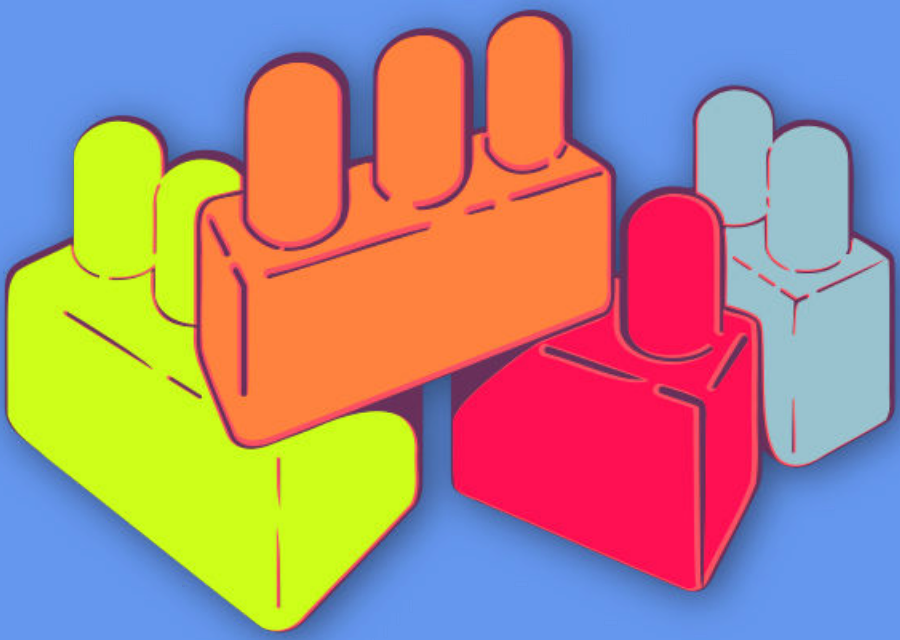

أسس الأمن الرقمي | الجولة الثانية

التخزين والتشفير

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

باب ١

التخزين والتشفير

- **الأهداف:** في هذه الجلسة، ستشددن على أهمية القيام بنسخ احتياطية للبيانات بشكلٍ دوري، وستناقشن كيفية منع التلاعب أو الوصول غير المسموح به لمعلومات المشاركات.
- **الطول:** 90 دقيقة
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أوتدريب مسبق
  - تعريف بمسألة التشفير (التشفير)
  - كيفية حماية حاسوبكن (أسس الأمن الرقمي،الجولة الأولى)
- **جلسات/تمارين ذات صلة:**
  - كيفية حماية حاسوبكن[١]
  - الخصوصية[٢]
  - الحملات الآمنة على الإنترنت[٣]

---

[١] https://vrr.im/ac95
[٢] https://vrr.im/819e
[٣] https://vrr.im/8e6b

- تعريف بمسألة التشفير[٤]

- **المواد اللازمة:**
  - شرائح (فيها النقاط المفتاحية الواردة أدناه)
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
  - نسخ مطبوعة عن نموذج النسخ الإحتياطي (أدناه)
  - مفاتيح يو إس بي أو نوع آخر من وسائط التخزين (لكل مشاركة)
- **التوصيات:** المشاركات في هذه الجلسة ستستخدمن إما برمجية "فيراكريبت" veracrypt أو "ماك كيبر" mackeeper (بحسب النظام التشغيلي الخاص بهن) للتدرّب على تشفير النسخ الاحتياطية للبيانات ووسائط التخزين – لتوفير الوقت، فكرن في الطلب من المشاركات تنزيل أي من هذه البرمجيات مسبقًا. بشكلٍ عام، ولا سيما للمبتدئات، لا ينصح بإجراء المشاركات لعملية تشفير شاملة للقرص الصلب على حاسوبهن الآن – عوضًا عن ذلك، يتوجب عليهن إختبار برمجيتي "فيراكريبت" أو "ماك كيبر" على وسيط تخزين خارجي (من قبيل مفتاح يو إس بي) باستخدام ملفات مزيّفة حضّرنها خصيصًا لهذه الجلسة. إذ حتمًا لا ترغبن في التعرّض لخطر فقدان إحدى المشاركات لإمكانية الوصول إلى أي بيانات خلال التدريب عن طريق الخطأ!

