Funded by the European Union

CROWN AGENTS
ACCELERATING SELF-SUFFICIENCY & PROSPERITY

OMSAR

كتيب التوعية بأمن المعلومات

(متاح للجمهور العام)

النسخة ٧٠,٤ تشرين الأول ٢٠١٩

أعده

هادي حصن الحائز على شهادة ماستر في أمن المعلومات، وعلى شهادات CISSP، وCISM، وISO27001 LA / L .

كبير مستشاري أمن المعلومات

ضبط النسخ

النّسخة	التّاريخ	تعليقات
V0.1	*10/10/19*	*مسودّة أوّليّة للمناقشة أثناء ورشة العمل.*
V0.2	*16/10/19*	*تمّ تحديثها بعد مراجعة تامّة من قبل فريق قوى الأمن الدّاخلي.*
V0.3	*24/10/19*	*تمّ تحديثها بعد مراجعة تامّة من قبل فريق قوى الأمن الدّاخلي.*
V0.4	*25/11/19*	*تمّ تحديثها بناءً على تعليقات لجنة فريق الاستجابة لطوارئ الكمبيوتر التّابعة لقوى الأمن الدّاخلي.*

الموافقة على الوثائق

الاسم	المنظّمة/ المنصب	التّاريخ
بيتر سلّوم	Crown Agents	
المقدّم خالد يوسف	المديريّة العامّة لقوى الأمن الدّاخلي(ID)	
المقدّم نادر عبد الله	المديريّة العامّة لقوى الأمن الدّاخلي (IT)	
بيندي داغر	وفد الاتّحاد الأوروبي	

١. الخلفيّة

١,١. المقدّمة

وفّر الإنترنت فرصًا جديدة لنا جميعًا، فقد سمح لنا بالاختلاط والتّواصل مع بعضنا والقيام بالأبحاث والعمل. لكنّ معظم المواطنين اللّبنانيّين لا يعون مخاطر الإنترنت الّتي قد يتعرّضون إليها مع عائلاتهم، فكلّ جزء من مجتمعنا مستهدف على الإنترنت على جميع المستويات.

من هنا، أصبح الأمن السّيبراني مشكلة الجميع، فبات يؤثّر على حياتنا، وعائلاتنا، وأصدقائنا، وبات كلّ مواطنٍ لبنانيّ يتشارك مخاطر الأمن السّيبراني مع المجتمع كلّه، وبات المواطنون يتشاركون مع الحكومة مسؤوليّة حماية الوطن من التّهديدات السّيبرانية.

بصفتكم مواطنين، يمكنكم اتّباع المبادئ التّوجيهيّة البسيطة التّالية لحماية حساباتكم ومعلوماتكم الشّخصيّة على الإنترنت. وقوى الأمن الدّاخلي متاحة لكم لتساعدكم على حماية أنفسكم على الإنترنت، فنحن دائمًا متوفّرون وجاهزون لدعمكم بكفاءة وسرّيّة لا سيّما على مستوى التّحقيق بالجرائم والحوادث السّيبرانية.

١,٢. الهدف

يتمحور هدف كتيّب أمن المعلومات هذا حول حشد الوعي بشأن تهديدات الأمن السّيبراني الأخيرة والخطوات والتّدابير المضادّة الّتي يمكنكم اتّخاذها لحماية أنفسكم وعائلاتكم على الإنترنت.

ومن أجل تحقيق ذلك، نقدّم لكم هذا الكتيّب الّذي يفصّل الخطوات البسيطة الّتي يمكنكم اتّباعها كمواطنين لبنانيّين لحماية أنفسكم، وعائلاتكم، وأجهزتكم، وأموالكم من تهديدات الأمن السّيبراني والأنشطة الخبيثة.

٢. كلّنا مستهدفون

لعلّنا لا نعي ذلك دائمًا لكنّنا جميعًا أهداف للمجرمين السّيبرانيّين، فكمبيوتراتنا، وهواتفنا النّقّالة، وحساباتنا على وسائل التّواصل الاجتماعي

في القسم التّالي، سنقدّم لكم بعض الأمثلة عن التّهديدات السّيبرانيّة على الإنترنت.

٢,١ الاستلاب والابتزاز

يحدث الاستلاب أو الابتزاز عندما يهدّد المجرم السّيبراني بكشف معلومات شخصيّة أو محرجة عن الضّحيّة أو أفراد عائلتها، أو كشف معلوماتٍ قد تضرّهم اجتماعيًّا أو تدينهم إذا لم يحصل على أموال أو ممتلكات أو خدمات.

