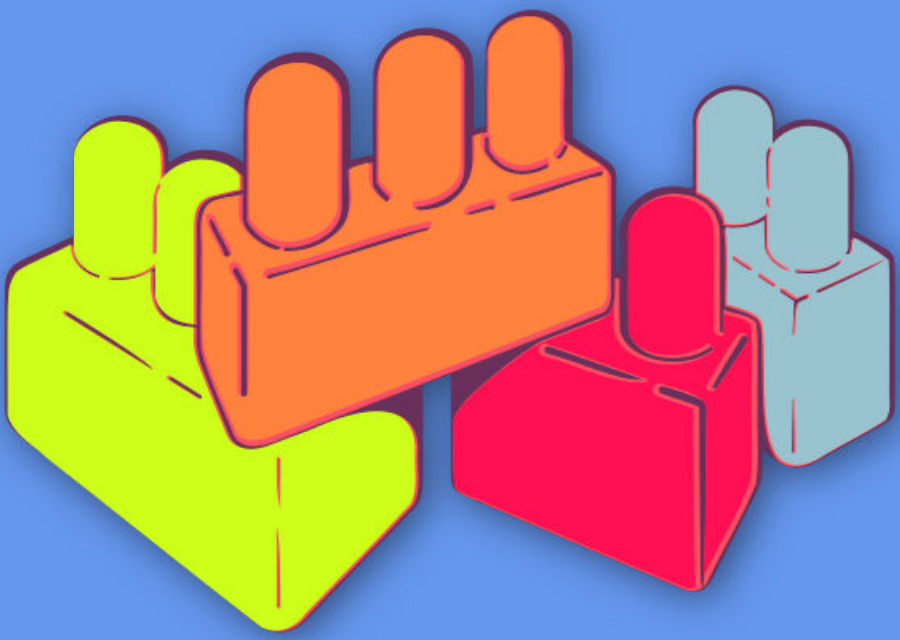

أسس الأمن الرقمي الجولة الأولى

أسس الأمن الرقمي الجولة الأولى

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

١ كيف يعمل الإنترنت؟ **٥**
إدارة الجلسة ٦
الجزء الأوّل – كيف يعمل الإنترنت – تدفق المعلومات ونقاط الضعف. ٦
الجزء الثاني – نقاط الضعف ٧
الجزء الثالث – الممارسات السليمة في الأمن الرقمي ٨
الجزء الرابع – الموارد والمسائل العالقة ١٠
المراجع ١٠

٢ بناء كلمات سرّ قويّة **١١**
إدارة الجلسة ١٢
الجزء الأوّل - المقدمة ١٢
الجزء الثاني – ما أهمية كلمات السرّ؟ ١٢
الجزء الثالث – ماذا قد يحصل في حال تعرض كلمة سرّكم للسرقة؟ . . ١٣
الجزء الرابع – كيفية تعرّض كلمات السرّ للسرقة عادةً؟ ١٤
الجزء الخامس – كيف يمكننا جعل كلمات سرّنا أقوى؟ ١٥
المراجع ١٦

٣ البرمجيات الخبيثة والفيروسات **١٧**
إدارة الجلسة ١٨

الجزء الأوّل – تعريف بالبرمجيات الخبيثة ١٨
الجزء الثاني – كيف يمكن أن تتعرض للإصابة بها؟ ١٨
الجزء الثالث – مشاركة أمثلة عن نساء ومدافعات عن حقوق الإنسان . ١٩

٤ التصفّح الآمن **٢١**
إدارة الجلسة ٢٢
الجزء الأول – إختيار المتصفّح ٢٢
الجزء الثاني – ممارسات التصفّح الأكثر أمانًا ٢٢
الجزء الثالث – الأدوات والبرامج المضافة من أجل تصفّح أكثر أمانًا . . ٢٤
المراجع ٢٦

