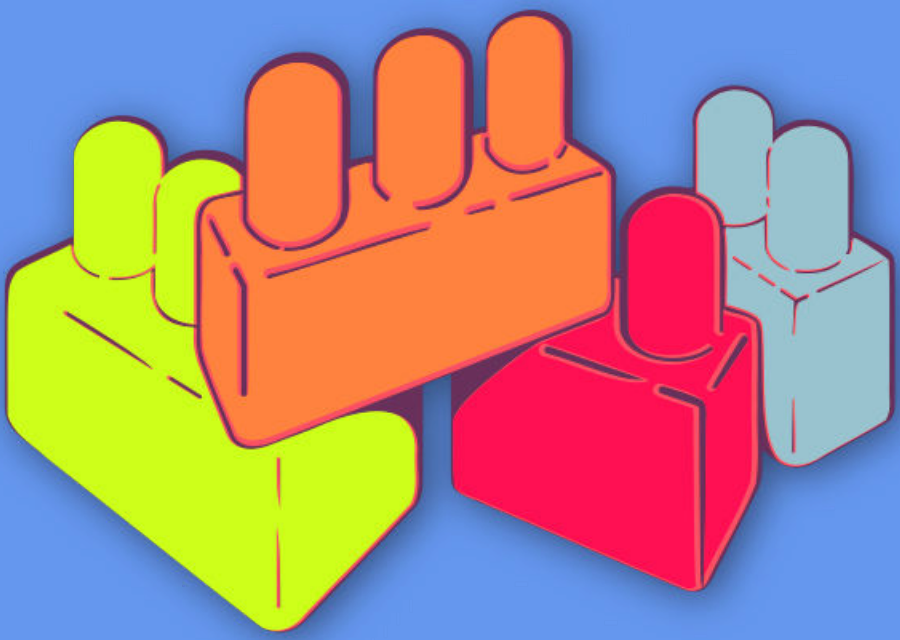

أسس الأمن الرقمي الجولة الأولى

كيفية حماية حاسوبكن

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

باب ١

كيفية حماية حاسوبكن

- **الأهداف:** تحديد الممارسات السليمة للمحافظة على سلامة حواسيبنا.
- **الطول:** 50 دقيقة
- **الشكل:** جلسة
- **مستوي المهارة:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات صلة:**
  - كيف يعمل الإنترنت؟[١]
  - البرمجيات الخبيثة والفيروسات[٢]
  - التصفّح الآمن[٣]
  - التخزين والتشفير[٤]
- **المواد اللازمة:**
  - شرائح (مع النقاط المفتاحية الواردة أدناه)

[١] https://vrr.im/7ba9
[٢] https://vrr.im/47e5
[٣] https://vrr.im/aee7
[٤] https://vrr.im/0ccc

- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز العرض
- نسخ مطبوعة عن نموذج متابعة النسخ الإحتياطي الوارد أدناه

• **التوصيات:** يوصى بأن تقمن بشرح مباشر - بواسطة جهاز عرض متصل بحاسوبكن - عن الأدوات التي تخترن التحدث عنها في هذه الجلسة، لكي تتمكن المشاركات من المتابعة والتدرّب على إستخدامها على حواسيبهن الخاصة من خلال إستخدام ملفات غير مهمة أنشئت لأغراض هذه الجلسة (وليس ملفات أو بيانات مهمة فعليًا!)

إدارة الجلسة

الجزء الأوّل - مقدمة

١. إسألن المشاركات إلى أي مدى حواسيبهن قيمة بالنسبة لهن - مدى فائدتها وضرورتها في حياتهن الشخصية والمهنية؟ ما هي كمية المعلومات المخزنة في حواسيبهن؟

٢. والآن، إسألن المشاركات - كم من الوقت يخصصن لصيانة أجهزتهن؟ غالبًا ما يكون الفرق بين مدى تقدير الناس لأجهزتهم وكم الوقت الذي يخصصونه لصيانتها والإعتناء بها كبيرًا جدًا. إشرحن للمجموعة أن هذه الجلسة ستركز على الممارسات الأساسية الخاصة بحماية الأجهزة.

