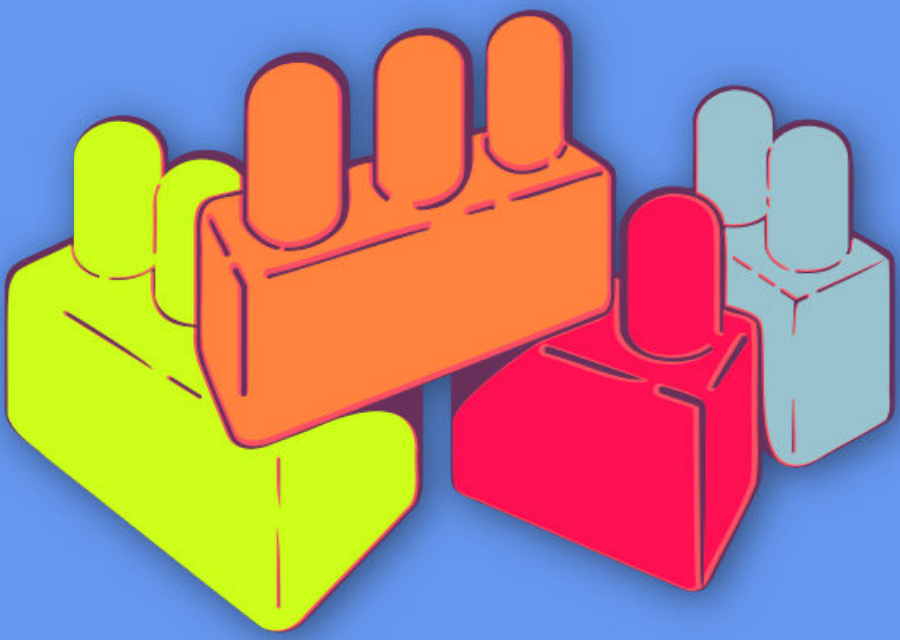

أسس الأمن الرقمي الجولة الأولى

البرمجيات الخبيثة والفيروسات

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

باب ١

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
- **مستوي المهارة:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات صلة:**
  - كيف يعمل الإنترنت؟[١]
  - كيفية حماية حاسوبكن[٢]
  - لنعد إلى خانة الصفر(إعادة الضبط)![٣]
- **المواد اللازمة:**

[١] https://vrr.im/7ba9
[٢] https://vrr.im/ac95
[٣] https://vrr.im/6a40

- 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 نحو مماثل، إحرصن بشكلٍ عام على إدراج دراسات حالات وأمثلة عن برمجيات خبيثة تواجهها المشاركات في تدريبكن ضمن بيئتهن.

الجزء الثاني – كيف يمكن أن تتعرضن 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 مبلغٍ مالي مقابل أن تستعيد إمكانية الوصول إلى معلوماتها.