وباستخدام الهندسة الاجتماعيّة، يمكن للمجرمين السّيبرانيّين أن يسجّلوا فيديوهات، أو يحصلوا على صورٍ شخصيّة أو حتّى إباحيّة يمكن أن يتمّ استخدامها لابتزاز الضّحيّة.

ومن الأمثلة عن الاستلاب والابتزاز نذكر:

- أخذ صوركم على كاميرة الكمبيوتر والمطالبة بمبلغ من المال مقابل التّخلّص منها أو عدم نشرها.
- حمل الضّحيّة على التّصديق بأنّ المجرمين يملكون صورًا أو فيديوهات حتّى وإن كان ذلك غير صحيحًا.
- تشفير كلّ البيانات على كمبيوتركم الشّخصيّ والمطالبة بمبلغ (فدية) لفكّ تشفيره (برنامج فدية).
- تتبّع المواقع الّتي تزورونها والتّهديد بنشرها.

٢,٢ سرقة الهويّة- ويتضمّن ذلك خطف، وتزوير، وانتحال الهويّات

يمكن تعريف سرقة الهويّة بأنّها استخدام المعلومات الشّخصيّة لشخصٍ آخر مثل جواز السّفر، أو وثيقة الهويّة، أو رخصة القيادة، او الحسابات على الإنترنت من أجل بيع المعلومات، أو الحصول على الأموال أو الأرصدة، أو الإساءة إلى سمعتكم.

وقد تتضمّن الأمثلة الأخرى والأعمق عن سرقة الهويّة سرقة حسابات التّواصل الاجتماعي من أجل انتحال شخصيّة الضّحيّة ومضايقة أصدقائها، أو الإساءة إلى سمعتها من خلال الإهانات، أو التّنمّر على أشخاص آخرين على مواقع التّواصل الاجتماعي.

أمّا أنواع هويّات الإنترنت الّتي يمكن أن تثير اهتمام المجرمين السّيبرانيّين فهي:

- حسابات الفيسبوك، والتويتر، والإنستغرام، والسنابشات، واللنكد إن.
- حسابات البريد الإلكتروني والرّسائل الفوريّة.
- حساب الألعاب على الإنترنت.
- الحسابات الماليّة– مثل حسابات المصارف وبطاقات الائتمان

٢,٣ خرق البيانات

ويتمثّل بنشر المعلومات الخاصّة بطريقة معتمّدة أو غير معتمّدة إلى طرفٍ غير موثوق به. وفي حالة خرق البيانات، يمكن نسخ المعلومات الشّخصيّة، أو نقلها، أو رؤيتها، أو سرقتها، أو استخدامها لأسباب غير مأذونة من قبل المجرمين السّيبرانيّين.

٢,٤ التّجسّس السّيبراني

يمكن تعريف التّجسّس السّيبراني بأنّه الاستحواذ على معلومات شخصيّة/ تنظيميّة من من دون معرفة حامل هذه المعلومات وإذنه من خلال تعريض الكمبيوتر الشّخصيّ أو الشّبكة كلّها للخطر.

٢,٥ تزوير بطاقة الائتمان

يتمّ تزوير بطاقة الائتمان عندما يقوم شخص – محتال أو سارق – باستخدام بطاقة ائتمان مسروقة أو معلومات من البطاقة للقيام بعمليّات شراء غير مأذون بها باسمكم أو لسحب سلف نقديّة باستخدام حسابكم.

٢,٦ تهديد بريد العمل الإلكتروني (BEC)

يستخدم السّارق التّصيّد الاحتيالي (Phishing) أو وسائل أخرى للوصول إلى بريد المسؤول الالكتروني أو انتحال شخصيّته (باستخ
كيفيّة العمل في المنظّمة أو الشّركة على مستوى الإجراءات المتعلّقة بالحوالات المصرفيّة، وتحرّكات الأموال، والعلاقات مع البائعين.

وبمجرّد أن يصبح اللّصوص محيطين بممارسات المنظّمة الرّوتينيّة، سيقومون باستخدام حساب البريد الإلكتروني المهدّد لتقديم طلب نقل أموال، وسيقوم المحتالون بمتابعة حساب البريد الإلكتروني باستمرار ليعيدوا توجيه الرّسائل الّتي تشكّك بأمر الحوالة المصرفيّة. وأثناء كلّ ذلك، لا يكون المسؤول على دارية بالطّلب ولا بأيّ رسائل من الموظّفين بهذا الشّأن.

