



# النساء فى فضاء الإنترنت



هواتف محمولة أكثر أمانًا

الهواتف المحمولة، الجزء الثاني

**INSTITUTE FOR  
WAR & PEACE REPORTING**



© 2019– Institute For War And Peace Reporting

<https://iwpr.net/>



نَسَبُ الْمُصَنَّفِ - الترخيص بالمثل 4.0 دولي

<https://creativecommons.org/licenses/by-sa/4.0/deed.ar>

# المحتويات

٥	الهواتف المحمولة، الجزء الثاني
٦	إدارة الجلسة
٦	الجزء الأول - التشفير في الهواتف المحمولة
٧	الجزء الثاني - استخدام برمجية جي بي جي على الهواتف المحمولة
٧	الجزء الثالث - هل يقوم هاتفك بتتبعك؟
٨	المراجع



## باب ١

# 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
  - مستوى المهارة: متوسط
  - المعرفة المطلوبة:
- ماركو بولو (هواتف محمولة أكثر أماناً)
  - الهواتف المحمولة، الجزء الأول (هواتف محمولة أكثر أماناً)
  - تعريف بمسألة التشفير (التشفير)
  - كيفية حماية حاسوبك (أسس الأمن الرقمي، الجولة الأولى)
  - جلسات/تمارين ذات صلة:
  - كيفية حماية حاسوبك<sup>١</sup>
  - التطبيقات والمنصات على الإنترنت: صديقة أم عدوة؟<sup>٢</sup>

---

<sup>١</sup><https://vrr.im/ac95>

<sup>٢</sup><https://vrr.im/47ba>

- ماركو بولو<sup>٣</sup>
- الهواتف المحمولة، الجزء الأول<sup>٤</sup>
- 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 سؤال 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، ذكرن المشاركات ببعض ممارسات الأمن الرقمي الأساسية التي يمكن تطبيقها في الهواتف المحمولة من قبيل: تحميل برمجيات مكافحة الفيروسات على الهواتف المحمولة، والشبكات الإقترابية 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 سيستخدمن أجهزتهن الخاصة في هذه الجلسة، لا بد أن يقمن بعملية نسخ احتياطي لبياناتهن من باب الاحتياط.

## إدارة الجلسة

### الجزء الأول - التشفير في الهواتف المحمولة

١. ذكرن المشاركات بالجلسات السابقة التي تناولت مفهوم التشفير، لا سيما جلسة التعريف بمسألة التشفير - ولعلكن أيضاً ناقشتن سابقاً التشفير من حيث تشفير الأقراص بشكلٍ شامل خلال جلسة كيفية حماية حاسوبكن. أذكرن للمشاركات أن النسخ الأحدث من أنظمة آي أو أس وأندرويد (أيار/مايو 2017) مزودة بتشفير مفعّل تلقائياً.

<sup>٣</sup><https://vrr.im/4450>

<sup>٤</sup><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، قد من لمن خدمة البريد الإلكتروني "كاي 9" K-9 وبرنامج "آي بي جي" APG. ناقشن إيجابيات وسلبيات استخدام تشفير جي بي جي على هاتف محمول (لا سيما خطر تخزين مفتاح جي بي جي خاص على هاتف محمول في مواجهة نقاط الضعف الخاصة بالهواتف المحمولة) - المقصود هنا هو التشديد على أن هذه القرارات قد تختلف من بيئة لأخرى؛ سيتوجب على المشاركات الاختيار بأنفسهن إن كانت إيجابيات استخدام جي بي جي على هاتف محمول أكبر وأهم من السلبيات.

إختياري: إنمنحن المشاركات الوقت الكافي لتثبيت والتدرّب على استخدام "كاي 9" و"آي بي جي" خلال الجلسة - قد يرغبن بتجربة المفتاحين الجديدين اللذين قمن بإنشائهما للتعرف على الأداة.

## الجزء الثالث - هل يقوم هاتفك بتعقبك؟

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 أيضاً بتعقب المحتوى فحسب بل تتعقب جهات الاتصال الخاصة بنا - فكل حديث مرتبط بفرد معين.

٤. قد ترغبن أيضاً في مناقشة كيف يمكن أن يعتبر نوع التعقب الذي يجريه الهاتف نوعاً من أنواع المراقبة، وكيف أن المراقبة قادرة على الحدوث من خلال طرق كثيرة أخرى غير الطرق الاعتيادية المتوقعة. إسألن المجموعة عن أنواع المخاطر أو التهديدات التي يشعرن أنها محددة 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>