الملحق الرابع عشر

لائحة تحقُّق: أمن أجهزة الحاسوب و الهاتف

لا يُراد بلائحة التحقُّق هذه أن تكون نموذجاً يُتَّبع في موقفكم الأمني. إنَّ سياقكم المخصوص هو العامل الأساسي في تحديد ما يتعيَّن اتخاذه من إجراءات. يتعيَّن أن تأخذوا في الحسبان ما تواجهونه من تهديدات، و ما قد يكون لديكم من نقاط الضعف، لتضيفوا على هذه اللائحة ما هو ضروري، و تجعلوها أكثر ملاءَمة لوضعكم. إنَّها أيضاً قائمةٌ بالنقاط الأساسية. أنظروا إصدارة الأمن في صندوق http://security.ngoinabox.org/ar لمعلوماتٍ إضافية و تفصيلية كثيرة.

تتضمن هذه المعلومات عدداً من النصائح التي توجد أيضاً على بطاقات الوعي في مشروع الأمن في صندوق – أنظر الرابط أعلاه.

١. **قوموا بحماية حاسوبكم من البرمجيات الخبيثة و المخترقين/ الهاكرز**:
- استخدموا برامج مضادة للفيروسات، و أخرى مضادة لبرمجيات التجسس، و جداراً نارياً firewall.
- لا تستخدموا البرمجيات المقرصنة – فهذه تجعلكم معرَّضين للقصور و بالتالي المخاطر، نظراً للنقص في تحديثات هذه البرمجيات، فضلاً عن الاتهام بحيازة برمجيات غير مرخصة.
- انظروا في إمكانية استخدام البرمجيات المجانية مفتوحة المصدر AVAST، مثل برنامج Spybot لمحاربة الفيروسات، و برمجية FOSS المضادة لبرمجيات التجسس، و جدار Comodor الناري.
- فكِّروا في استخدام متصفح إنترنت أكثر أمناً، مثل Firefox، الذي يتضمن إعدادات خاصة بالأمن.

يمكنكم الاطلاع على الفصل الأول من إصدارة الأمن في صندوق لمزيد من المعلومات حول كيفية حماية الحاسوب الخاص بكم.

٢. **أعِدُّوا كلمات سرٍّ آمنة و حافظوا عليها**:
- كلما طالت كلمة السر كان ذلك أفضل، و ينبغي أن تزيد على اثني عشر رمزاً (حرفاً أو عدداً أو علامة ترقيم)، و أن تتضمن حروفاً في الحالتين العُليا و السُفلى (توضيح: في اللغة الإنجليزية تُكتب الحروف إما ((Upper case: A,B,C أو (Lower case: a,b,c) المترجمة)، بالإضافة إلى الأرقام، و الرموز الخاصة، و فراغ space إذا أمكن.
- من المحبَّذ ألاّ تتضمن كلمة السر الخاصة بكم كلمات توجد في القاموس و/ أو معلومات متاحة للجميع عن شخصكم، كتاريخ الميلاد أو اسم الصديق المقرَّب. قوموا بخلط الكلمات أو استبدلوها برموز معينة أو أرقام، أو اخلطوا بين لغتين أو أكثر.
- فكروا في إمكانية استخدام عبارة لتكون كلمة السر، و يمكن أن يكون هذا عنوان كتاب ما أو مقطعاً من أغنية (مع استبدال الحروف بالرموز أو الأرقام).
- غيِّروا كلمات السر في أوقات متقاربة.
- أعِدُّوا كلمات سر قوية (أي يصعب اكتشافها أو تخمينها)، و لتكن مختلفة في كل خدمة، و قوموا بتحديثها بانتظام، و لا تطلعوا أحداً على كلمات السر (انظروا في إمكانية استخدام KeePass لحفظ جميع كلمات السر – يمكنكم الاطلاع على الفصل الثالث من إصدارة الأمن في صندوق لمزيد من المعلومات عن KeePass).
- لا تطلعوا أي شخص على الإطلاق على كلمات السر الخاصة بكم.
- لا تسمحوا مطلقاً لأي مواقع إلكترونية و برامج بتخزين كلمات السر الخاصة بكم.