٥ كيفية حماية حاسوبكن **٢٧**
إدارة الجلسة ٢٨
الجزء الأوّل – مقدمة ٢٨
الجزء الثاني – المحيط المادي والصيانة ٢٨
الجزء الثالث – سلامة البرمجيات ٢٩
الجزء الرابع – حماية البيانات والنسخ الإحتياطية ٣١
الجزء الخامس – حذف الملفات إستعادتها ٣٢
المراجع ٣٣

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

باب ٢

بناء كلمات سرّ قويّة

- **الأهداف:** في هذه الجلسة، ستقمن مع المشاركات بمراجعة تداعيات سرقة كلمة سرّ، وكيفية تعرضها للسرقة عادةً، وكيفية إنشاء كلمات سر أقوى، واكتساب عادات أفضل خاصة بكلمات السرّ.
- **الطول:** 45 دقيقة
- **الشكل:** جلسة
- **مستوي المهارة:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات صلة:**
  - كيف يعمل الإنترنت؟[١]
  - كيفية حماية حاسوبكن[٢]
- **المواد اللازمة:**
  - جهاز عرض
  - شرائح

---

[١] https://vrr.im/7ba9
[٢] https://vrr.im/ac95

- أوراق
- إمكانية اتصال بشبكة إنترنت لاسلكي/إنترنت من أجل تنزيل برمجية "كي باس" KeePass

تستند هذه الجلسة إلى وحدة "ممارسات كلمات السرّ الآمنة" الموضوعة من قبل تشيكاي سينكو Cheekay Cinco وكارول واترز Carol Waters وميغان ديبلوا Megan DeBlois لصالح "ليفل أب" LevelUp

إدارة الجلسة

الجزء الأوّل - المقدمة

١. إبدأن هذه الجلسة بطرح الأسئلة التالية على المشاركات:

متى كانت المرة الأخيرة التي قمن بها بتغيير أي من كلمات سرّهن؟

هل لديهن كلمات سرّ مختلفة لحساباتهن المختلفة؟

هل كلمات سرّهن مكتوبة على أوراق ملصقة في مكان ما؟

هل قمن بتخزين كل كلمات السرّ في أحد المستندات؟

هل هواتفهن مزودة بكلمة سرّ؟

الجزء الثاني – ما أهمية كلمات السرّ؟

٢. قبل أن تبدأن بالتحدث عن أهمية كلمات السرّ، أطلبن من المشاركات وضع لائحة بكل المعلومات المحمية بواسطة كلمة سرّ. ما هي المعلومات المتوفرة لديهن على حسابات بريدهن الإلكتروني وحساباتهن على مواقع التواصل الإجتماعي وهواتفهن المحمولة؟ ماذا قد يحصل في حال تمكن شخصٌ آخر من الوصول إلى تلك المعلومات؟

٣. والآن، شاركن مع المشاركات بعض الأسباب التي تبرر أهمية كلمات السرّ:

توفر كلمات السرّ إمكانية الوصول إلى عدد من الحسابات المهمة كحساب البريد الإلكتروني والحسابات المصرفية ومواقع التواصل الاجتماعي، إلخ.

غالبًا ما تحتوي هذه الحسابات على معلومات حساسة، ونحن في الغالب نتصرف على سجيتنا ونتفاعل بتلقائية مع الآخرين بواسطة خدمات رقمية متنوعة ونقوم بتبادل معلومات عديدة حساسة – وقد يتضمن ذلك إرسال رسائل عبر شبكات التواصل الإجتماعي أو إرسال رسالة بريدية إلكترونية أو إجراء علميات شراء على الإنترنت...،إلخ.

الحصول علي كلمات سر الأشخاص الآخرين تسمح بإنتحال صفاتهم/ن الشخصية- فأي شخص قادر على الوصول إلى كلمة سرّ حساب ما، يمكنه فعليًا التصرّف على الإنترنت وكأنه صاحب الحساب.

تمنح كلمات السرّ أيضًا إمكانية الوصول إلى عدد من الأمور الأخرى – نقاط التواصل مع شبكة الإنترنت اللاسلكية وفك كلمات سر الأجهزة المحمولة وتسجيل الدخول إلى الحواسيب وفكّ تشفير الأجهزة والملفات وغيرها.

