. ذكرن المجموعة أن تنتبه للمتطلبات اللوجستية اللازمة، ولا سيما عامل الوقت – قد لا يتوفر للأخريات في منظمتهن الوقت الكافي لتخصيص فترة ما بعد الظهر كاملةً، أو يوم كامل أو فترة أطول من ذلك حتى للتدريب. وتتطلب عملية تغيير عادات قديمة وقتًا طويلاً والكثير من الصبر، لذا يفضل أن تبحث المشاركات عن طرق لطرح هذه المسائل (أو التدريبات) خلال الاجتماعات الدوريّة الموجودة أو خلال تجمعات أخرى. إليكن هيكلية بسيطة قد تتبعها المشاركات لزيادة مستوى الوعي بشأن مواضيع معيّنة – تبدأ هذه بنقاش حول أهمية الأمن الرقمي بالنسبة للمنظمة، ومن ثمّ يأتي دور الجلسات (من هذا المنهاج) التي تعرض تفاصيل أكثر عن مواضيع الأمن الرقمي – وتعود مسألة اختيار 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 الأوّل (هواتف محمولة أكثر أمانًا)]
- **الجلسة**: [الاتصالات المشفّرة (التشفير)]
- **الجلسة**: [نموذج المخاطر القائمة على النوع الاجتماعي (تحديد الحلّ الأفضل)]

٦. ذكرن المشاركات أن هذه ليست سوى مقاربة مقترحة – لهن الحريّة في تعديل الجلسات والمواضيع وفقًا لما يرينه مناسبًا. لابد أن تكنّ متواجدات 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
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - وجهات النظر الشخصية حيال الأمن (إعادة النظر بعلاقتنا بالتكنولوجيا)
  - بمن نثقن؟ (تمارين بناء الثقة)
- **المواد اللازمة:**
  - كرة مطاطية (أو أي شيء صغير من الممكن رميه من شخص لآخر)
- **التوصيات:** الرعاية الذاتية جزء أساسي من ممارسة الأمن الرقمي الشامل، وهي عنصر مهم في عملية التعزيز والتشجيع بشكلٍ دائم – يوصى بأن توزعن تمارين هذه الوحدة على إمتداد فترة التدريب.

في هذه الجلسة وفي كل جلسات تدريبكن، تنبهن دائمًا لقدرات النساء البدنية وحدودها المختلفة.

يفضل تقديم هذا التدريب في بداية التدريب أوفي بداية يوم تدريبي ما، 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 – إسألن المشاركات إن كنّ يعرفن هذا المفهوم أو سمعن به قبل الآن. عرّفن المجموعة بمفهوم الرعاية الذاتية وإشرحن أن هذا التمرين سيركز 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 للتحرّك في الغرفة وتمديد عضلاتهن – ومن ثمّ، أطلبن منهن الوقوف في حلقة. ستبدأن برمي كرة صغيرة بلطف (أوأي شيء من الممكن رميه من شخص لآخر) إلى إحدى المشاركات. عندما تلتقطنها، ستسألنهن سؤالاً لإستنباط أفكارهن بشأن جوانب الرعاية الذاتية بما أنها مرتبطة بهن شخصيًا (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 الاستمرار في التمرين، إلى أن تتسنى 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 لكن؟ 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 عليكن التفكير بأنكن جديرات بالرعاية؟ هل يصعب عليكن التفكير في شخص جدير بالرعاية؟ كمدافعات عن حقوق الإنسان، هل تعتقدن أننا نميل أكثر لتقديم الرعاية الذاتية للآخرين على حساب أنفسنا؟ هل تشعرن أنكن منتبهات لما تحتاج له أجسادكن وأرواحكن؟

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

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 وأحيانًا حتى العمل والزملاء – التي يفرضها المجتمع غالبًا على النساء.

٥. حللن كيف تؤثر هذه المسؤوليات الإضافية على عملهن كمدافعات عن حقوق الإنسان، وقمن بمقارنتها مع التحديات التي يواجهها الرجال. يمكنكن هنا التطرق أيضًا لمسألة الشعور بالذنب الذي ينتاب المدافعات عن حقوق الإنسان في أغلب الأحيان – إذ عليهن الاختيار في حالات كثيرة بين نشاطهن وحياتهن الشخصية وعائلاتهن ويشعرن، بغض النظر عن خيارهن، أن اعتماد خيار ما يعني إهمال الخيار الآخرى إلى حدٍ كبير.

٦. 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، أوتخصيص فترات أقصر وأكثر للإستراحة وتناول وجبات طعام معيّنة معًا، إلخ.