٣. احموا أنفسكم وعائلتكم

ستسمح لكم المبادئ التّوجيهيّة والنّصائح التّالية بالحفاظ على سلامتكم وسلامة عائلتكم على الإنترنت. لا تقلقوا، فإنّ تطبيقها أسهل بكثير ممّا تتخيّلون.

٣,١ أمّنوا حساباتكم على الإنترنت من خلال استخدام كلمات مرور قويّة

- استخدموا عبارات مرور قويّة يصعب تنبّؤها، واستخدموا مجموعةً من الأحرف العلويّة والسّفليّة، والأرقام، والرّموز للدّخول إلى حساباتكم على الإنترنت.
- تجنّبوا استخدام عبارات مرور تحتوي على معلومات شخصيّة مثل الأسماء، أو أرقام الهواتف، أو تواريخ الميلاد.
- تجنّبوا الكلمات الّتي يمكن تخمينها بسهولة في عبارات المرور مثل "كلمة المرور" (password) أو "مستخدم" (user).
- تجنّبوا استخدام المفاتيح المتتالية على لوحة المفاتيح في عبارات المرور: مثل "qwerty" و"asdzxc" و"١٢٣٤٥٦".
- استخدموا كلمات مرور مختلفة لحساباتكم على الإنترنت مثل حسابات البريد الإلكتروني، ووسائل التّواصل الاجتماعيّة، والألعاب، والصّيرفة، وغيرها.
- فكّروا في استخدام أنماط تتذكّرونها أو برنامج يساعدكم على إدارة عبارات المرور كلّها.
- انتبهوا إلى المكان الّذي تحتفظون فيه بلائحة كلمات المرور فبعضها قد يكون مهدّدًا مثل الهاتف المحمول، أو الكمبيوتر، أو ورقة صغيرة.
- توخّوا الحذر عند مشاركة كلمات المرور مع أيّ أحد، بل من الأفضل ألّا تعلموا أيّ شخص بكلمات المرور الّتي تستخدمونها.
- قوموا مباشرةً بتغيير كلمة المرور بمجرّد أن تشكّوا أنّ حسابكم تعرّض للخرق.

٣,٢ أمن مواقع التّواصل الاجتماعي (مثل الفيسبوك، والإنستاغرام، والتويتر، والسنابشات، وغيرها) وخصوصيّتها

- راجعوا القسم ٣,١ للنّظر إلى أفضل الممارسات الّتي يمكنكم اتّباعها عند اختياركم كلمات مرور قويّة.
- لا تقدّموا أيّ معلومات إضافيّة عند فتحكم حسابًا على موقع من مواقع التّواصل الاجتماعي.
- راجعوا إعدادات الأمن على حسابات مواقع التّواصل الاجتماعي واختاروا الإعدادات الّتي تعزّز أمنها مثل عمليّة التّوثيق القائمة على عاملين (two-factor authorization)، والحدّ من الوصول إلى حسابكم، وتلقّي الإخطارات عند أيّ دخول جديد، واختيار أصدقاء تثقون بهم للتّواصل معهم، إلخ.

- توخّوا الحذر من المعلومات الّتي تشاركونها على حسابات التّواصل الاجتماعي. وتذكّروا أنّكم تصبحون عاجزين عن التّحكّم بها بمجرّد أن تشاركوها.
- احرصوا على عدم تشارك معلومات شخصيّة مفصّلة عنكم وعن عائلتكم على مواقع التّواصل الاجتماعي.
- تجنّبوا المشاركة في نشاطات الإنترنت المؤذية كالابتزاز، والتّخويف، والاستلاب.
- لا تتواصلوا على الإنترنت إلّا مع أفرادٍ تثقون بهم. وتوخّوا الحذر من المجرمين والمتنمّرين السّيبرانيّين الّذين يرسلون إليكم طلبات الصّداقة.
- تذكّروا أنّ الأشخاص على الإنترنت ليسوا دائمًا من يدّعونه، فالبعض يغيّر هويّته وعمره أو يختار عدم الإفصاح عنها على مواقع التّواصل الاجتماعي.
- تجنّبوا استخدام كلمات مرور مواقع التّواصل الاجتماعي على أيّ مكان آخر على الإنترنت، ولا تعلموا أيّ أحدٍ بها.
- تجنّبوا مشاركة معلومات الدّخول إلى حساباتكم على مواقع التّواصل الاجتماعي مع أيّ أحد.
- أغلقوا حساباتكم على مواقع التّواصل الاجتماعي إن كنتم لا تستخدمونها.

