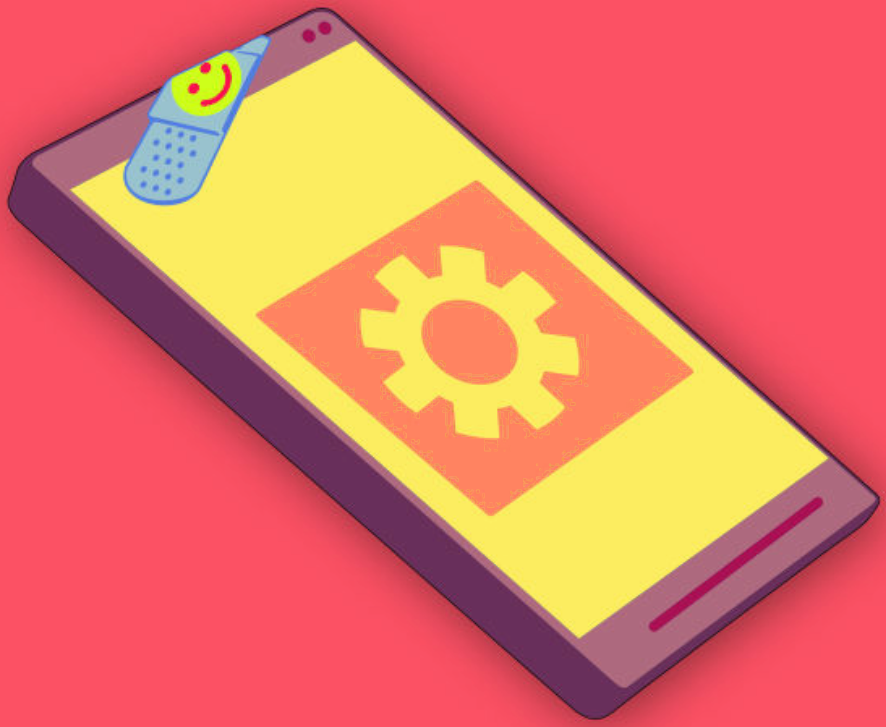

هواتف محمولة أكثر أمانًا

هواتف محمولة أكثر أمانًا

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

باب ١

ماركو بولو

- **الأهداف:** هذا التمرين البسيط مثاليّ لشرح كيفية عمل الهواتف المحمولة للمشاركات وكيفية تلقينا للرسائل النصية القصيرة والاتصالات الهاتفية وبيانات الاتصال بالإنترنت على أجهزتنا.
- **الطول:** 15 دقيقة
- **الشكل:** تمرين
- **مستوي المهارة:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات صلة:**
  - الخصوصية[١]
  - الجمهور الشبكي[٢]
- **المواد اللازمة:**
  - الإبداع!

يستند هذا التمرين إلى تمرين "ماركوبولو" الذي أنشأته مؤسسة كاريزما

[١] https://vrr.im/819e
[٢] https://vrr.im/a184

إدارة الجلسة

١. إختر إحدى المشاركات في المجموعة للعب دور "الهاتف المحمول" – من بعد تحديد المتطوّعة، أطلبن منها مغادرة الغرفة.

٢. في المساحة المتوفرة لديكن في مكان التدريب، قسّمن بقية المجموعة إلى "مبانٍ" و"هوائيات لاسلكية" وزعهن في كافة أرجاء الغرفة. إحرصن أن تتوزع الهوائيات بشكلٍ متساوٍ، بحيث تستطيع كل واحدة تحديد "نطاقٍ" خاص بها في الغرفة.يمكن لكل مشاركة وضع دائرة علي الأرض لتحديد نطاقها الخاص إذا كانت مساحة التدريب تسمح بذلك.

٣. أطلبن من الهاتف المحمول العودة إلى الغرفة، وإغماض عينيها. فسرن لها أنه سيتوجب عليها تحديد مواقع كل الهوائيات في الغرفة من خلال منادة كلمة "ماركو" – وستجيب الهوائيات بكلمة "بولو" ولكن فقط إذا مرّ الهاتف المحمول في جولتهن بالنطاق الخاص بكل هوائي .في هذا الأثناء يجب على المباني أن تبقى صامتة.