باب ٤٧

لمسة محبة

- **الأهداف:** في هذا التمرين الهادف للإسترخاء، ستبني المشاركات علاقات مع بعضهن البعض من خلال لمس بعضهن البعض، ما يعكس فعل تقديم الحنان والمحبة والرعاية وتلقيها.
- **الطول:** 30-20 دقيقة
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - قواعد اللعبة (تمارين بناء الثقة)
  - بناء الرعاية الذاتية النسوية (الرعاية الذاتية)
- **المواد اللازمة:**
  - فرش أو بطانيات
  - مخدات أو وسادات
  - موسيقى هادئة
- **التوصيات:** الرعاية الذاتية جزء أساسي من ممارسة الأمن الرقمي الشامل وهي ضرورية

للتعزيز والتشجيع على الدوام – يوصى بأن توزع تمارين هذه الوحدة على مختلف أنحاء التدريب. في هذه الجلسة وفي كل جلسات تدريبكن، تنبهوا ولا تنسوا أن لكل امرأة قدرات جسدية مختلفة. يجب ألا تنسين أنتن والمشاركات الأخريات التنبه والوضع في الإعتبارأنه بعض النساء قد لا يشعرن بالإرتياح في حال لمستهن نساء آخريات (لا سيما في بعض الثقافات) – لهذا السبب، يفضّل تنفيذ هذا التمرين مع مجموعات من النساء اللواتي يعرفن بعضهن البعض ويثقن ببعضهن البعض. في حال إختارت بعض النساء عدم المشاركة في هذا النشاط، أخبرنهن أن ذلك مقبولٌ تمامًا من قبلكن. أكّدن لهن أنهن لن يُدفعن إلى القيام بأي أمر يزعجهن وذكرنهن أنه يمكنهن المشاركة عبر الإستلقاء والإسترخاء لبضعة دقائق من خلال التنفس بعمق وبطء. لإنشاء بيئة تشجّع 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 ديفندرز" IM Defenders Self-Care Manual

إدارة التمرين

١. رتبن البطانيات والوسادات على شكل حلقة على الأرض – أطلبن من نصف المجموعة الإستلقاء على ظهورهن في الحلقة، ورؤوسهن موجهة نحو وسط الحلقة وكأنهن يشكّلن بتلات زهرة. أطلبن منهن إغماض أعيونهن والإسترخاء. إحرصن على وجود مساحة تكفي لشخص واحد على الأقل بين كل مشاركة.

٢. أطلبن من النصف الآخر من المجموعة التركز في المساحات الموجودة بين مشاركات النصف الأوّل من المجموعة، وأن يجلسن بالقرب من ركب المشاركات المستلقيات.

٣. ستقدن هذه الجلسة بواسطة صوتكن، إشرحن للمجموعة الجالسة أنهن سيمنحن "لمسة محبة" للنساء المستلقيات إلى جانبهن. سيلمسنهن بطريقة محترمة وغير مزعجة ستصفونها لهن الآن. وأولئك اللواتي يزعجنهن لمس الأخريات، يمكنهن وضع أيديهم على رأس

أوكتف شريكتهن فقط أو بكل بساطة إغلاق أعيونهن والإستماع إلى صوتكن.

٤. بصوتٍ هادئٍ ونبرة لطيفة، ستعطين النساء الجالسات إرشادات متعددة بشأن لمسات المحبة، التي تفصل بينها دقيقتان أو ثلاثة دقائق. ذكروا الجميع أن التنفس مهم جدًا في هذا التمرين – عليهن جميعًا التنفس ببطء وإستنشاق الهواء من أنوفهن وإخراجها من أفواههم:

- **التوجيه الأوّل:** إلمسن و حركن بأيديكن ببطء على رأس شريكتكن.
- **التوجيه الثاني:** إلمسن و حركن بأيديكن ببطء على جبهة شريكتكن.
- **التوجيه الثالث:** إلمسن و حركن بأيدكن على كتف شريكتكن.
- **التوجيه الرابع:** إلمسن و حركن بأيدكن على أيدي وأصابع شريكتكن.

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

- مدافعات عن حقوق الإنسان، لا وقت لدينا عادةً لأنفسنا. وبالتالي المشاركات اللواتي يقمن بلمسة الحنان لشريكاتهن يمنحنهن فرصة نادرة للإسترخاء والشعور بأن أحدًا يهتم لأمرهن.

- الأعباء والمسؤوليات الاجتماعية الملقاة على كاهل النساء – كمدافعات عن حقوق الإنسان وأمهات وأخوات، يتوقع منّا دائما الإهتمام بالآخرين ولكن هل نهتم بأنفسنا؟ ففي حياتنا نادرا ما يتاح الوقت لنهتم بأنفسنا على الصعيد الفردي أوالجماعي.

٦. بعد أن تنتهي المشاركات الجالسات من لمس أيدي وأصابع شريكاتهن، أطلبن من النساء المستلقيات بعد بضعة لحظات من فتح أعينهن، تبادل الأماكن مع شريكاتهن. 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
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - لمسة محبة (الرعاية الذاتية)
  - بناء الرعاية الذاتية النسوية (الرعاية الذاتية)
- **المواد اللازمة:**
  - ذهن متفتح وهادئ
- **التوصيات:** الرعاية الذاتية جزء أساسي من ممارسة الأمن الرقمي الشامل، ومن الضروري تعزيزها وتشجيعها بشكل دائمٍ. يوصى أن توزعن تمارين هذه الوحدة على إمتداد فترة التدريب.

في هذه الجلسة وفي كل جلسات تدريبكن، تنبهن دائمًا لقدرات النساء البدنية وحدودها المختلفة.

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

إدارة التمرين

١. إبدأن بشرح مدى سهولة طغيان الشعور بالرتابة والإستياء والحزن و الرغبة في الانقطاع عن الناس التي يجب تخطيها في الحياة اليومية للناشطات والمدافعات عن حقوق الإنسان.

٢. واصلن شرح ذلك، وخلال التمرين، ستتناول المشاركات تلك الأحاسيس التي يشعرن بها حين يعانين أو يشعرن بالضياع أو يفقدن البوصلة – سيقمن بذلك عبر تفعيل نقطة طاقة تقوم وفقًا للطبّ التقليدي الشرقي، بتفعيل الرغبة في الحلم والوقوع في حب الحياة من جديد.