٣,٣ أمن البريد الإلكتروني (Gmail، Hotmail، Yahoo، إلخ)

- راجعوا القسم ٣,١ للنّظر إلى أفضل الممارسات الّتي يمكنكم اتّباعها عند اختياركم كلمات مرور قويّة.
- راجعوا إعدادات الأمن على حسابات بريدكم الإلكتروني واختاروا الإعدادات الّتي تعزّز أمنها مثل عمليّة التّوثيق القائمة على عاملين (two-factor authorization)، وإبطال خاصيّة إعادة توجيه الرّسائل، وتمكين الحماية من الرّسائل المتطفّلة، واستخدام فلتر الرّسائل، إلخ.
- لا تعطوا بريدكم الإلكتروني إلّا إلى الشّركات والأشخاص الّذين تثقون بهم.
- يفضّل أن تستخدموا عدّة حسابات بريد إلكتروني إذا كان الأمر معقولًا، فيمكن استخدام الحساب الثّاني لاستعادة الحساب الأوّل في حال تعرّض للخرق أو السّرقة.
- تجنّبوا استخدام بريدكم الإلكتروني للالتحاق بالمسابقات أو الألعاب أو غيرها إذا كنتم لا تثقون بمصداقيّتها.
- انتبهوا من أن ينظر أحدٌ ما إلى شاشتكم عندما تفتحون بريدكم الإلكترونيّ أمام الآخرين أو في الأماكن العامّة.
- احذفوا الرّسائل الإلكترونيّة المتطفّلة مباشرةً ولا تجيبوا، فحتّى إذا جاوبتم على الرّسائل الإلكترونيّة لإلغاء اشتراككم، قد تتعرّضون لخطر الحصول على المزيد من الرّسائل المتطفّلة.
- احذروا الرّسائل الإلكترونيّة غير الموجّهة إلى اسمكم مباشرةً أو الّتي تحتوي على تحيّاتٍ عموميّة مثل عزيزي "المستخدم" أو "مستخدم البريد الإلكتروني" إذ إنّها أمثلة عن محاولات التّصيّد الاحتياليّ (phishing).

- احذروا الرّسائل الّتي تشعركم بالإلحاح أو بوجود حالة طوارئ قد تطالكم (مثل الرّسائل الّتي تدّعي أنّكم تخطّيتم حصّتكم من الرّسائل، أو أنّكم كنتم ضحيّة تصيّد احتيالي، أو أنّهم سيغلقون بريدكم الإلكترونيّ).
- احذروا قبول الرّسائل الإلكترونيّة من الحسابات الّتي لا تعرفونها أو فتح مرفقات الرّسائل، حتّى في الرّسائل الّتي تتلقّونها من الأصدقاء أو العائلة، فمن السّهل على المجرمين السّيبرانيّين تغيير تفاصيل بريدهم الإلكتروني.
- احذروا من مشاركة معلومات بطاقة الائتمان أو أيّ معلوماتٍ حسّاسة أخرى عن أنفسكم أو عائلتكم عبر البريد الإلكتروني.
- تحقّقوا من كلّ حسابات البريد الإلكتروني في حقل إلى: (أو :TO) قبل الرّدّ على الكلّ (Reply all).
- تجنّبوا الرّسائل المغرية الّتي تدّعي أنّكم ربحتم جوائز أو مبالغ من المال، فمن الممكن أن تكون رسائل تطفّليّة.
- احرصوا على الاحتفاظ بنسخ احتياطيّة لرسائلكم المهمّة عبر تحميلها على جهازكم أو إرسالها إلى حساب بريدكم الإلكتروني الثّاني.
- أغلقوا حساب بريدكم الإلكتروني إذا كنتم لا تستخدمونه.