الجزء الثالث – ماذا قد يحصل في حال تعرض كلمة سرّكم للسرقة؟

٤. في هذا الجزء من الجلسة، سنقوم بتوزيع الأوراق على المشاركات وسنطلب منهن وضع لائحة بكل المنصات التي يتذكرن أنه لديهن حسابات عليها. والآن أطلبن من المشاركات وضع لائحة بما قد يحصل في حال إستحوذ أحدهم على كلمة سرّهن وتمكن من الدخول إلى حساباتهن أو أجهزتهن:

قد تتعرض معلومات أو ملفات مهمة للسرقة (للنسخ) أو للحذف، في حال تعرضها للسرقة، قد لا تلاحظن ذلك مباشرة. وقد تكون المعلومات المسروقة أي شئ مثل مستندات أو ملفات مهمة أو حساسة جدًا أو قائمة جهات إتصال أو رسائل بريدية إلكترونية.

قد تتعرض أموال وحسابات بنكية للسرقة أو الصرف من خلال إمكانية الوصول إلى البطاقات الإئتمانية أو معلومات الدخول على الحسابات المصرفية.

يمكن إستخدام حسابات البريد الإلكتروني أومواقع التواصل الإجتماعي لإرسال الرسائل المزعجة أو لإنتحال شخصيتكن أو شخصية أصدقائكن أو أفراد عائلتكن أو زملائكن.

قد تصبح إمكانية الدخول إلي حساباتكن محتجزة إلى أن تقمن بدفع شكل من أشكال "الفدية" – قد يتضمن ذلك، دفع المال أو منح إمكانية وصول إلى جهات إتصال أو إلى حسابات أخرى.

قد يستخدم شخص ما كلمة السرّ الموجودة بحوزته للوصول إلى إتصالاتكن ونشاطاتكن ومراقبتها من دون علمكن.

قد تؤدي إمكانية الوصول إلى بريدكن الإلكتروني إلى تعرض حساباتكن الأخرى للخطر، إذ تستخدم لإعادة ضبط كلمات سرّ الحسابات الأخرى من خلال طلب روابط إعادة ضبط كلمات السرّ، وفي نهاية المطاف يصبح من المستحيل عليكن الوصول إلى حسابات أخرى كثيرة في حال لم تغيّرن كلمة السرّ.

الجزء الرابع – كيفية تعرّض كلمات السرّ للسرقة عادةً؟

٥. شاركن بعض الممارسات الشائعة التي قد تؤدي إلى حصول أشخاص آخرين على كلمات سرّكن:

حين تشاركنها مع الآخرين، أو تخزنّها بطريقة سهلة الكشف – من ضمن الأمثلة الشائعة، كتابة كلمة السرّ الخاص بتسجيل الدخول إلى حاسوبكن على ورقة صغير ملصقة على الحاسوب نفسه أو بالقرب منه. حين يرى أحدهم كلمة السرّ أثناء إدخالها على شاشتكن ويكتبها أو يحفظها عن غيب.

في حال إستخدام مقدم لخدمة البريد الإلكتروني من دون بروتوكول طبقة المنافذ الآمنة

(https) على مدى الجلسة، أو إستخدامه فقط على صفحة تسجيل الدخول، حيث يعرض ذلك كلمات السرّ والمعلومات الحساسة الأخرى للكشف أمام أي شخص لديه إمكانية الوصول إلى الرابط بعد تسجيل الدخول. يمكن الوصول إلى جهاز يدوياً، أما كلمات السرّ فيمكن الحصول عليها من خلال خاصيتيّ "احفظ كلمة سرّي" "Save My Password" أو "تذكرني" "Remember Me" الموجودتين على مواقع إلكترونية من خلال أي متصفح – يصبح ذلك ممكنًا بشكلٍ خاص في حال لا يتم إستخدام تشفير شامل للقرص على أي جهاز. البرمجيات الخبيثة كبرمجيات "كي لوغر" keylogger التي تعمل على توثيق كل نقرة على لوح المفاتيح على جهازٍ ما ومن ثمّ إرسالها لطرف آخر يريد هذه المعلومات. هذه البرمجيات الخبيثة ليست قادرة على كشف كلمات السرّ وحسب بل قد تصل أيضًا إلى معلومات حساسة أو شخصية. من الممكن أيضًا إختراق المنصات أو نقاط الضعف الموجودة في أنظمتها مما يتسبب بكشف معلومات مستخدميها.