الجزء الثاني - المحيط المادي والصيانة

٣. أخبرن المجموعة أن عددًا لا بأس به من الممارسات المرتبطة بسلامة الجهاز هي في الحقيقة مرتبطة أكثر بالسلامة المادية أكثر مما هي مرتبطة بالأمن الرقمي (هذه طريقة مفيدة لتعزيز التركيز الشامل لهذا المنهاج). أحد الأمثلة المفيدة في هذا الصدد هو أهمية تنظيف الأجهزة، أي التخلّص من الأوساخ أو الرواسب التي قد تتكدس داخل الجهاز، وإجراء عمليات تحقق دورية لتحديد ما إذا كان الجهاز قد تعرّض لأي تعديلات

مادية أو محاولات تطفّل ماديّة. في هذا الصدد، يمكنكن التوصية باعتماد ممارسات رقمية أساسية – كإستخدام كلمة سرّ لإقفال الجهاز في حال لم يكنّ في حوذتكن بعد إغلاقه – بالإضافة إلى أدوات الحماية المادية، كإستخدام حامي لوح المفاتيح (keyboard protector) أو سلك ضد سرقة لوحة المفاتيح (an anti-theft cable chain) لمنع أي سرقة أوإمكانية وصول غير مرغوبٍ بها. إحرصن على أن تشرن هنا إلى أن أهم جانب من جوانب سلامة أجهزتهن المادية هو الوعي. لابد من معرفة مكان وجود جهازٍ ما في أي لحظة – إما بحوزتهن وإما في غرفة أخرى وإما في مكان آمنٍ آخر.

٤. أطلبن من المشاركات إستذكار بعض التفاصيل عن مكان عملهن – ما هي المخاطر المادية المحتملة؟ هل حاسوبهن معرّض للسرقة؟ هل من أسلاك موضوعة بغير مكانها الصحيح؟ هل من الممكن أن يتعرض حاسوبهن للحرّ الشديد أو البرد أو الرطوبة؟ إليكن بعض الجوانب المهمة الأخرى المرتبطة بالوعي – الوعي المادي لا يقتصر فقط على الحرص بألا يصل أي خصم إلى أجهزتهن بل يتضمن أيضًا الضرر المحتمل الذي يتسبب به المكان الذي يتواجد فيه الجهاز.

الجزء الثالث – سلامة البرمجيات

٥. إشرحن للمشاركات مخاطر إستخدام برمجيات مقرصنة (من عيوب البرمجيات المقرصنة أنها تؤدي إلي إحتمالية أكبر لتحميل برمجيات خبيثة في أجهزتكن، ولايمكن إجراء عمليات تحديث دورية بالطريقة ذاتها التي تعتمدها البرمجيات المرخّصة... إلخ)؛ إلا أن البرمجيات المرخصة قد تكون باهظة الثمن في معظم الأحيان لذلك يمكنكن عندها مشاركة بعض الموارد مع المجموعة التي قد تساعد في معالجة هذه المشكلة مثل:

أوسلت Osalt[٥]

إفتحن متصفحًا وإبحثن عن "أوسلت" – هذا موقع إلكتروني يقدّم بدائل مجانية ومفتوحة المصدر لمعظم منصات البرمجيات المهمة المرخّصة (مثلاً استخدام نظام

[٥] http://www.osalt.com

أوبونتو Ubuntu بدل عن نظام ويندوز Windows؛ ليبر أوفيس LibreOffice بدل عن برنامج مايكروسوفت وورد Microsoft Office؛ إنكسكايب InkScape بدل عن أدوبي إلستراتور Adobe Illustrator).

تك سوب TechSoup[٦]

بواسطة "تك سوب"، يصبح المدافعون والمدافعات عن حقوق الإنسان ومنظماتهم مخوّلين للحصول على نسخ مجانية أو خاضعة لتخفيضات هائلة من البرمجيات التجارية: قد يبحث المستخدمون عن موزعين رسميين من ضمن مقدمي خدمات تقنية المعلومات والإنترنت المحليين أو يطلبون حسومات على الترخيص للقطاع العام أو لمنظمة لا تهدف للربح. تدير تك سوب شبكة توزيع كبيرة للبرمجيات المتبرّع بها – الرابط أعلاه يحتوي على قائمة بالشركاء والدول التي يعملون بها.

