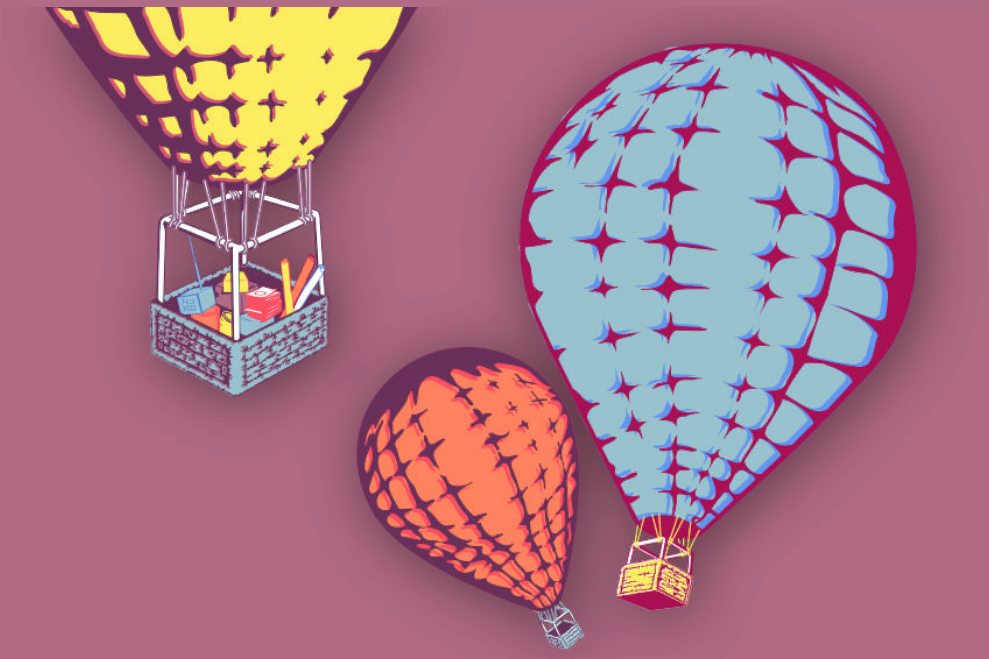

المناصرة الآمنة على الإنترنت

الحملات الآمنة على الإنترنت

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

باب ١

الحملات الآمنة على الإنترنت

- **الأهداف:** تهدف هذه الجلسة إلى مشاركة توصيات الأمن الرقمي للمدافعات عن حقوق الإنسان اللواتي يعملن على حملات على الإنترنت.
- **الطول:** 50 دقيقة
- **الشكل:** جلسة
- **مستوى المهارة:** متوسط
- **المعرفة المطلوبة:**
  - بمن نثقن؟ (تمارين بناء الثقة)
- **جلسات/تمارين ذات صلة:**
  - بمن نثقن؟[١]
  - بناء كلمات سرّ 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