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

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

حددن مكان نقطة الطاقة – هي موجودة بين العينين، تحت الحاجبين وفوق عظمة الأنف تمامًا.

خذن نفسًا عميقًا وإحبسنه.

بواسطة إبهامكن، إضغطن على نقطة الطاقة – وأثناء عملية الزفير، فكرن بشيء يلهمكن ويشعركن بحبّ 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 أحيانًا ليس عيبًا 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 جيّد أصلاً، وتلك التي يمكنهن تحسينها وتلك التي يتوجب عليهن اعتمادها.
- **الطول:** 30-20 دقيقة (وفقًا لتقديركن)
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - أنا صاحبة القرار[1]

[1] https://cyber-women.com/ar/قرارك-بصحتك-أنت/حلول-رقمية/

- لمسة محبة[٢]
- بناء الرعاية الذاتية النسوية[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 الرقمي الشامل، ومن الضروري تعزيزها وتشجيعها بشكل دائمٍ. يوصى أن يتم توزيع تمارين هذه الوحدة على طيلة فترة التدريب.

لإنشاء بيئة مؤاتية للإسترخاء ومراجعة الذات، يمكنكن إضاءة شموع أوحرق البخور أوتشغيل موسيقى هادئة تبعث على الإسترخاء خلال هذه التمارين.

إدارة التمرين

١. قدمن لكل مشاركة مرآة صغيرة أوفي حال عدم استخدام المرايا، أطلبن منهن جلب صور لهن. وزعن الملصقات المدوّرة عليهن.

٢. إشرحن لهن أنكن ستقرأن مجموعة من الجمل التي يتوجب على المشاركات الإجابة عنها سلبًا أم إيجابًا. في كل مرّة يُجبن سلبًا على إحدى الجمل، عليهن وضع ملصق مدوّر على المرآة أو على صورتهن.

٣. يرد أدناه لائحة بالجمل التي يمكنكن استخدامها خلال هذا التمرين؛ ولكن، إستنادًا إلى ما تعرفنه عن المجموعة (ومدى إرتياح المشاركات لبعضهن البعض على المستوى الفردي)

٢/ةبحم-ةسمل/ةيتاذلا-ةيعارلا/https://cyber-women.com/ar

٣/ةيوسنلا-ةيتاذلا-ةيعارلا-ءانب/ةيتاذلا-ةيعارلا/https://cyber-women.com/ar

٤/يرظنأ/ةيتاذلا-ةيعارلا/https://cyber-women.com/ar

يمكنكن إضافة جمل أو تفادي أخرى:

- كل ليلة، إنال ما لا يقلّ عن ثماني ساعات من النوم واستيقظ مرتاحة وأنا جاهزة لبدء نهاري؛
- خلال الأشهر الستّ/ السنة الماضية، إتيحت لي فرصة التمتع بعطلة وإستغليتها؛
- اتبع حمية غذائية صحّية وأقوم بتمارين رياضية بشكلٍ منتظم، للمحافظة على صحّة وإتزان جسمي وذهني؛
- أخصص دائمًا 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 دائمًا تولي مهام إضافية؛
- أخضع للفحوصات النسائية التي يوصي بها الأطباء كل ستة أشهر ؛
- أخصص الوقت الكافي لتوضيح وحلّ أي سوء تفاهم مع أحبائي أوزملائي في العمل حين تنشأ أي نزاعات؛
- أحافظ على نظام عمل من 8 ساعات في اليوم، أحترمه وتحترمه منظمتي؛

٤. بعد الإنتهاء من طرح الأسئلة، إسألن المشاركات – ماذا يرين في المرآة (أو في صورهن)؟ إجمعن المجموعة في حلقة وناقشن تأثيرات أعباء العمل الزائدة عن حدها، أو الممارسات الاجتماعية السئية في العمل، أوا 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 آنفًا 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 بشكلٍ أفضل.
- **الطول:** 10 إلى 15 دقيقة
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - لا يوجد
- **المواد اللازمة:**
  - الصدق و الحساسية
- **التوصيات:** الرعاية الذاتية جزء أساسي من ممارسة الأمن الرقمي الشامل، ومن الضروري تعزيزها وتشجيعها بشكل دائمٍ. يوصى أن توزعن 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. قدّمن التمرين عبر التحدث مع المجموعة عن الضغوطات التي يمارسها المجتمع على النساء – أي الأعراف الاجتماعية والثقافية التي تفرض على النساء مثل العمل ضعفي 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 أوتحقيق 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 أوأي طلب لخدمة ما أو تلبية إلتزام آخر ولكن لم تستطعن فعل ذلك في الواقع. يمكنكن البدء بإخبار قصة من قصصكن، عن حادثة أردتن الرفض فيها – على سبيل المثال:

كنت أخطط لتناول طعام العشاء مع صديقاتي، 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. إخبرن 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 اختيارية ولكن قد تشكّل طريقة جيّدة للتفكير بشكلٍ صحيّ 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 أنفسهن وفي مخاوفهن والإجراءات التي يمكنهن إتخاذها للتخفيف من الضغوطات المفروضة عليهن.
- **الطول:** 20 دقيقة
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - 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، يمكنكن كتابة الجمل الواردة أدناه على ورقة لوح ورقي كبيرة أو على لوح إعلاني