٣,٤ أمن برامج الرّسائل الفوريّة (WhatsApp، iMessage، Skype، Signal، Telegram، إلخ)

- راجعوا إعدادات الأمن والخصوصيّة على حسابات الرّسائل الفوريّة واختاروا الإعدادات الّتي تعزّز أمنها، مثل عمليّة التّوثيق القائمة على عاملين (two–factor authorization)، وتشفير الرّسائل، والتّخزين على السّحابة (Cloud)، وإظهار إخطارات الأمن، وغيرها.
- احذروا المرفقات أو الرّوابط أو الرّسائل الاحتياليّة في تطبيقات الرّسائل الفوريّة، فيمكن أن تكون برامج خبيثة أو محاولة لسرقة المعلومات.
- بلّغوا عن محاولات التّطفّل بمجرّد أن تتلقّوها إلى بائع تطبيق الرّسائل الفوريّة الّذي تستخدمونه.
- جمّدوا (block) حسابات المستخدمين لتمنعوهم من التّواصل معكم مباشرةً.
- اتركوا مجموعات الرّسائل الفوريّة إذا كنتم تجدون المحتوى مهينًا لكم أو إذا كنتم تتلقّون التهديدات.
- ألغوا حساب الرّسائل الفوريّة من هاتفكم المحمول قبل التّبرّع به، أو بيعه، أو إعادة تدويره.

٣,٥ أمن العائلة على الإنترنت

- من المهمّ التّحدّث والتّواصل باستمرار عن تهديدات الإنترنت مع عائلتكم، لا سيّما عن التّنمّر السّيبراني على مواقع التّواصل الاجتماعي وبرامج الرّسائل الفوريّة.
- ناقشوا أنواع المواقع الّتي يمكن أن يزورها أطفالكم والّتي تلائم أعمارهم.
- يفضّل وضع كمبيوتر المنزل في منطقة مفتوحة من المنزل.
- شجّعوا أطفالكم على عدم التّواصل والاختلاط مع الغرباء على الإنترنت.

- شجّعوا أطفالكم على اختيار ألقاب عندما يلعبون على الإنترنت وعلى ألّا يفصحوا عن أيّ معلوماتٍ عن هويّتهم إذا كانوا يتحدّثون مع الغرباء في اللّعبة.
- شجّعوا أطفالكم على التّفكير قبل تحميل صورهم على الإنترنت لأنّ أيًّا كان يمكن أن يأخذها ويتشاركها ويغيّرها.
- شجّعوا أطفالكم على عدم مشاركة معلومات أو فيديوهات أو صور قد تضرّ بسمعتهم أو تعرّضهم للملاحقة القانونيّة.
- شجّعوا أطفالكم على تفادي إرسال صورٍ خاصّة لأنّهم لا يعرفون أين سينتهي بها المطاف، حتّى وإن كانوا يعرفون الشّخص جيّدًا.
- شجّعوا أطفالكم على عدم الاستجابة للمنشورات السّلبيّة وتجميد (block) حساب أيّ شخص يرسل إليهم رسائل مسيئة على الإنترنت.
- شجّعوا أطفالكم على عدم تحميل نسخ غير قانونيّة عن البرامج، أو الأغاني، أو الأفلام.
- شجّعوا أطفالكم على عدم الضّغط على الإعلانات، أو المسابقات، أو الجوائز على الإنترنت.
- شجّعوا أطفالكم على عدم فتح رسائل إلكترونيّة من مرسلين مجهولين.
- شجّعوا أطفالكم على التّبليغ عن أيّ تهديدات أو شيء غريب يشعرهم بعدم الرّاحة وعلى مناقشة هذه الأمور معكم.
- شجّعوا أطفالكم على استخدام محرّكات البحث المخصّصة للأطفال (مثل Kiddle.co، و Kidrex.org).
- غيّروا إعدادات متصفّح الإنترنت الّذي تستخدمونه ومكّنوا خاصيّات منع ظهور الإعلانات (Ad blocking) وفلترة المواقع (web filtering).
- تفحّصوا صفحات أطفالكم على مواقع التّواصل الاجتماعي بانتظام واسألوا أنفسكم، "هل يمكن أن يستفيد أيّ غريب من هذه المعلومات؟"
- تأكّدوا من أنّ المواقع والألعاب الّتي يزورها أطفالكم ملائمة لأعمارهم.
- تفحّصوا صفحة السّجل (history) على متصفّح الإنترنت للتّأكّد من ماهية المواقع الّتي يزورها أطفالكم.
- ألغوا معلومات بطاقة الائتمان خاصّتكم من أجهزة أطفالكم للتّأكد من أنّهم لن يقوموا بأيّ عمليّات شراء في التّطبيقات من دون إذنكم.
- استخدموا برامج المراقبة الأبويّة (parental control) الّتي تسمح لكم (كأهل) بوضع بعض القيود على أنشطة أولادكم على الإنترنت وبمراقبتها.
- راجعوا الشّبكة الاجتماعيّة الّتي يريد أن يلتحق بها أطفالكم على الإنترنت قبل السّماح لهم بفتح حسابٍ جديدٍ عليها، فهذا سيسمح لكم بالتّأكّد من إذا ما كانت الخدمة معروفة ومن ماهية المعلومات الّتي سيقوم أطفالكم بمشاركتها ومن الطّريقة الّتي سيتواصلون فيها مع الآخرين.