الجزء الخامس – كيف يمكننا جعل كلمات سرّنا أقوى؟

٦. إشرحن للمشاركات أنه في حال إستخدامنا كلمات السرّ ذاتها لكل الحسابات، وتعرّض إحداها للسرقة، ستصبح كل حساباتنا مكشوفة. شاركن بعض ميزات كلمات السرّ الأكثر أمنًا وقوةً مع المجموعة:

الطول: بكل بساطة، كلما زاد طول كلمة السرّ كلما صارت أفضل! يوصى بإستخدام 14 حرفًا كحدٍ أدنى للحصول على كلمات سرّ قوية وفي حال إستخدام 20 حرفًا تصبح كلمة السرّ أقوى بكثير.

التعقيد: إستخدمن كلمة سرّ فيها أحرف وأرقام مع أحرف كبيرة وصغيرة مع تشكيلة غنيّة من الأرقام والرموز.

التغيير المستمر: غيّرن كلمات سركن بشكلٍ دوريّ، لا سيما تلك الخاصة بحساباتكن الحساسة، ولابد من تغييرها في حال وصلتكن رسائل بريدية موثوقٍ بها (ليست رسائل

تصيّد) تذكرن بأن حسابات المستخدمين آخرين وكلمات السرّ لديهم تعرّضت للسرقة.

إستخدام جمل سرّ بدلا عن كلمات السر (تخيلن كلمات سرّ مرتبطة ببعضها ضمن جملة) مثال آخرى عن ممارسة كلمات سرّ قوية – إليكن بعض الأمثلة:

SayNoToSexualHarassmentInMiddleEast ("لا للتحرش الجنسي في الشرق الأوسط")

MyRightToDecentShelter ("حقي في مسكن لائق)

WeDidNotChooseToBecomeRefugeesWeWereForcedToComeHere (لم نختر أن نصبح لاجئين/ات، بل أجبرنا على المجيئ إلى هنا)

٧. أطلبن من المشاركات التفكير لبضع دقائق قبل البدء بإنشاء بعض الأمثلة عن كلمات السرّ القوية. ذكرن المشاركات أنه يتوجب عليهن التفكير في مدى حساسية المعلومات الموجودة في حساب معيّن أثناء تفكيرهن في طول وتعقيد كلمات سرّهن – قد يرغبن في إستخدام أقوى كلمات السرّ لأهم حساباتهن، وفي الوقت عينه إستخدام أقلها تعقيدًا (مع المحافظة على قوتها) للحسابات الأقل أهمية.

المراجع

- https://level-up.cc/curriculum/protecting-data/creating-and-managing-strong-passwords/input/safer-password-practices/

باب ٣

البرمجيات الخبيثة والفيروسات

- **الأهداف:** تعالج هذه الجلسة أساسيات ماهية البرمجيات الخبيثة، وكيف يمكن أن تصبح الأجهزة المستخدمة معرّضة لأنواع مختلفة من البرمجيات الخبيثة، في سياق المخاطر المحدقة عادةً بالمدافعات عن حقوق الإنسان.
- **الطول:** 30 دقيقة
- **الشكل:** جلسة
- **مستوي المهارة:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات صلة:**
  - كيف يعمل الإنترنت؟[١]
  - كيفية حماية حاسوبكن[٢]
  - لنعد إلى خانة الصفر(إعادة الضبط)![٣]
- **المواد اللازمة:**

[١] https://vrr.im/7ba9
[٢] https://vrr.im/ac95
[٣] https://vrr.im/6a40

- شرائح (مع االنقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز العرض

• **التوصيات:** يفضل أن تتبع هذه الجلسة، جلسة كيفية حماية حاسوبكن، الموجودة في هذه الوحدة أيضًا.

