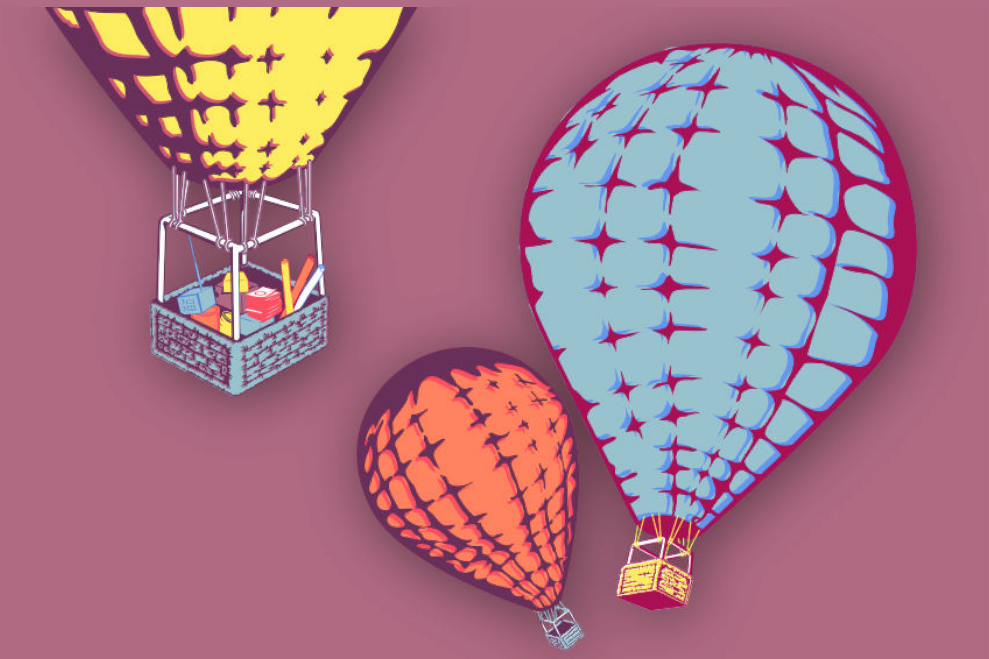

المناصرة الآمنة على الإنترنت

مواقع إلكترونية أكثر أمانًا

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