٦. إشرحن للمشاركات أهمية المحافظة على كافة برمجياتهن محدّثة – لأن ذلك يحميها من نقاط الضعف الأمنية. يجب أن تقمن بتنزيل كل البرمجيات والتحديثات من مصادر موثوقٍ بها فقط؛ على سبيل المثال، عند تحديث برنامج أدوبي أكروبات ريدر Adobe Acrobat Reader، يجب أن تستخدم التحديثات المنزّلة مباشرة من أدوبي وليس من مواقع أخرى.

٧. بعد ذلك، إشرحن للمشاركات أهمية توفر برنامج مكافح للفيروسات على حواسيبهن – وفرن بعض المعلومات التي قد تساعد في تفكيك بعض المعتقدات الشائعة الخاطئة المرتبطة ببرامج مكافحة الفيروسات، على شاكلة:

إستخدام برنامجين أو أكثر لمكافحة الفيروسات يوفر حماية إضافية. نظامي تشغيل ماك ولينوكس ليسا بحاجة لبرمجية مكافحة فيروسات لأنه لا يمكن أن تصاب بفيروسات. استخدام نسخة مقرصنة من برمجية مكافحة فيروسات آمن للغاية. برامج مكافحة الفيروسات المجانية غير آمنة أو موثوقة بها بالقدر ذاته كالبرامج المدفوعة.

٨. شاركن هذه الأفكار الشائعة، إلى جانب أي معتقدات أخرى قد تشاركها المشاركات معكن – ومن ثمّ ناقشن بعض الممارسات الآمنة الأساسية الخاصة باستخدام برمجيات

[٦] http://www.techsoupglobal.org/network

مكافحة الفيروسات والحماية من البرمجيات (راجعن جلسة البرمجيات الخبيثة والفيروسات من هذه الوحدة). بعض الممارسات المفيدة التي يجب التركيز عليها هنا، في حال لم تتحدث عنها في جلسة البرمجيات الخبيثة والفيروسات في هذه الوحدة، هي:

إستخدام البرنامج المضاف على المتصفحات "يوبلوك" uBlock لتفادي النقر على إعلانات قد تؤدي إلى تنزيل ملفات برمجيات خبيثة على حاسوبهن. التنبه لمحاولات التصيّد، وللروابط أو الملفات المرفقة المشبوهة الموجودة في رسائل بريد إلكتروني بشكلٍ خاص، والتي تبدو أنها أُرسلت من حسابات غير معروفة أو حسابات تبدو وكأنها مشابهة لجهات اتصال موثوقٍ بها. هذه فرصة سانحة جيدة للأتيان على ذكر جدران الحماية Firewalls – حيثُ تقدم جدران الحماية طبقة تلقائية من الحماية على حواسيبهن. شاركن أدوات من قبيل "كومودو فايروول" Comodo Firewall و"زون ألارم" ZoneAlarm و"غلاسوايز" e.Glasswir نسخ أحدث (مرخّصة) لنظاميّ التشغيل ويندوز وماك تتمتع بجدران حماية قوية مثبتة أصلاً.

الجزء الرابع – حماية البيانات والنسخ الإحتياطية

٩. إسألن المشاركات – كم مرة قمن بإنشاء نسخ إحتياطية لملفاتهن؟ شاركن أمثلة عن أفضل الممارسات المرتبطة بإنشاء نسخ احتياطية للبيانات، على غرار الإحتفاظ بالنسخ الإحتياطية في مكان آمن منفصل عن حاسوبهن، وإنشاء نسخ إحتياطية لمعلوماتهن بشكلٍ دوري ومعتاد – بحسب المعلومات التي أنشئت لها نسخ إحتياطية – والتفكير أيضًا في تشفير القرص الصلب أو وسيلة التخزين حيث ستُخزن البيانات.

١٠. شاركن مع المشاركات نموذج متابعة النسخ الإحتياطي الوارد أدناه، وأطلبن منهن البدء بملئه كل واحدة على حدة. فسرن للمجموعة أن هذه طريقة مفيدة لإنشاء سياسة شخصية لنسخ البيانات الاحتياطية – يمكنهن العودة إليه بعد التدريب، كمورد مفيد لمعرفة مكان تخزين البيانات والموعد اللاحق الذي يجب فيه إنشاء نسخ احتياطية جديدة.

