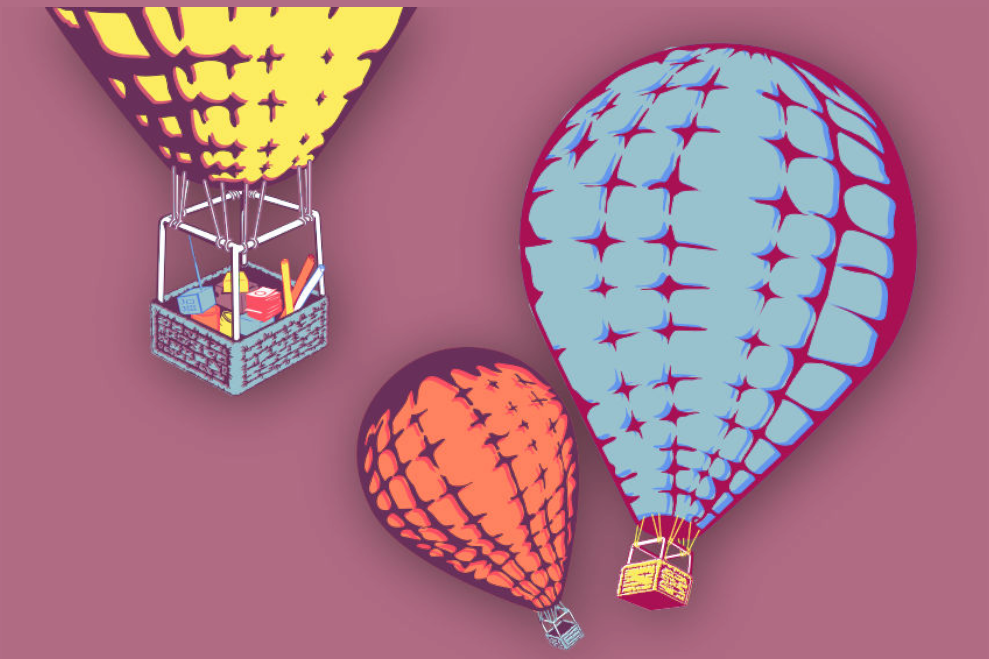

المناصرة الآمنة على الإنترنت

المناصرة الآمنة على الإنترنت

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

باب ١

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
- **مستوي المهارة:** متقدم
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أوتدريب مسبق
  - معرفة سابقة بكيفية إدارة المواقع الإكترونية
  - بمن نثقن؟ (تمارين بناء الثقة)
- **جلسات/تمارين ذات صلة:**
  - بمن نثقن؟[١]

[١] https://vrr.im/bd0d

- التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟[٢]
- الحملات الآمنة على الإنترنت[٣]

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

• **التوصيات:** هذه الجلسة تناسب مجموعات معينة أكثر من غيرها – 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 أواختراقات 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

[٢] https://vrr.im/47ba
[٣] https://vrr.im/8e6b

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 مناسبًا، 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. إستنادًا إلى الأمثلة التي تمت مشاركتها، يمكنكن الآن البدء بمشاركة بعض التوصيات الأولية بشأن الممارسات لتحسين مستوى حماية مواقعهن الإلكترونية. بعض الأمثلة تتضمن ما يلي – بحسب المستويات المختلفة من المعرفة ضمن المجموعة، قد يتوجب عليكن تقديم شروحات أكثر تفصيلاً لكل واحدة منها:

إختياري: حتى بالنسبة للمجموعات المزوّدة بحد أدنى من المعرفة أو المعلومات بشأن إدارة المواقع، قد يكون من المفيد شرح الطرق التي تدار المواقع بواسطتها قبل الإنتقال إلى التوصيات الواردة أدناه. قد تتضمن بعض مواضيع الأمثلة أنواع النطاقات ونظام أسماء النطاقات (Domain Name System DNS) و استضافة المواقع 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 (wid-gets) 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 الإحتياطية 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.