٤. أطلبن من الهاتف المحمول أن يحاول تحديد مواقع كل الهوائيات في الغرفة من خلال منادة كلمة "ماركو" - ما أن تنجح في تحديد مواقع كل الهوائيات، يمكنكن الآن شرح الوظائف الأساسية لشبكة الهواتف المحمولة:

تشغّل شركات الإتصالات هوائيات في مناطق مختلفة، توفر كل واحدةٍ منها التغطية لمنطقة (أو نطاق) معيّن؛

تتلقى الهواتف المحمولة التغطية عبر إرسال طلبات إلى الهوائيات الجديدة التي تلتقي بها ("ماركو") أثناء تنقلها من مكانٍ لآخر، وترد الهوائيات بـ ("بولو") على الطلبات عبر تقديم التغطية.

باب ٢

الهواتف المحمولة،الجزء الأوّل

- **الأهداف:** تقدم هذه الجلسة للمشاركات لمحة عامة تعريفية حول كيفية عمل الهواتف المحمولة من خلال شبكات الإتصالات الهاتفية.
- **الطول:** 60 دقيقة
- **الشكل:** جلسة
- **مستوي المهارة:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات صلة:**
  - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟[١]
  - ماركو بولو[٢]
- **المواد اللازمة:**
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
  - أوراق
  - شرائح (عليها النقاط المفتاحية الواردة أدناه)

---

[١] https://vrr.im/47ba
[٢] https://vrr.im/4450

- **التوصيات:** هذه الجلسة لها فعالية قصوى في حال قدّمت مباشرة من بعد تمرين ماركو بولو من هذه الوحدة، ولكن يمكن تقديمها وحدها أيضًا.

هذه الجلسة نسخة معدّلة من نشاط "كيف تعمل الهواتف المحمولة؟" التي وضعتها أليكس دون Alix Dunn (من منظمة "ذا أنجن روم" The Engine Room) لصالح منظمة "ليفل أب" LevelUp

إدارة الجلسة

إبدأن الجلسة بشرح المكونات الرئيسية للهواتف المحمولة للمشاركين. يمكنكن عرض صور لكل مكوّن منها ثناء الشرح.

الجزء الأوّل – ما هي مكونات الهاتف؟

١. على الرغم من أن بعض الهواتف، لا سيما الهواتف الذكية منها، تتمتع بقدرات متطوّرة، تتشارك كل الهواتف مكوّنات أساسية عدّة منها الآتي:

الهوائي

الهوائيات اللاسلكية، التي تسمح بالتواصل بين الهاتف المحمول والشبكات الخارجية، قد تكون ظاهرة في الأجهزة الأقدم – حيث في بعض الأجهزة القديمة جدًا كان من الضروري إخراجها يدويًا للتمكن من استخدامها. معظم الهواتف الحديثة العهد مزودة بهوائيات ضمن الجهاز مباشرةً، لذا لم تعد "ظاهرة". عدا عن الهوائي المسؤول عن التواصل مع شبكة الهواتف، قد تكون هذه الهواتف الحديثة مزوّدة بهوائيات للاتصال بشبكة الإنترنت اللاسلكي؛ بعض المصنعين يجمعون هاتين الوظيفتين في هوائي واحد للجهاز.

البطارية

البطارية هي ما يخزّن الطاقة اللازمة لتشغيل الهاتف المحمول، في معظم الهواتف من السهل إزالة البطارية. وفي بعض الهواتف الذكية الأحدث (لا سيما هواتف الآي فون ولاحقًا هواتف سامسونغ غالاكسي إس)، لم تُصمم البطاريات بشكلٍ يمكن المستخدم من إزالتها وقد يصعب الوصول إليها حتى. البطاريات القابلة للإزالة مفضّلة للمستخدمين الذين يعتمدون تكتيكات لرفع مستوى أمنهم.

المعالج المصغّر للنطاق الأساسي Baseband Microprocessor

يتولى هذا المكوّن إدارة إتصالات الهاتف، بما في ذلك الإتصالات والأوامر التي يصدرها المستخدم للهاتف، ومن الهاتف من وإلى شبكة الهواتف. يعتبر النطاق الأساسي في أي هاتف عادةً "ملكية" مهمة من قبل المصنعين وقد يعتبر "الصندوق الأسود" (لا يمكن الوصول إليه ويصعب التلاعب به) من حيث بروتوكولات إتصالاته وكيفية التحكّم بها والوظائف الأخرى الخاصة بالشبكة/الجهاز. قدرة شبكات الهواتف على تشغيل الهاتف وتحديد موقعه والإستماع عبر المايكروفون وتنزيل البيانات من الجهاز كلها مرتبطة بالنطاق الأساسي للجهاز.