٤. احموا أجهزتكم

ستساعدكم المبادئ التّوجيهيّة والنّصائح التّالية على المحافظة على سلامة أجهزتكم والتأمين على المعلومات الّتي تحتويها في جميع الأوقات.

٤,١ أمّنوا كمبيوتركم النّقّال وكمبيوتركم المكتبي

- راجعوا إعدادات الأمن على كمبيوتراتكم النّقّالة والمكتبيّة ومكّنوا الإعدادات الّتي تعزّز أمنها، مثل التّشفير، وجدار حماية التّطبيق (firewall)، وتحديثات البرمجيّات التّلقائيّة– مثل التّطبيقات، والبرامج، ومتصفّحي الإنترنت، وأنظمة التّشغيل، وحافظات الشّاشة الّتي تغلق الكمبيوتر تلقائيًّا (بعد فترة معقولة، أي حوالي عشر دقائق لا أكثر)، وغيرها.
- راجعوا القسم ٣,١ للنّظر إلى أفضل الممارسات الّتي يمكنكم اتّباعها عند اختياركم كلمات مرور قويّة للدّخول إلى كمبيوتركم المحمول أو المكتبيّ.
- حمّلوا برامج مكافحة الفيروسات (Antivirus) من مصدر موثوق.
- احرصوا على تغطية كاميرة الكمبيوتر دائمًا إذا كنتم لا تستخدمونها.
- أبطلوا سمات الأجهزة والاتّصال الاجتماعي (مثل مكبّر الصّوت، والبلوتوث– Bluetooth، والاتّصال قريب المدى– NFC، والواي–فاي– WiFi) إذا كنتم لا تستخدمونها.
- احرصوا على إغلاق أجهزتكم إذا كنتم بعيدين عنها.
- حمّلوا التّطبيقات الّتي تحتاجونها من مصادر موثوقة فقط مثل متجر ويندوز (Windows Store)، ومتجر ماك أبل (Mac Apple Store).
- أغفلوا التّحذيرات والإخطارات المنبثقة (Pop–ups) الّتي تطلب منكم تحميل برامج تدّعي أنّها تنظّف كمبيوتركم الشّخصيّ.
- احذروا عروضات تحميل الموسيقى، والألعاب والتّطبيقات المجّانيّة، فمن المعروف أنّها وسائل لتوزيع البرامج الخبيثة.
- تأكّدوا من الأذونات الّتي تطلبها التّطبيقات قبل تحميلها.
- أزيلوا التّطبيقات والبرامج الّتي لا تستخدمونها.
- تفادوا العمل على الوثائق والمعلومات الحسّاسة في الأماكن المزدحمة الّتي لا تحمي خصوصيّتكم (مثل الطّائرات، والقطارات، والمقاهي، وصالات المطارات).
- مكّنوا حماية كلمات المرور أو تشفيرها على الأقراص الخارجيّة (مثل أجهزة الذّاكرة الومضيّة– USB).
- احذروا من أخذ أجهزة ذاكرة ومضيّة مجهولة أو استخدامها لأنّها قد تحتوي على برامج خبيثة.
- إذا كنتم مضطرّين إلى استخدام كمبيوتركم في الأماكن العامّة (أي في مقاهي الإنترنت، أو المكتبات، أو مراكز العمل في الفنادق)، احرصوا على الخروج من كلّ حساباتكم، وإلغاء سجلّ متصفّح الإنترنت (history) وملفّات تعريف الارتباط (cookies)، وإقفال الكمبيوتر.

- احتفظوا بنسخ احتياطيّة عن بياناتكم (على السّحابة– cloud، والأقراص الخارجيّة– external disk، إلخ) من أجل التّخفيف من تأثير تعدّيات برامج الفدية أو الكمبيوترات المحمولة المسروقة.
- ألغوا البيانات الحسّاسة من كمبيوتراتكم المحمولة أو المكتبيّة قبل التّبرّع بها، أو إعادة بيعها أو تدويرها.