إدارة الجلسة

الجزء الأوّل – نسخ البيانات الاحتياطية والتخطيط

١. إسألن المشاركات – كم مرّة في السنة يقمن بنسخ احتياطية لملفاتهن؟ شاركن أمثلة عن الممارسات الفضلى في مجال إنشاء نسخ احتياطية للبيانات، من قبيل الإحتفاظ بالنسخة الاحتياطية في مكان آمن منفصل عن حاسوبهن، وإنشاء نسخ احتياطية لمعلوماتهن بشكلٍ دوري ومتكرر، بحسب للمعلومات التي يُنشأ لها نسخ احتياطية، والتفكير أيضًا في تشفير القرص الصلب أووسيط التخزين حيث سيقمن بتخزين البيانات.

[٤] https://vrr.im/f5d4

٢. شاركن مع المشاركات نموذج تنظيم النسخ الإحتياطي الوارد أدناه، وأطلبن منهن البدء بملئه بشكلٍ فرديّ. إشرحن للمجموعة أن الإستعانة به طريقة مفيدة لوضع سياسة شخصية خاصة بإنشاء نسخ احتياطية للبيانات – يمكنهن الإستعانة بهذا النموذج بعد التدريب، كمورد مفيد في متابعة مكان تخزينهن للبيانات وعدد المرّات التي يجب فيها إنشاء نسخ احتياطية للبيانات.

نموذج تنظيم النسخ الإحتياطي

- نوع المعلومات
- الأهمية/القيمة
- ما وتيرة إنتاجها أوتغييرها؟
- كم عدد المرات التي يجب فيها إنشاء نسخ احتياطية لها؟

الجزء الثاني – تشفير التخزين والنسخ الاحتياطية

٣. بعد أن تنتهي المشاركات من ملء نموذج تنظيم النسخ الاحتياطية، أطلبن منهن مراجعة أنواع المعلومات (إلى جانب أهميتها وقيمتها) الموجودة على لائحتهن مجددًا – أثناء قيامهن بذلك، أطلبن منهن التفكير في ما قد يحدث في حال وصلت هذه المعلومات إلى أحد خصومهن، أوفي حال فقدن هذه المعلومات كلها. ما أثر ذلك عليهن شخصيًا وعلى منظمتهن؟

٤. والآن، قدّمن مفهوم التشفير للمجموعة – إشرحن لهن أنهن على الأرجح يجدن التشفير مرات عدّة في حياتهن اليومية، فهو مستخدم بطرق مختلفة في أدوات ومنصات مختلفة. على سبيل المثال، يمكنكن الإشارة إلى أن "إيتش تي تي بي إس" هو نفسه شكل من أشكال تشفير البيانات "المتنقلة" (البيانات المنتقلة من النقطة "أ" إلى النقطة "ب") في حين أنهن في هذه الجلسة، ستناقشن تشفير البيانات "الثابتة" (أي البيانات المخزّنة في مكان واحد).

٥. ذكرن المشاركات بأنه طلب منهن تنزيل إما برمجية "فيراكريبت" أو برمجية "ماك كيبر" على حواسيبهن. إمنحن المشاركات الوقت اللازم لتثبيت هذه الأدوات وإختبارها،

بواسطة وسيط تخزين خارجي (من قبيل مفاتيح يو إس بي) وملفات مزيّفة حضّرنها خصيصًا لهذه الجلسة. لا ينصح بإجراء عملية تشفير شاملة لقرص الحاسوب الصلب الآن، لا سيما للمشاركات المبتدئات - إذ حتمًا لا ترغبن في التعرّض لخطر فقدان إحدى المشاركات لإمكانية الوصول إلى أي بيانات خلال التدريب عن طريق الخطأ!

المراجع

- https://securityinabox.org/en/guide/veracrypt/windows/
- https://securityinabox.org/en/guide/veracrypt/mac
- https://securityinabox.org/en/guide/veracrypt/linux