إختياري: 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 ٢

الحملات الآمنة على الإنترنت

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

[١] https://vrr.im/bd0d
[٢] https://vrr.im/f794
[٣] https://vrr.im/47e5
[٤] https://vrr.im/ac95
[٥] https://vrr.im/819e

- التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟[٦]
- مواقع إلكترونية أكثر أمانًا[٧]
- نموذج المخاطر القائمة على النوع الإجتماعي[٨]

• **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؟

[٦] https://vrr.im/47ba
[٧] https://vrr.im/bdeb
[٨] https://vrr.im/c0c3

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 نثقن؟. 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 الإجتماعي؟

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 إحتياطية 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[٩] وبرمجية "ويندوز بيتلوكر" (Windows BitLocker[١٠] 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.

[٩] https://en.wikipedia.org/wiki/FileVault
[١٠] https://en.wikipedia.org/wiki/BitLocker

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 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" KeeP-ass/" كي باس إكس" KeePassX[١١] بإنشاء ملفات قواعد بيانات فردية لكلمات سرّ الحسابات، التي تكون محمية بدورها بواسطة كلمة سرّ رئيسية؛ على نحو مماثل، بالنسبة للحسابات على غوغل وفايسبوك وتويتر يوصى بتفعيل خاصية التحقق بخطوتين التي توفر مستوى إضافي من القدرة على التحكّم، في حال كان لابد من مشاركة كلمة سرّ ما مع

[١١] http://keepass.info/

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[١٢] أو عبر الرسائل المشفّرة (بواسطة تطبيق سيجنال على هاتف محمول) من الخيارات الأكثر أمانًا – في حال إستخدام تطبيق سيجنال، إحرصن على تحديد بروتوكول مع أعضاء الفريق حول عملية حذف الرسائل المزوّدة بكلمات السرّ من أجهزتهن ما إن تصلهن.

الجزء الرابع – اختيار التطبيقات للحملات

١٠. عند تنفيذ وتنظيم حملة على الإنترنت، من الشائع استخدام تطبيقات وأدوات معيّنة للتمكن من متابعة أرقام وسائل التواصل الإجتماعي/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 الإجتماعي يمكننا متابعتها والتفاعل معها؟ ماذا يقول المستخدمون الآخرون عن التطبيق على الإنترنت على قنوات التواصل الإجتماعي الخاصة بهم؟

هل تتوفر أي منشورات على مدونات عن التطبيق مؤخرًا؟

[١٢] https://tutanota.com/

الجزء الخامس – بناء المجتمعات من خلال فايسبوك

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

يجب أن تدرك المشاركات أن لإستخدام 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 إستخدام 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 والإتصالات 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 إتصال وتنظيم بديلة – قد تتضمن هذه القنوات:

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

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

إستخدام خدمة تخدمة قوائم "رايز أب" Riseup[١٣] لإنشاء مجموعات بريد إلكتروني

[١٣] https://www.lists.riseup.net

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 خطراً كبيراً لذا يوصى بعدم عقد مثل هذه اللقاءات؛

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 ٣

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
- **مستوي المهارة:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات صلة:**
  - الجمهور الشبكي[١]
  - الحملات الآمنة على الإنترنت[٢]

[١] https://vrr.im/a184
[٢] https://vrr.im/8e6b

- **المواد اللازمة:**
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
  - شرائح (عليها النقاط المفتاحية الواردة أدناه)
  - أمثلة عن أدوات لتحليل البيانات الوصفية وإزالتها
- **التوصيات:** مع أن ذلك ليس ضروريًا، إلا أن هذه الجلسة سوف تكون أفضل بشكلٍ كبير في حال حصلت المشاركات من قبل على جلسة الجمهور الشبكي . غالبًا 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 جدًا 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.

غالبًا ما يعتبر موضوع البيانات الوصفية من الموضوعات المعقّدة التي يمكن تقديمها في العملية التدريبية، لذا إحرصن على سؤال المشاركات إن كان المفهوم واضحًا 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/