٤,٢ تأمين هوافتكم الذّكيّة ولوحاتكم

- راجعوا إعدادات الأمن على هاتفكم الذّكيّ ولوحتكم ومكّنوا الإعدادات الأكثر أمنًا مثل عبارات المرور القويّة، والمصادقة عبر الأنماط أو المقاييس الحيويّة، وخاصيّة العثور على الهاتف (Find my Phone)، والتّحديثات التّلقائيّة لكلّ البرامج– مثل التّطبيقات، وأنظمة التّشغيل، وشاشات الإغلاق التّلقائيّة (بعد فترة معقولة، أي حوالي عشر دقائق لا أكثر)، وغيرها.
- تفادوا التّلاعب بإعدادت المصنع (مثل كسر الحماية– jailbreaking، وتغيير الصّلاحيّات– rooting).
- أبطلوا سمات الاتّصال الاجتماعي (مثل البلوتوث– bluetooth، والاتّصال قريب المدى– NFC، والواي–فاي– WiFi) إذا كنتم لا تستخدمونها.
- تأكّدوا من الأذونات الّتي تطلبها التّطبيقات (مثل مشغّل الموسيقى والفيديوهات، والرّسائل الفوريّة، والطّقس) قبل تحميلها، وتوخّوا الحذر من التّطبيقات الّتي تطلب الوصول إلى الكاميرة، ومكبّر الصّوت، والموقع، وقائمة الاتّصالات، وحقوق المسؤول، إلخ).
- حمّلوا التّطبيقات الّتي تحتاجونها من مصادر موثوقة فقط، مثل متجر تطبيقات آبل (Apple App Store)، أو متجر غوغل بلاي (Google Play Store).
- قبل تحميل أيّ تطبيق، اقرأوا مراجعات المستخدمين حول أداء التّطبيق وعمله.
- حمّلوا تطبيقات مكافحة الفيروسات (Antivirus) على هاتفكم الذّكيّ.
- ألغوا التّطبيقات والبرامج الّتي لا تستخدمونها.
- تفادوا حفظ كلمات المرور أو المحتويات الحسّاسة على هاتفكم.
- احتفظوا بنسخ احتياطيّة عن البيانات المهمّة بانتظام (مثل قائمات الاتّصالات، والمذكّرات، ومحادثات الرّسائل الفوريّة).
- لا تسمحوا لجهازكم إلّا بتذكّر الشّبكات اللّاسلكيّة الّتي تثقون بها (مثل شبكة المنزل أو المكتب).
- أبقوا نظركم على جهازكم في الأماكن العامّة ولا تتركوه بعيدًا عن متناولكم حتّى لفترةٍ قصيرة من الزّمن.
- أعيدوا تعيين إعدادات المصنع (factory reset) على هاتفكم الذّكيّ قبل التّبرّع به، أو إعادة بيعه أو تدويره.

٤,٣ تأمين واي–فاي المنزل والمكتب والأجهزة الموصولة على الإنترنت

- راجعوا إعدادات أمن جهاز الواي–فاي ومكّنوا الإعدادات الأكثر أمنًا مثل تغيير اسم الواي–فاي المعطى، وتغيير اسم المستخدم وكلمة المرور، وتنزيل التّحديثات التّلقائيّة على برنامج الرّواتر الثّابت (router firmware)، إلخ.
- راجعوا القسم ٣,١ للنّظر إلى أفضل الممارسات الّتي يمكنكم اتّباعها عند اختياركم كلمات مرور قويّة لشبكتكم اللّاسلكيّة.

- غيّروا عبارة مرور الواي–فاي بانتظام.
- مكّنوا خاصيّة تشفير الشّبكة على جهازكم اللّاسلكيّ. ونذكّركم هنا بالأنواع العديدة المتاحة للتّشفير وأحدثها وأكثرها فعاليّةً هو نوع "WPA3".
- مكّنوا عمليّة التّوثيق القائمة على عاملين (two–factor authorization) على أيّ جهازٍ يتّصل بالإنترنت (IOT device) إذا كان الأمر ممكنًا (مثل منظّم الحرارة، وجرس الباب بخاصيّة الفيديو، والكاميرات).