- **التوصيات:** الرعاية الذاتية جزء أساسي من ممارسة الأمن الرقمي الشامل، ومن الضروري تعزيزها وتشجيعها بشكل دائمٍ. يوصى أن توزعن تمارين هذه الوحدة على طيلة فترة التدريب. وفقًا 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 يهتممن بالموارد الأهم لديهن في نشاطهن (ألا وهي أنفسهن)؟

إدارة التمرين

١. على شريحة معدّة مسبقًا أوورقة من أوراق لوح ورقيّ إعرضن على المشاركات ما يلي:

عزيزتي .....،

تحية طيبة وبعد،

أنا أراقبكِ مؤخرًا، وأعلم أنكِ تمُرّين بظروف صعبة فيما يخص....

أعلم أيضًا أنكِ خائفة على....

أردت فقط أن تعرفي أن...

تذكري أنكِ بارعة جدًا في....

أعتقد أنه يتوجب عليكِ....

حاولي أن..... في الأسابيع القادمة.

مع محبتي،
نفسكِ

٢. وزعن ورقة لكل مشاركة – أطلبن منهن ملء الفراغ إلى جانب "عزيزتي" بإسمائهن، ومن ثمّ إكمال الجمل الأخرى الموجودة أمامهن.

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

تمارين الختام والمراجعة

باب ٥٢

الحكواتيات

- **الأهداف:** هذا التمرين الحركيّ سيساعدكن على رفع مستوى نشاط وطاقة المشاركات والمحافظة على تركيز واهتمام المجموعة. يقدم هذا التمرين إستراحة من المحتوى التدريب التقني، وفي الوقت عينه هو مرتبط بمواضيع الأمن الرقمي.
- **الطول:** 10 إلى 15 دقيقة (وفقًا لحجم المجموعة)
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - قصتها مع التكنولوجيا[1]
- **المواد اللازمة:**
  - كراسي (تحديدًا أقل بعدد واحد كرسيّ عن عدد المشاركات)

[1]-عم-اهتصق/ايجولونكتلاب-انتقالعب-رظنلا-ةداعإ/https://cyber-women.com/ar/ايجولونكتلا/

إدارة التمرين

١. 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.

٢. رتّبن الكراسي على شكل حلقة وأطلبن من المشاركات الجلوس عليها – يفترض أن يكون عدد الكراسي أقل بعدد واحد كرسيّ عن عدد المشاركات وبالتالي ستبقى مشاركة واحدة واقفة.

٣. زودن كل مشاركة باسم إمرأة بارزة في مجال التكنولوجيا أو العمل النسوي (الخيار يعود لكنّ) – يمكنكن حتى استخدام اسماء النساء ذاتها التي تحدثتن عنها في جلسة قصتها مع التكنولوجيا. زودن مشاركات عدّة بالاسم ذاته.

٤. إشرحن للمشاركات من هن الحكواتيات – هن نساء يجمعن النساء حولهن ليخبرن ويسردن قصصًا وحكايات – وقلن لهن أنهن معًا سيشكّلن مجموعة حكواتيات يتبادلن قصصهن الخاصة!

٥. إبدأن التمرين بقصة (من نسج الخيال) عن بعض النساء المتخصصات في عالم التكنولوجيا اللواتي يردن تكريمهن:

في كل مرة يجئ على ذكر اسم من أسماء هؤلاء النساء، سيتوجب على المشاركات اللواتي زودتنهن بإسمها أن يغيّرن مقاعدهن بسرعة (المشاركة التي كانت واقفة يمكنها أن تحاول إيجاد كرسي فارغ لتجلس عليه). المشاركة التي تبقى واقفة سيتوجب عليها الاستمرار في إختراع بقية الحكاية إلى أن تذكر ميسرة الجلسة اسم آخر فتغيّر المشاركات مقاعدهن مجددًا. في حال ذكرت ميسرة الجلسة كلمة "حكواتية" خلال القصة، فهذا يعني أنه سيتوجب على الجميع الوقوف بسرعة وتغيير المقاعد.

٦. 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

القِدْر المغلي (المِرْجَل)

- **الأهداف:** رتبن المساحة المخصصة للمشاركة في التمرين. عند العمل مع مجموعة، قد يميل أشخاص معينين إلى التحدث أكثر من غيرهن – الغاية من هذا التمرين هوتوعية المشاركات لهذا الجانب من الواقع، وفي الوقت عينه، تشجيع المشاركات اللواتي لا يتكلمن كثيرًا، على المبادرة والتعبير عن أنفسهن.
- **الطول:** 15 إلى 20 دقيقة (وفقًا لحجم المجموعة)
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - لا يوجد
- **المواد اللازمة:**
  - قصاصات ورقية معدّة مسبقًا (من 3 إلى 5 قصاصات لكل مشاركة)
  - وعاء أو حوض

- **التوصيات:** تمرين القِدْر المغلي (المِرْجَل) تمرين قد يستفاد منه طيلة فترة تدريبكن – في حال تقديمه في بداية ورشة العمل، يمكنكن استخدام هذا التمرين في كل مرّة تطرحن سؤالاً على المجموعة خلال الجلسة. بهذه الطريقة، تُتاح للجميع فرصة التحدّث أكثر من العادة، واللواتي يخجلن من الإجابة على الأسئلة المطروحة ستكون لديهن فرصة الشعور براحة أكبر. يرتكز هذا التمرين على نقاش جماعي، حول أي موضوعٍ كان؛ ولكنه فعّال أكثر حين يكون موضوع النقاش يركّز على موضوع من مواضيع التدريب. يمكنكن تقديم موضوع جديد، أواستخدام هذا التمرين كعملية مراجعة لموضوع تمت مناقشته مسبقًا – 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 تتكلم إحداهن، عليهن رمي قصاصة ورقية واحدة في القِدْر المغلي (المِرْجَل). وحين تنتهي القصاصات لدى مشاركة ما، يصبح ممنوعًا عليها التكلّم.