إدارة الجلسة

الجزء الأوّل – تعريف بالبرمجيات الخبيثة

١. إشرحن للمشاركات ماهية البرمجيات الخبيثة وراجعن معهن بعض أنواع بالبرمجيات الخبيثة الموجودة – كحد أدنى، يوصى بأن تغطى البرمجيات التالية:

حصان طروادة (Trojan Horse)

برمجيات التجسس (Spyware)

برمجيات الفدية (Ransomware)

برمجيات تسجيل نقرات/ضربات لوحة المفاتيح (Keylogger)

تعرض معظم المدافعات عن حقوق الإنسان لبرمجيات الفدية وتسجيل النقرات الخبيثة بشكلٍ متزايد؛ في حال كنتن تعملن مع مجموعة من النساء لابد من معالجة هذه البرمجيات بالذات. على نحو مماثل، إحرصن بشكلٍ عام على إدراج دراسات حالات وأمثلة عن برمجيات خبيثة تواجهها المشاركات في تدريبكن ضمن بيئتهن.

الجزء الثاني – كيف يمكن أن تتعرضن للإصابة بها؟

٢. فسرن بعض الطرق الشائعة التي قد تصبح أجهزتكن من خلالها مصابة ببرمجية خبيثة، وما هي الممارسات غير الآمنة التي قد تؤدي إلى مثل هذه الإصابات. لابد أيضًا من شرح الأهداف أو المحفزات المختلفة التي تدفع إلى نشر البرمجيات الخبيثة:

تنشر بعض البرمجيات الخبيثة على نطاق واسع من دون هدف محدد. تستهدف أنواع أخرى الناشطات أو الصحافيات أو المناضلات بشكلٍ خاص من أجل الإستحواذ على بياناتهن أو االتصالاتهن.

بعض الأنواع الأخرى تستهدف أفرادًا يعرف عنهم إرتباطهم بعدد من الناشطات أو الصحافيات أو المناضلات على أمل إصابة أهداف متعددة ضمن الشبكة.

الجزء الثالث – مشاركة أمثلة عن نساء ومدافعات عن حقوق الإنسان

٣. إختتمن الجلسة بمشاركة بعض الأمثلة عن سيناريوهات إصابة ببرمجيات خبيثة تواجهها عادةً النساء والمدافعات عن حقوق الإنسان، يمكنكن مشاركة دراسات حالات معيّنة من مدونات أو مقالات أو تجربة شخصية عن نساء أو مدافعات عن حقوق الإنسان تعرضن لهذه التجربة . تذكرن أن لا تكشفن عن هوية الشخص المعني إلا إذا كان لديكن إذن صريح منها بالإفصاح عن أسمها.

إليكن بعض الأمثلة عن حالات عامة، وقد تعرفن حالات مشابهة في بيئتكن أيضًا:

تلقت إمرأة رسالة بريد إلكتروني عن فرص الحصول على تذاكر مجانية لحضور حفلة موسيقية، تسبب الرابط الموجود في الرسالة بإصابة هاتفها الذكي ببرمجية خبيثة.

إمرأة ناشطة تلقت رسالة مما يبدو أنه عنوان البريد الإلكتروني الخاص بزميلتها، بعد النقر على الرابط في البريد الإلكتروني، بات القرص الصلب في حاسوبها "مشفّرًا" وظهرت رسالة على شاشاتها تطالبها بتسديد مبلغٍ مالي مقابل أن تستعيد إمكانية الوصول إلى معلوماتها.