نموذج متابعة النسخ الإحتياطي

نوع المعلومات	الأهمية/ القيمة	ما وتيرة إنتاجها أو تغييرها؟	كم مرة في الشهر/السنة يجب إنشاء نسخ احتياطية عنها؟

١١. فسّرن بعد ذلك، أنه على الرغم من توفر أدوات تقوم بنسخ إحتياطية بشكلٍ تلقائي (على غرار Duplicati.com أو كوبيان Cobian)، ولكنه يسهل عليهن البدء بإنشاء نسخهن الاحتياطية يدويًا عبر وضع الملفات في وسيلة التخزين الاحتياطية. هذا يعتمد في النهاية على مدى تعقيد أو كمية البيانات التي يتوجب عليهن التعامل معها – بالنسبة للمستخدم العادي غالبًا ما تكون عملية إنشاء النسخ الاحتياطية يدويًا أكثر من كافية.

١٢. لمتابعة النسخ الاحتياطية المحمية للبيانات، راجعن بإيجاز مفهوم تشفير وسائل التخزين. إشرحن للمشاركات ما يعني القيام بذلك، ولماذا يعتبر تشفير أقراصهن الصلبة أو وسيلة التخزين مفيدًا. تعتبر خدمتي "فيراكريبت" VeraCrypt و"ماك كيبر" MacKeeper من الخدمات الشائعة نسبيًا التي يستعان بها لتشفير الملفات أو الأقراص ويمكن ذكرها في هذا السياق كخيارات تستطيع المشاركات اعتمادها.

الجزء الخامس – حذف الملفات إستعادتها

١٣. إقرأن بصوتٍ عالٍ الجملة التالية:

من الناحية التقنية، لا وجود فعلي لخاصية حذف المعلومات على حاسوبكن.

إسألن المجموعة عن رأيها بتلك الجملة – هل هذه الجملة منطقيّة؟ كيف يمكن ألا تكون هذه الخاصية موجودة فعلاً؟ ذكرن المشاركات أنهن قادرات على توصيل الملف إلى سلّة المهملات على سطح مكتب حاسوبهن ومن ثمّ إفراغ السلّة، ولكن هذه العملية تقتصر

فقط على إزالة رمز الملف وإزالة أسم الملف من الفهرس المخبّأ الخاص بكل شيء على حاسوبهن ومن ثمّ إخبار نظام التشغيل أنه يمكن استخدام هذه المساحة لغرض آخر.

١٤. إسألن المجموعة – برأيكن ماذا يحدث للبيانات التي تقمن "بحذفها"؟. إلى أن يستخدم نظام التشغيل هذه المساحة الفارغة الجديدة، ستبقى مملوءة بمحتويات مرتبطة بالمعلومات المحذوفة، تمامًا كخزانة ملفات أزيلت فيها كل بطاقات التعريّف ولكن بقيت فيها كل الملفات الأصلية.

١٥. والآن إشرحن لهن أن ذلك يعود لكيفية إدارة الحاسوب لمساحة تخزين البيانات فيه، وفي حال توفرت لديهن البرمجية المناسبة وتصرفن بسرعة كافية، يمكنهن إستعادة المعلومات المحذوفة عن طريق الخطأ؛ لذلك تتوفر أيضًا أدوات يمكن إستخدامها لحذف الملفات بشكلٍ دائم (وليس فقط إزالتها من فهرس الملفات إلى أن تُشغل المساحة الشاغرة). إغتنمن هذه الفرصة لتقديم برمجية "سي كلينر" CCleaner، و/أو برمجية "إيرازر" Eraser، و/أو برمجية "بليتش بت" Bleachbit، كأدوات يمكن استخدامها لحذف الملفات وبرمجية "ريكوفا" Recuva كخيار يمكن اعتماده لإستعادة الملفات المحذوفة.

المراجع

- https://seguridaddigital.github.io/segdig/
- https://securityinabox.org/en/guide/malware
- https://level-up.cc/curriculum/malware-protection/using-antiviru s-tools
- https://securityinabox.org/es/guide/avast/windows
- https://securityinabox.org/en/guide/ccleaner/windows
- https://securityinabox.org/en/guide/backup
- https://securityinabox.org/en/guide/destroy-sensitive-information
- https://chayn.gitbooks.io/Avanzado-diy-Privacidad-for-every- woman/content/Avanzado-pclaptop-security.html