٣. إطرحن موضوعًا وسيّرن النقاش عبر طرح سلسلة من الأسئلة على المجموعة. على سبيل المثال، في حال كان الموضوع عن البرمجيات الخبيثة والفيروسات، يمكنكن 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 لحاسوبكن أو هاتفكن الذكي أن أصيب ببرمجيات خبيثة؟ في حال حدث ذلك لكن من قبل، كيف إكتشفتن ذلك؟

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

٤. أكملن النقاش إلى أن تنفذ القصاصات من جميع المشاركات - يمكنكن إعادة تفعيل النقاش في حال رغبتن بذلك، عبر الإنتقال 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 الأوّل أو اليومين الأوّلين من التدريب) وجهّن المشاركات في هذا التمرين لتحفيزهن وتشجيعهن على الاستمرار.
- **الطول:** 10 دقائق
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - لا يوجد
- **المواد اللازمة:**
  - قصاصات ورقية صغيرة
  - قلم
  - أزهار (حقيقية أم ورقية/بلاستيكية)
- **التوصيات:** يمكن إجراء هذا التمرين مرّات عدّة في مختلف مراحل التمرين - يمكنكن

إختتام اليوم الأوّل 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=_dq1thtiu8o

إدارة التمرين

١. قبل البدء بهذا التمرين، سيتوجب عليكن التحضير له مسبقًا:

- أكتبن رسائل تشجيع قصيرة على قصاصات الورق الصغيرة – إليكن بعض الأمثلة:
  - بعد هذه التجربة، لن تحتجن لشخص "متخصص تقنيًا" بعد اليوم.
  - هناك مجتمع خاص بالنساء/النسويات موجود وسيحميني.
  - آخذ نفسًا عميقًا وأعيد ضبط حاسوبي.
  - أنا قادرة على القيام بذلك – فقد أنجزت أمورًا أصعب من قبل.
  - لا تملك أجهزتي سطوة سحريّة عليّ – أنا أمسك بزمام الأمور.
  - الشخص الوحيد القادر على إتخاذ القرارات بشأن ممارستي للأمن الرقمي هوأنا.
- بعد أن تكتبن هذه الجمل، ضعن كل قصاصات الورق داخل الأزهار.

٢. أطلبن من المجموعة الجلوس ضمن حلقة وإسألنهن – كم مرّة شعرتن بالإحباط أو بسيطرة التكنولوجيا عليكن؟ ذكّرن الجميع أن هذا طبيعي جدًا، 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 تخطي أي مشكلة إذا عملن مع بعضهن البعض.

٥. والآن، أطلبن من المشاركات فتح أزهارهن – درن على الحلقة وأطلبن من كل واحدة قراءة الرسالة الموجودة فيها بصوتٍ عالٍ. إسألنهن إن كنّ يرغبن في مشاركة أحاسيسهن أو العبر المستخلصة من اليوم هذا، وما إذا كنّ يرغبن في مشاركة ما تعنيه الرسالة لهن.

باب ٥٥

الحلقة السحرية

- **الأهداف:** يقدم هذا التمرين خاتمة مناسبة لعملية التدريب أولجلسة واحدة، تقوم خلالها المشاركات بتحديد نيتهن بالاستمرار في مشاركة ما تعلمنه مع الأخريات.
- **الطول:** 30 دقيقة
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - لا يوجد
- **المواد اللازمة:**
  - ورقة وقلم

إدارة التمرين

١. تزداد المعرفة أو التجارب الجديدة فائدة عند مشاركتها وتعاطيها مع أشخاص آخرين. إشرحن أن الهدف من هذا التمرين هو أن تحدد المشاركات نيّة الاستمرار في مشاركة مع تعلّمنه خلال عملية التدريب مع الآخرين.

٢. أطلبن من المجموعة تشكيل حلقة – يمكنهن الجلوس على الأرض أو على كراسٍ أو الوقوف، وفقًا 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 المشاركين فيها حلقة حيث يُعتقد أنه من خلال الطاقة المنبعثة بين الأشخاص الواقفين على شكل حلقة، من الممكن طرد الأرواح الشريرة وإبقاء الأرواح الخيّرة؛
- 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 يحتلّ المركز الأوّل أو المركز الأخير – الجميع متساوٍ.

٤. أطلبن 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 مهمًا بالنسبة لها تعلمته خلال التدريب. ما أن ينتهي الجميع من كتابة شيء، أطلبن منهن ثني الورقة عند المنتصف.