باب ٤

التصفّح الآمن

- **الأهداف:** توفر هذه الجلسة مقدمة حول ممارسات تصفّح الإنترنت الآمنة، بما في ذلك لمحة عامة عن البرامج المضافة والمنافع الأخرى الممكن استخدامها لإنشاء بيئة تصفّح أكثر أمانًا.
- **الطول:** 45 دقيقة
- **الشكل:** جلسة
- **مستوي المهارة:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات صلة:**
  - كيف يعمل الإنترنت؟[١]
  - كيفية حماية حاسوبكن[٢]
- **المواد اللازمة:**
  - شرائح (مع النقاط المفتاحية الواردة أدناه)

---

[١] https://vrr.im/7ba9
[٢] https://vrr.im/ac95

- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز العرض
- إمكانية اتصال بشبكة إنترنت لاسلكي

إدارة الجلسة

الجزء الأول – إختيار المتصفّح

١. إبدأن الجلسة بسؤال المشاركات عن متصفحات الإنترنت التي يستخدمنها والخيارات الأخرى التي سمعن عنها. قدمن لهن متصفّح فايرفوكس Firefox – إشرحن فوائد استخدامه وناقشن بإيجاز الفرق بينه وبين المتصفحات الشائعة الأخرى من قبيل غوغل كروم Google Chrome أو إنترنت إكسبلورير Internet Explorer.

إختياري: عند العمل مع النساء الناطقات باللغة العربية، قد تجدن هذا الفيديو مفيدا لبدء النقاش.

https://www.youtube.com/watch?v=cTrN1OAMYkM

الجزء الثاني – ممارسات التصفّح الأكثر أمانًا

٢. تتوفر بعض ممارسات التصفّح الأكثر أمانًا التي يمكنكن مناقشتها مع المشاركات – ومع أنكن غير مضطرات للتحدث عنها جميعها معهن، يوصى بأن تشاركن ما يكفي لإعطاء المشاركات خيارات متنوعة (لا تنسين أيضًا أن تحرصن على أن يكون المحتوى مناسبًا ومهماً لبيئة المشاركات).

٣. إشرحن للمجموعة أنكن ستقمن بمراجعة بعض ممارسات التصفّح الآمن معهن، ولكن لن تركزن الآن على أدوات محددة غير المتصفحات بحد ذاتها. بعض المشاركات قد يرغبن منذ هذه اللحظة بتغيير المتصفحات التي يستخدمنها ولكن الأخريات قد لا يكن جاهزات لذلك – لذا قبل مناقشة بعض الأدوات المحددة كالبرامج المضافة إلى

المتصفحات، لابد من إبقاء تركيز النقاش على الممارسة في البدايةً.
إليكن بعض الممارسات التي يمكنكن طرحها للنقاش:

البقاء متيقظات تجاه محاولات التصيّد والتصيّد المستهدف.
حجب الإعلانات المضمنة (embedded ads) والإعلانات المفاجئة. (pop-up ads)
معرفة كيفية عمل ملفات تعريف الإرتباط (كوكيز) – إحرصن على التحدث عن مدى تسهيلها للتصفّح ولكن أيضًا عن سلبياتها.
تعطيل ومحو ملفات تعريف الإرتباط من المتصفحات.
محو سجل التصفّح؛
عدم حفظ كلمات السرّ في إعدادات متصفحكن.
التحقق من البرامج المضافة التي قمتن بإضافتها إلى متصفحكن.
تشغيل خيار "عدم التعقّب" (Do Not Track) في متصفحكن.
استخدام بدائل عن محرّك بحث غوغل (مثل دك دك غو Duck Duck Go)
معرفة من يقوم بالتعقّب على الإنترنت ولماذا؟ (كلا الرابطين الموردين أدناه جيدين عن هذه المسألة https://trackography.org/
و https://www.mozilla.org/es-MX/lightbeam/)؛
ناقشن الفرق بين HTTP و HTTPS؛
ما هي الشبكات الإفتراضية الخاصة ومتى يجب إستخدامها؟
كيف يعمل بالظبط التصفّح المتخفي (Incognito Mode or Private Browsing)، ومتى يجب استخدامه؟

الجزء الثالث – الأدوات والبرامج المضافة من أجل تصفّح أكثر أمانًا

٤. إشرحن، بعد أن عالجتن بعض الممارسات الأساسية للتصفّح الآمن، أنه يمكنكن أيضًا إقتراح أدوات معيّنة – البرامج المضافة بالتحديد – التي قد تساعد أو تسهّل عملية إعتماد بعض تلك الممارسات تلقائيًا.