يمكنكم الاطلاع على الفصل الثالث من إصدارة الأمن في صندوق لمزيد من المعلومات عن كلمات السر الآمنة.

٣. **كيفية حماية الملفات الحساسة على جهاز الحاسوب**:
- قوموا بإعداد نسخ احتياطية للملفات بانتظام، و احتفظوا بالنسخة في مكان آمن.
- قوموا بإخفاء الملفات الحساسة تحت أسماء عادية لا تشير إلى محتواها الحقيقي.
- انظروا في إمكانية ترميز جميع ملفاتكم (غير أن الترميز غير قانوني في بعض البلدان، و يمكن أن يلفت الانتباه إليكم).
- في وسع أحد تطبيقات FOSS المسمَّى TrueCrypt أن يرمِّز ملفاتكم و يخفيها معاً.
- يمكن أن يقوم خبير باسترجاع الملفات التي قمتم بمسحها – انظروا في إمكانية استخدام أداة مسح آمنة، مثل (CCleaner (التي تمحو الملفات المؤقتة) و Eraser.

- تحققوا إن أمكن من سُمعة مزوِّد خدمة الإنترنت أو الموقع الذي تعتزمون منه الاتصال بالإنترنت، كأحد مقاهي الإنترنت مثلاً.
- تأكدوا من أن الأشخاص الذين تتراسلون معهم يملكون بدورهم الوعي بالمسائل الأمنية و قضايا الخصوصية. إن الاتصال عملية ثنائية الاتجاه. و لن تجدي محاولاتكم نفعاً إذا كان الطرف الآخر غير مهتم بالأمن و الخصوصية.

يمكنكم الاطلاع على الفصلين الرابع و السادس من إصدارة الأمن في صندوق لمزيد من المعلومات.

٤.الإبقاء على خصوصية اتصالاتكم بواسطة الإنترنت:

- إن الكثير من حسابات البريد الإلكتروني غير آمنة (بما في ذلك Yahoo و Hotmail)، و تقوم بعرض عنوان IP الخاص بكم في الرسالة التي تبعثون بها. إنَّ حسابات Gmail و Riseup أكثر أماناً (على الرغم من أن Google أذعنت فيما مضى لمطالب الحكومات التي تفرض القيود على الحريات الرقمية).
- يمكن أن يعرضكم استخدام مقاهي الإنترنت إلى المراقبة – كونوا مدركين تماماً للمخاطر، و متنبِّهين للأشخاص الذين تتواصلون معهم و للمعلومات التي تتبادلونها. قوموا بمحو كلمة السر و تاريخ التصفُّح browsing history بعد الانتهاء.
- استخدموا https بدلاً من http عندما تتصلون بالخدمات التي تستعملونها على الإنترنت، بقدر الإمكان، بحيث يتم نقل اسم المستخدم الذي يخصكم، و كلمة السر، و سواها من المعلومات على نحو آمن.
- لا تقوموا بفتح المرفقات بالرسائل الإلكترونية الواردة من أشخاص لا تعرفونهم، أو ما يبدو منها باعثاً على الريبة.
- كونوا متنبِّهين بنحو خاص عندما ترسلون معلومات حساسة أو تتلقونها أو تشاهدونها، بواسطة الإنترنت.
- انظروا في إمكانية استخدام خدمة proxy أو أحد تطبيقات المجهولية anonymity، التي تجعلكم أشخاصاً غير معروفين كمستخدمين محددين للإنترنت؛ إذ يسمح لكم هذا بالوصول إلى الإنترنت و التواصل عبرها مستخدمين عنوان IP يخص حاسوباً آخر.
- إن التراسل الفوري chat ليس أداة آمنة في العادة، و مع ذلك، فإنَّ Skype قد يكون أكثر أمناً من نظرائه لهذه الغاية.