٥. على كل مشاركة حمل الورقة المطوية التي كتبت عليها بيدها اليمنى. إشرحن لهن أن اليد اليمنى ترمز لقدرة الفرد على مساعدة الآخرين وأن اليد اليسرى ترمز لحاجته للتبادل

- يجب على المشاركات الآن الإمساك بأيدي بعضهن البعض في الحلقة، فتمسك اليد اليمنى لكل شخص اليد اليسرى للشخص الواقف إلى يمينه.

٦. على الجميع الآن إعطاء الرسالة المكتوبة للشخص الواقف إلى يمينه ونقلها من يده اليمنى إلى يد المتلقي اليسرى.

٧. على الجميع الآن قراءة ما على الورقة التي تلقينها - يمكنهن إما القيام بذلك بصوتٍ عالٍ أو بصمت.

٨. أثناء قراءتهن للرسائل، تحدث مع المجموعة عن فكرة التآخي بين النساء - الحب بين النساء اللواتي ينظر إليهن على أنهن متساويات وحليفات لبعضهن البعض، يبنين علاقات تضامن وتعاضد تحميهن من العنف والظلم وانعدام المساواة التي تواجههنا في حياتهن اليومية من أجل غدٍ أفضل. إشرحن لهن أنكن معًا، تدعمن بعضكن البعض ضمن علاقات أخوية نسائية وعبر مشاركة المعرفة والمعلومات مع بعضهن البعض.

باب ٥٦

الفوازير!

- **الأهداف:** غالبًا ما تكون التدريبات مكثّفة جدًا، وتقدّم كميات كبيرة من المعلومات يجب إستيعابها في مدّة قصيرة. هذا التمرين أداة يمكنكن استخدامها لإختبار معرفة وفهم المشاركات وفي الوقت عينه يقدّم بيئة مسلّية ومريحة تساعد على إزالة الإحساس بالإجهاد.
- **الطول:** 15 دقيقة
- **الشكل:** Exercise
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات علاقة:**
  - لا يوجد
- **المواد اللازمة:**
  - مصطلحات وحقائق عن أدوات السلامة الرقمية
  - شريط لاصق أو دبابيس
  - موسيقى (لتشغيلها في الخلفية)

- **التوصيات:** في حال صَعُب على بعض المشاركات التوصل إلى إجابات على الفوازير الخاصة بالمصطلحات والحقائق الخاصة بأداة الأمن الرقمي، في حين أن أخريات أنجزن التمرين في مجموعاتهن من شخصين، يمكن للواتي أنجزن التمرين مساعدة الأخريات على معرفة الإجابات على الأدوات المعطاة لهن.

إدارة التمرين

١. أطلبن من المشاركات الوقوف في خط واحد وهنّ يدرن ظهورهن 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 الملصقة المعطاة لهن!

٢. بعد الإنتهاء من ذلك، أطلبن من المشاركات توزيع أنفسهن في مساحة كبيرة فارغة في الغرفة (يمكن ترتيب ذلك عبر إزالة الكراسي أو المكاتب). إشرحن لهن أن المصطلح أو الحقيقة الملصقة على ظهر كل واحدة منهن تمثّل مفهومًا أو أداةً ناقشنها خلال التدريب.

٣. ضعن بعض الموسيقى – يمكن للمشاركات الآن التحرّك بحرّية في المساحة المتاحة. يمكنهن مدّ أجسادهن أو المشي أو التحرّك بأي طريقة يرغبن بها (ولكن عليهن عدم التوقف عن الحركة). إشرحن لهن أنه حين توقفن الموسيقى، على الجميع التوقف عن الحركة والبقاء في مكانه.

٤. أوقفن الموسيقى وأطلبن 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 الملصق على ظهرهن. بعد إن تتمكن 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 الملصقة على ظهورهن.

باب ٥٧

سباق الأمن الرقمي

- **الأهداف:** لإختتام التدريب بنشاط، ستوجهن المشاركات في سباق مشوّق لمراجعة المعرفة بشأن السلامة الرقمية التي تعلمنها.
- **الطول:** 45 دقيقة (وفقًا لسرعة المشاركات)
- **الشكل:** تمرين
- **المستوى المهاري:** أساسي
- **المعرفة المطلوبة:**
  - تتغيّر وفقًا لما تم تقديمه خلال التدريب.
- **جلسات/تمارين ذات علاقة:**
  - تتغيّر وفقًا لما تم تقديمه خلال التدريب.
- **المواد اللازمة:**
  - أقلام وأوراق لكتابة الرسائل ومغلفات
  - أوراق مطبوعة بالأسئلة (واحدة لكل مشاركة
  - مكان واسع في الخارج أو مساحة في الداخل فيها غرف وممرات مختلفة
- **التوصيات:** محتوى الحالات الذي ستستخدمنه في هذا السباق يعتمد على المحتوى الذي

تم تقديمه خلال التدريب – بما أن الهدف من هذا النشاط هو إجراء مراجعة شاملة للتدريب، يفضّل أن يجرى السباق في نهاية التدريب. الغاية من السباق هذا أيضًا مساعدتكن أنتن كمدربات على تحديد مكامن قوّة المشاركات والمجالات التي تحتجن فيها للمزيد من التدريب أو الدعم. هذا السباق مصمم بشكلٍ يتيح للمشاركات فرصة تطبيق ما تعلمنه خلال التدريب على المستوى العملي المباشر – لهذا السبب، لابد أن تركز الحالات المقدمة للمشاركات في هذا التمرين (أمثلة عن الحالات متوفرة أدناه) على سيناريوهات الإستجابة المباشرة للحوادث عوضًا عن التوصية بإجراءات وقائية.