٥. قدمن لهن الأدوات التالية، شارحاتٍ لهن كيفية عمل كل واحدة منها، ولا تنسين أيضًا مشاركة الروابط اللازمة لتنزيلها مع المشاركات. لابد أن تفهم المشاركات أهمية وفائدة كل أداة تمت مشاركتها معهنّ؛ ففي حال لم تشرحنها بشكلٍ واضح، قد يؤدي ذلك إلى إتخاذ المشاركات قرارات مبنية على معلومات خاطئة بشأن خصوصيتهن أوإخفاء هويتهن على الإنترنت.

أدوات متصفح سطح المكتب

أداة "نو سكريبت" [٣](NoScript)

أداة "آدبلوك بلس" [٤](AdBlock Plus)

أداة "برايفيسي بادجر" [٥](Privacy Badger)

أداة "إيتش تي تي بي إس إفريوير" [٦](HTTPS Everywhere)

أداة "كليك أند كلين" [٧](Click & Clean)

متصفّح "تور" [٨](Tor)

---

[٣] https://noscript.net/
[٤] https://adblockplus.org/es/
[٥] https://www.eff.org/es/privacybadger
[٦] https://www.eff.org/https-everywhere
[٧] https://www.hotcleaner.com/
[٨] https://www.torproject.org/download/download-easy.html.en

أداة "يوبلوك" [٩](uBlock)

أداة "ديسكونكت" [١٠](Disconnect)

أداة "يومايتركس" [١١](uMatrix)

أدوات متصفحات الهواتف المحمولة

أداة "إيتش تي تي بي إس إفريوير" [١٢](HTTPS Everywhere)

مكافح الفيروسات "أفاست" [١٣]Avast

أداة "أورفوكس" [١٤](Orfox)

أداة "أوربوت" [١٥](Orbot)

متصفح "تور" [١٦](Tor) لهاتف آيفون

ممارسات وميزات أخرى

التصفّح المتخفي (Incognito Mode/InPrivate Mode)

غالبًا ما تتسبب هذه الميزة بالإلتباس لأنها غير مفهومة بشكلٍ مناسب – وقد لا يتوفر لدى المشاركات فكرة واضحة عن كيفية عمل التصفّح المتخفي كميزة من ميزات المتصفحات ومتى يكون استخدامها مفيدًا. فسّرن لهن كيفية عمل ميزة التصفّح (والميزات المشابهة)، وقدمن لهن بعض الأمثلة عن الحالات التي قد تكون فيها هذه الميزات مفيدة فعليًا.

---

[٩] https://www.ublock.org/

[١٠] https://disconnect.me/

[١١] https://addons.mozilla.org/es/firefox/addon/umatrix/

[١٢] https://www.eff.org/https-everywhere

[١٣] https://www.avast.com

[١٤] https://guardianproject.info/apps/orfox/

[١٥] https://www.torproject.org/docs/android.html.en

[١٦] https://mike.tig.as/onionbrowser/

الممارسات الآمنة على شبكة الإنترنت اللاسكي

ختامًا، ناقشن لبعض الوقت، وقدمن شرحًا إذا أمكن، لبعض الممارسات الآمنة الأساسية الخاصة بالإتصال بشبكات الإنترنت اللاسكي - يتضمن ذلك ممارسات كتغيير كلمات السرّ المحددة مسبقًا الخاصة بالمودم، وشرح كيفية مراقبة الأجهزة المتصلة بشبكة الإنترنت اللاسلكي الخاصة بهن.

المراجع

- https://myshadow.org/ckeditor_assets/attachments/189/datadetoxkit_optimized_01.pdf
- https://myshadow.org/train
- https://myshadow.org/how-to-increase-your-privacy-on-firefox
- https://securityinabox.org/en/guide/firefox/linux/

باب ٥

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