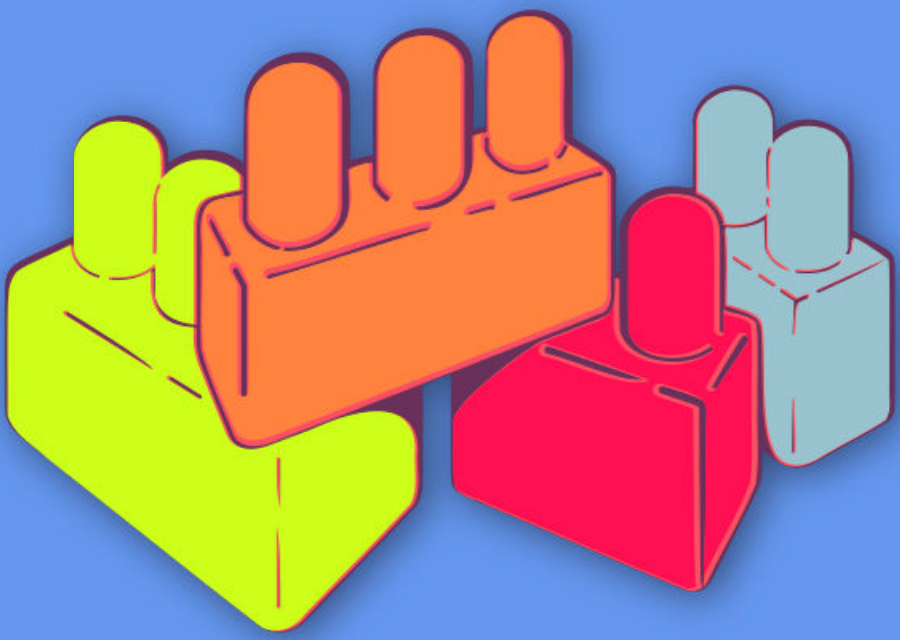

أسس الأمن الرقمي الجولة الأولى

كيف يعمل الإنترنت؟

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

باب ١

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
- **مستوي المهارة:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات صلة:**
  - حقوقكن والتكنولوجيا الخاصة بكن[١]
- **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

[١] https://vrr.im/1151

+ (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.

إختياري: 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:

إنعدام الأمن المادي: يفضل التخفيف من عرض الأجهزة في منظمتكن للغرباء إنعدام الأمن المادي: وضع كلمة سر على الحواسيب في المكتب وفي المنزل فقدان معلومات: المحافظة على نسخة إحتياطية في مكان غير المكتب أو المنزل فقدان معلومات: تحديد شخص مسؤول عن النسخ الإحتياطية 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) إنعدام التشفير: البدء في إستخدام أدوات وتقنيات تشفير مأمونة إنعدام 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 الإتصالات. المراقبة الدولية: الإنتقال إلى إستخدام 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) إستخدام 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 الإنتهاء من استخدامها. إستخدام 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: إستخدام زر + Cmd النقرة اليمنى لإفراغ سلّة المهملات على حاسوب
ماك حذف غير آمن: إستخدام 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