إدارة التمرين

الجزء الأوّل – 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) – يفضّل أن ينفّذ 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 أنتن والمشاركات – سيمنحكن ذلك دفعًا إيجابيًا نظرًا لتغيير المكان.

٣. ستتضمن كل مرحلة حالة يتوجب على المشاركات حلّها 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 وتفادي الإزدحام عند أي مرحلة.

إليكن أدناه الموارد التي تحتاجن لها للإعداد للإختبار:

المورد الأوّل: ترتيب المراحل ودليل مسار الفرق

الفريق الأوّل	الفريق الثاني
المرحلة الأولى (الإنطلاق)	المرحلة الخامسة (الإنطلاق)
المرحلة الثانية	المرحلة الثالثة
المرحلة الثالثة	المرحلة الأولى
المرحلة الرابعة	المرحلة الرابعة
المرحلة الخامسة	المرحلة الخامسة
خط النهاية!	خط النهاية!E

المورد الثاني: الأدوات الخاصة بالحالة

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

المورد الثالث: الحالات الأمثلة

الحالة رقم 1

إنتهت مخرجة سينمائية لتوّها من تصوير فيلم وثائقيّ عن الإختفاءات القصرية في مصر. في مساء أحد الأيام، تترك 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 تعرّضت لمداهمة – والأسوأ في ذلك كله، هو أنها إنتبهت لأن الحاسوب المحمول الذي يحتوي على ملف الوثائقي النهائي مفقود (ولا تتوفر أي نسخ احتياطية له). بماذا تنصحن في هذه الحالة؟

الإجابة النموذجية الأداة الواجب استخدامها (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 احتياطية مادية أو على السحابة الإلكترونية لتسجيلات غير منقحة أومقابلات مصوّرة أوصور .... إلخ، يمكنها إستعادتها وتخزينها بشكلٍ آمن؛
- مراجعة أي ملفات يمكن إستعادتها لمعرفة ما لا يزال متوفراً معها، بالإضافة إلى تحديد مواقع الأجهزة أو المعدات التي إستخدمتها لتسجيل الوثائقي وتنقيحه؛

الحالة رقم 2

سارة ناشطة – قريبًا جدًا، ستبدأ بالعمل مع مجموعة من الناشطات على توثيق جرائم قتل النساء في لبنان. سيتوجب عليهن تشارك المستندات على الإنترنت ومناقشة معلومات حساسة عبر الهاتف، وسيكلّف عدد منهن بمهمة السفر إلى مدن معيّنة لإجراء مقابلات مع عائلات. بماذا توصين؟

الإجابة النموذجية الأداة الواجب استخدامها (من ضمن مجموعة الأدوات): البروتوكولات الأمنية

التوصيات:

- إعقدن إجتماعًا للمجموعة لإجراء عملية تقييم للمخاطر
- إتفقن على إجراءات الأمن الرقمي التي سيتوجب على المجموعة تنفيذها بالإضافة إلى بروتوكول السفر
- إتفقن على استخدام 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 الاتصال بالإنترنت قد نفذت على هاتفها وقررت عدم شراء تعبئة للبيانات أو لدقائق الاتصال لأنها ستترك البلاد. أثناء انتظارها للطائرة، أرادت الإطلاع على بريدها الإلكتروني عبر وصل هاتفها بشبكة الإنترنت اللاسلكية الخاصة بالمطار، ماذا يتوجب عليها فعله؟

الإجابة النموذجية الأداة الواجب استخدامها (من ضمن مجموعة الأدوات): الشبكات الإفتراضية الخاصة

الحالة رقم 4

مريم صحافية مغربية تجري تحقيقًا في حالة اختلاس أموال. لهذه الغاية، قدمت طلبات حصول على معلومات من حكومتها. ما هي الطريقة التي توصين باستخدامها من قبلها لتقديم هذه الطلبات بشكلٍ آمن

الإجابة النموذجية الأداة الواجب استخدامها (من ضمن مجموعة الأدوات): متصفح تور وحساب بريد إلكتروني مجهول الهوية

الحالة رقم 5

جماعة نسوية تدافع عن حق المرأة في إتخاذ القرارات تتعرّض للمضايقة منذ أسبوع على شبكات التواصل الاجتماعي، ماذا يمكنهن فعله لحماية أنفسهن؟

الإجابة النموذجية الأداة الواجب استخدامها (من ضمن مجموعة الأدوات): نموذج المخاطر القائمة على الجندر

التوصيات:

يمكن للجماعة تحليل المخاطر الناجمة عن الهجمات، وآثار واحتمالات ارتفاع 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 وفقًا لعدد أفراد المجموعة – لكي تتسنى للجميع فرصة المشاركة والمساهمة بشكلٍ متساوٍ، يوصى بألا يتخطى عدد أعضاء كل مجموعة الخمس مشاركات. لا تنسين أنه على كل فريق اختيار اسم مبتكر خاص به!

٥. والآن بعد أن الإنتهاء من تشكيل الفرق وتجهيز المراحل، إشرحن قواعد سباق الأمن الرقمي للمشاركات:

- وفقًا 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 لهن – يمكنهن اعتماد أسلوب الإبتكار في إجاباتهن: تمامًا كما هوالحال في الواقع، فلا حلول جاهزة لإسقاطها على أي مشكلة من أي حجمٍ كانت!
- أتركن للفرق بعض الوقت لتجهيز أنفسها – ومن ثمّ نادينَ "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 فى فضاء الإنترنت

INSTITUTE FOR
WAR & PEACE REPORTING
IWPR

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

البلد .....