يمكنكم الاطلاع على الفصلين السابع و الثامن من إصدارة الأمن في صندوق لمزيد من المعلومات.

٥.شبكات التواصل الاجتماعي:

- فكِّروا مليَّاً في المعلومات التي تعلنونها عن أنفسكم، و عن محل تواجدكم، و أصدقائكم، إلى آخره.
- احصلوا على موافقة الأشخاص المعنيين إذا كنتم ستنشرون معلومات أو وثائق أو صوراً تتعلق بآخرين.
- تأكدوا من أن تكون كلمات السر التي تخصكم آمنة، و قوموا بتغييرها بانتظام.
- كونوا حذرين عندما تتصلون بحسابكم في شبكة التواصل الاجتماعي من مكان عام – لا تستخدموها من موضع معين إلا إذا كنتم متأكدين من أنه محل ثقة. قوموا بمحو كلمة السر و تاريخ التصفُّح browsing history بعد الانتهاء من استخدام متصفح أو حاسوب عام.
- قوموا بقراءة و فهم أحكام اتفاقية انتهاء رخصة المستخدم End User License Agreement ، و/ أو وثائق إرشادات الخصوصية. يمكن أن تتغير هذه الوثائق في المستقبل، و لذا فإن من المهم أن يقوم المرء بالرجوع إليها بانتظام.
- تأكدوا من أن تكونوا على دراية بإعدادات الخصوصية لحسابكم في شبكة التواصل الاجتماعي. لا تعتمدوا على الإعدادات التلقائية default settings ، بل قوموا بتغييرها customise و مراجعتها بانتظام، لأن خدمة الشبكة قد تقوم بتغييرات.
- كونوا متنبهين عند تحميل التطبيقات التي تقترحها خدمات التواصل الاجتماعي. استخدموا هذه التطبيقات فقط إذا كنتم تثقون بمصدرها، و كونوا على دراية بالمعلومات التي ستكشفها، و تأكدوا من قدرتكم على التحكم في تداول معلوماتكم.

يمكنكم الاطلاع على الفصل العاشر من إصدارة الأمن في صندوق لمزيد من المعلومات.

٦.أمن الهواتف النقَّالة:

- إنَّ أنظمة الهواتف النقالة و التكنولوجيا المتعلقة بها في الوقت الحاضر (بما في ذلك الرسائل النصية القصيرة و المكالمات الصوتية) غيرُ آمنة – يمكن تتبُّع مكان تواجدكم، و التدخل في اتصالاتكم، و لهذا فإن عليكم أن تفكروا دوماً في أسلم الطرق لتناقل المعلومات الهامة.
- إنَّ أكثر الاتصالات أمناً تتم من الهواتف غير المسجَّلة التي تستخدم طريقة شحن الرصيد بقدر الحاجة، و التي يتم التخلص منها بعد استخدامها.

- قوموا بتفعيل كلمة السر أو الرمز السري للقفل pin lock على هاتفكم النقال.
- لا تخزنوا معلومات حساسة على هاتفكم، أو قوموا بترميزها إذا كنتم مضطرين إلى ذلك.
- كونوا متنبهين باستمرار إلى المحيط الذي فيه تستخدمون هاتفكم النقال، و امتنعوا عن استخدامه في الأماكن أو المواقف التي من شأنها أن تعرضكم إلى الخطر.
- تأكدوا من مسح جميع المعلومات التي تخصكم عن الهاتف قبل بيعه أو إرساله للصيانة.
- قوموا بتدمير الهواتف التي لا يمكن استخدامها و بطاقات SIM القديمة قبل التخلص منها.
- عندما تعملون مع أفراد و منظمات و يتضمن ذلك تناقل معلومات حساسة، انظروا في تخصيص هاتفين و بطاقَتَي SIM مختلفتين للعمل و للأغراض الشخصية.

يمكنكم الاطلاع على الفصل التاسع من إصدارة الأمن في صندوق لمزيد من المعلومات.