شريحة الهاتف ومكان وضعها

هذا هو مكان تخزين شريحة الهاتف في الجهاز المحمول. قدرة تخزين البيانات على شريحة هاتفكن محدودة، ويمكن لبعض المستخدمين إتخاذ القرار بشأن حفظ بيانات معيّنة على شريحة هاتفهم أو في الذاكرة الداخلية للهاتف أو على وسائط قابلة للإزالة من عدمه. لا تنسين ذكر أن بعض الهواتف مصممة لتحمّل أكثر من شريحة واحدة؛ الهواتف الأخرى التي لا تعمل على شبكات غير شبكات النظام العالمي للاتصالات المتنقلة (GSM) (عادةً شبكات الوصول المتعدد باستخدام الشفرة المقسمة CDMA) غير مزوّدة بشريحة.

الوسائط القابلة للإزالة

الوسائط القابلة للإزالة تشمل أي نوع من وسائط تخزين الذاكرة الخارجية التي يمكن إدخالها وإزالتها من أي جهازٍ محمول، غالبًا ما تكون هذه الوسائط شرائح الذاكرة أو شرائح

الذاكرة المصغّرة. بعض الهواتف مزوّدة أيضًا بمنافذ أشعة تحت الحمراء (infrared) لنقل البيانات عبر الأشعة من هاتف لآخر، بالإضافة إلى خاصية البلوتوث Bluetooth)

آلات التصوير

معظم الهواتف اليوم مزودة بآلات تصوير قادرة على إلتقاط الصور و/أو الفيديو، لا سيما الهواتف الذكية. وعدد لا بأس به منها مزوّدٌ أيضًا بآلات تصوير في كل من الجهة الأمامية والجهة الخلفية من الجهاز، وغالبًا ما تستخدم آلتي التصوير هذه في تطبيقات إتصالات الفيديو من قبيل فايسبوك مسنجر أوسكايب.

الجزء الثاني – الممارسة التطبيقية

٢. أطلبن من المشاركات العمل ضمن مجموعات من شخصين ووضع لائحة بالمخاطر أو التهديدات المرتبطة بالهواتف المحمولة؛ ومن ثمّ، أطلبن منهن وضع لائحة أخرى ببعض الممارسات الموصى بها التي يعتقدن أنها قادرة على حماية أجهزتهن، في ما يتعلق بكل مكوّن من المكوّنات المذكورة في الجزء الأوّل أعلاه.

٣. ما إن تنتهي كل مجموعة من العمل، أطلبن منها عرض حلولهن على بقية المجموعة. إنصتن لما يذكر من الممارسات والأدوات التالية في عروضهن – في حال لم يتم ذكر أحدها، إحرصن على ذكر شرح موجز عنها بعد أن تنتهي كل المجموعات من العرض: برامج مكافحة الفيروسات على الهواتف المحمولة الشبكات الإفتراضية الخاصة التحقق من إعدادات ضبط التطبيقات كلمات سرّ قوية النسخ الإحتياطية للبيانات عدم شحن هواتفكن بواسطة منفذ مفتاح اليواس بي على أجهزة حاسوب عامة

المراجع

- https://securityinabox.org/en/guide/mobile-phones

https://level-up.cc/curriculum/mobile-safety/how-mobile- •
networks-work/input/how-do-mobile-devices-work/

باب ٣

الهواتف المحمولة،الجزء الثاني

- **الأهداف:** تعرّف هذه الجلسة المشاركات ذوات المعرفة المتوسطة بالأدوات والتوصيات اللازمة لتحسين مستوى أمن هواتفهن المحمولة.
- **الطول:** 50 دقيقة
- **الشكل:** جلسة
- **مستوي المهارة:** متوسط
- **المعرفة المطلوبة:**
  - ماركو بولو (هواتف محمولة أكثر أمانًا)
  - الهواتف المحمولة،الجزء الأوّل (هواتف محمولة أكثر أمانًا)
  - تعريف بمسألة التشفير (التشفير)
  - كيفية حماية حاسوبكن (أسس الأمن الرقمي،الجولة الأولى)
- **جلسات/تمارين ذات صلة:**
  - كيفية حماية حاسوبكن[١]
  - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟[٢]

[١] https://vrr.im/ac95
[٢] https://vrr.im/47ba

- ماركو بولو[٣]
- الهواتف المحمولة،الجزء الأوّل[٤]