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

لم تحدث مطلقًا (صفر نقاط)

في الأشهر الستة الماضية (نقطة واحدة)

خلال الأيام الثلاثين الماضية (خمس نقاط)

منذ أكثر من ستة أشهر (صفر نقاط)

لدينا النظام الأحدث مثبتًا على هذا الحاسوب (خمس نقاط)

هي قيد التحديث حاليًا (ثلاث نقاط)

لا أعرف هذه المعلومة (صفر نقاط)

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

لم تحدث مطلقًا (صفر نقاط)

منذ أكثر من سنة (نقطة واحدة)

خلال الأشهر الستة الماضية (نقطان)

خلال الأيام الستين الماضية (ثلاث نقاط)

خلال الأيام الثلاثين الماضية (أربع نقاط)

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

لا أعرف (صفر نقاط)

3. هل قرصكم الصلب أو خدمة السحابة الإلكترونية مشفّرة؟

نعم، كلاهما مشفّر (خمس نقاط)

لا (صفر نقاط)

إحداهما فقط مشفّر (ثلاث نقاط)

لا أعرف (صفر نقاط)

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

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

كل البرامج مقرصنة (صفر نقاط)

بعض البرامج مقرصنة (نقطة واحدة)

معظم البرامج برامج أصلية مرخّصة (نقطان)

كل البرامج مرخّصة وأصليّة (خمس نقاط)

معظم البرامج برامج مفتوحة المصدر (نقطان)

كل البرامج برامج مفتوحة المصدر (خمس نقاط)

لست متأكداً/متأكدةً (صفر نقاط)

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

نعم، الحاسوب والهاتف المحمول (خمس نقاط)

فقط على حاسوبي (ثلاث نقاط)

فقط على هاتفي المحمول (ثلاث نقاط)

ليس لدي برامج مكافحة للفيروسات (صفر نقاط)

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

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

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

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

نعم (خمس نقاط)

لا (صفر نقاط)

جهاز واحد فقط من هذين الجهازين مزوّد بكلمة سرّ

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

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

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

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

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

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

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

استخدم أحيانًا شبكات الإنترنت اللاسلكي في الفنادق أو المطارات أو المقاهي ولكن من دون الاتصال بها عبر خدمة شبكة افتراضية خاصة. (نقطان)

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

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

نعم (خمس نقاط)

لا (صفر نقاط)

لبعض المستندات فقط (ثلاث نقاط)

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

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

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

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

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

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

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

شريكي/شريكتي في الحياة (صفر نقاط)

أخوتي وأخواتي و/أو أهلي (صفر نقاط)

صديقي/صديقتي المفضل/ة (صفر نقاط)

زملائي في العمل (صفر نقاط)

لا أحد (خمس نقاط)

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

نعم (خمس نقاط)

لا (صفر نقاط)

واحد منها فقط (ثلاث نقاط)

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

نعم (خمس نقاط)

لا (صفر نقاط)

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

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

14. اتخذت قرارات إستراتيجية بشأن كيفية إدارة هوياتي على مواقع التواصل الاجتماعي

لحسابتي الشخصية والحسابات الخاصة بعملي/نشاطي استنادًا إلى مستوى الخطر المحدق بي. (على سبيل المثال، استخدام هويات وحسابات مختلفة/مزيّفة للنشاط/العمل، أو استخدام اسمي وصورتي وهويتي الحقيقية في حال لا أشعر أنني مهدد...)؟

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

لا – لم أفكر بالموضوع (صفر نقاط)

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

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

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

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

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

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

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

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

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

17. في ما يخص حساباتكم الشخصية على مواقع التواصل 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 (خمس 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 (نقطان)

أتوقع وصولها (ثلاث نقاط)

أعرف المرسل ويكون المرسل متحققًا منه (خمس نقاط)

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

نعم (خمس نقاط)

لا (صفر نقاط)

أحيانًا (نقطان)

لا أعرف ما هذا (صفر نقاط)

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

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

نعم (خمس نقاط)

لا (صفر نقاط)

فقط في مكتبي (نقطان)

فقط في منزلي (نقطان)

فقط لبعض الأجهزة (نقطان)

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

باب 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 إدناه.

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

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

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

ورشة عمل من يوم واحد ونصف اليوم حول تقييم المخاطر

المدة الزمنية التقريبية اللازمة: 10 ساعات

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

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

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

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

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

المدة الزمنية التقريبية اللازمة: 5 ساعات

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

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

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

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

المدة الزمنية التقريبية اللازمة: 7 ساعات

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

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

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

أمثلة عن جدوال أعمال لورش عمل ممتدة على ثلاثة أيام

تدريب تمهيدي ممتد على ثلاثة أيام

المدة الزمنية التقريبية اللازمة: 15 ساعة

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

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

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

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

تدريب متوسط المستوى ممتد على ثلاثة أيام

المدة الزمنية التقريبية اللازمة: 15 ساعة

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

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

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

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

تدريب متقدم ممتد على ثلاثة أيام

المدة الزمنية التقريبية اللازمة: 12 ساعة

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

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

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