- **المواد اللازمة:**
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
  - شرائح (عليها النقاط المفتاحية الواردة أدناه)
- **التوصيات:** إن أمكن ذلك، حاولن معرفة أنواع الهواتف التي تستخدمها المشاركات قبل التدريب – على سبيل المثال، قد يرد سؤالٌ عن ذلك ضمن عملية مسح تقييمية قبل التدريب. سيساعدكن ذلك في تعديل محتوى جلستكن ليتناسب وخصائص الأجهزة/أنظمة التشغيل التي تستخدمها المشاركات أصلاً. قبل البدء بالجلسة، ذكّرن المشاركات ببعض ممارسات الأمن الرقمي الأساسية التي يمكن تطبيقها في الهواتف المحمولة من قبيل: تحميل برمجيات مكافحة الفيروسات على الهواتف المحمولة، والشبكات الإفتراضية الخاصة للهواتف المحمولة، والتحقق من إعدادات التطبيقات وأذوناتها. أطلبن من المشاركات إجراء عملية نسخ احتياطي للملفات الموجودة على أجهزتهن قبل البدء بهذه الجلسة! بما أنهن سيتخدمن أجهزتهن الخاصة في هذه الجلسة، لابد أن يقمن بعملية نسخ إحتياطي لبياناتهن من باب الإحتياط.

إدارة الجلسة

الجزء الأوّل – التشفير في الهواتف المحمولة

١. ذكّرن المشاركات بالجلسات السابقة التي تناولت مفهوم التشفير، لا سيما جلسة التعريف بمسألة التشفير – ولعلكن أيضًا ناقشتن سابقًا التشفير من حيث تشفير الأقراص بشكلٍ شامل خلال جلسة كيفية حماية حاسوبكن. أذكّرن للمشاركات أن النسخ الأحدث من أنظمة آي أو أس وأندرويد (أيار/مايو 2017) مزوّدة بتشفير مفعّل تلقائيًا.

[٣] https://vrr.im/4450
[٤] https://vrr.im/7c02

الجزء الثاني – استخدام برمجية جي بي جي على الهواتف المحمولة

٢. في حال كانت المشاركات تعرفن التشفير بواسطة برمجية جي بي جي GPG، قدمن لهن خدمة البريد الإلكتروني "كاي 9" K-9 وبرنامج "آي بي جي" APG. ناقشن إيجابيات وسلبيات إستخدام تشفير جي بي جي على هاتف محمول (لا سيما خطر تخزين مفتاح جي بي جي خاص على هاتف محمول في مواجهة نقّاط الضعف الخاصة بالهواتف المحمولة) – المقصود هنا هوالتشديد على أن هذه القرارات قد تختلف من بيئة لأخرى؛ سيتوجب على المشاركات الإختيار بأنفسهن إن كانت إيجابيات إستخدام جي بي جي على هاتف محمول أكبر وأهم من السلبيات.

إختياري: إمنحن المشاركات الوقت الكافي لتثبيت والتدرّب على إستخدام "كاي 9" و"آي بي جي" خلال الجلسة – قد يرغبن بتجربة المفتاحين الجديدين اللذين قمن بإنشائهما للتعرّف على الأداة.

الجزء الثالث – هل يقوم هاتفكن بتعقبكن؟

٣. إسألن المشاركات – ما كمية المعلومات التي تعرفها هواتفنا عنّا؟ الهواتف هي وسيلة نستخدمها لإجراء عدد لا بأس به من أحاديثنا وبالتالي، هي قادرة على الوصول إلى معظم محتوياتها إن لم تكن كلها؛ وعلى نحو مماثل، لا تقوم الهواتف أيضًا بتعقّب المحتوى فحسب بل تتعقّب جهات الاتصال الخاصة بنا – فكل حديث مرتبط بفرد معيّن.

٤. قد ترغبن أيضًا في مناقشة كيف يمكن أن يعتبر نوع التعقّب الذي يجريه الهاتف نوعًا من أنواع المراقبة، وكيف أن المراقبة قادرة على الحدوث من خلال طرق كثيرة أخرى غير الطرق الإعتيادية المتوقعة. إسألن المجموعة عن أنواع المخاطر أو التهديدات التي يشعرن أنها محدقة بهواتفهن المحمولة، لا سيما في بيئة عملهن كمدافعات عن حقوق الإنسان.

المراجع

- https://securityinabox.org/en/guide/mobile-phones
- http://www.zeit.de/datenschutz/malte-spitz-data-retention