٤,٤ التّصفّح الآمن على الإنترنت

- توخّوا الحذر عند استخدام الواي–فاي في الأماكن العامّة، فمن الأسهل تعريض جهازكم للمخترقين في الأماكن العامّة (أي في المقاهي، أو المطاعم، أو الفنادق مثلًا).
- توخّوا الحذر عند الضّغط على روابط المواقع، أو النّوافذ المنبثقة، أو إعلانات الإنترنت لأنّها قد تحتوي على برامج خبيثة.
- توخّوا الحذر عندما يطلب منكم إدخال معلومات الدّخول إلى الحسابات على المواقع المجهولة.
- حاولوا تصفّح المواقع الآمنة فقط (ابحثوا عن رمز القفل 🔒، أو عن https في عبارة محدّد الموقع– URL).
- حمّلوا إضافة منع ظهور الإعلانات (ad blocking) على متصفّح الإنترنت.
- استخدموا خاصيّة الخصوصيّة على متصفّحي الإنترنت على الكمبيوترات في الأماكن العامّة أو الكمبيوترات الّتي تتشاركونها مع الآخرين (من خلال تمكين نافذة التّصفّح المتخفّي– Incognito mode على متصفّح كروم– Chrome أو إن برايفت– InPrivate على متصفّح إنترنت إكسبلورر– Internet Explorer) للحرص على ألّا يتتبّعكم المتصفّح. كما ستمكّنكم هذه الخاصيّة من إخفاء نشاطكم على الإنترنت عن الأشخاص الآخرين الّذين يستخدمون الجهاز نفسه.
- أزيلوا ملفّات تعريف الإرتباط (cookies) وسجلّ التّصفّح (history) بانتظام عن المتصفّح الّذي تستخدمونه.
- لا تعطوا أكثر من المعلومات المطلوبة على استمارة المتصفّح (التّسجيل، أو الحجز، أو الشّحن، إلخ).
- استخدموا شبكة خاصّة افتراضيّة موثوقة (VPN) إذا وجدتم أنفسكم بحاجة إلى تعزيز أمنكم على الإنترنت، لا سيّما أنّ هذا النّوع من الشّبكات يوفّر اتّصالًا آمنًا بين جهازكم وخادم إنترنت لا يسمح لأحد بمراقبته أو بالوصول إلى البيانات الّتي تتبادلونها عليه.

٥. احموا أموالكم

ستساعدكم المبادئ التّوجيهيّة والنّصائح التّالية على الحفاظ على سلامة أموالكم وبطاقات الائتمان وأنتم تستخدمون الإنترنت.

٥,١ تأمين الصّيرفة على الإنترنت

- تواصلوا مع فريق الاحتيال في مصرفكم إذا كنتم تشكّون أنّكم وقعتم ضحيّةً للاحتيال أو حتّى لمحاولة احتيالٍ.
- لا تقوموا بأيّ حوالاتٍ مصرفيّة إلّا على أجهزةٍ موثوقة، وتفادوا القيام بها على شبكة واي–فاي عامّة، أو على مواقع لا يظهر عليها رمز القفل أو Secure https
- لا تفصحوا عن تفاصيل حسابكم المصرفيّ وبطاقة الائتمان إلّا لأشخاصٍ تثقون بهم (مثل ممثّلي المصرف، والفنادق، ومتاجر الإنترنت، والمطاعم، إلخ).
- احذروا طبيعة المعلومات الّتي تفصحون عنها لأيّ متّصل يسأل عن تفاصيلكم المصرفيّة ومدفوعاتكم. وتذكّروا أنّ ممثّل المصرف لن يطلب منكم رقم التّعريف الشّخصيّ (PIN) أو كلمة المرور على الهاتف.
- احرصوا على ألّا تفصحوا عن أيّ تفاصيل مصرفيّة أو معلومات ماليّة لأيّ أحدٍ يتّصل بكم من دون علمكم ويعلمكم بوجوب استرداد مبلغٍ ما.
- راجعوا حسابكم المصرفيّ بانتظام لتأكيد الحوالات والتّبليغ عن أيّ حوالات أو دفعات مشبوهة لم تقوموا بها بأنفسكم إلى مصرفكم.
- تأكّدوا مرّتين على الأقلّ من أيّ طلبات لدفعات جديدة أو لتغيير تفاصيل حسابكم مع شخصٍ موثوقٍ به في المصرف.
- فكّروا بطلب تأكيدات إضافيّة (مثل إعادة الاتّصال بصاحب الطّلب) لأيّ دفعات تتخطّى سقفًا محدّدًا تحدّدونه بأنفسكم.
- تفادوا الإفصاح عن كلمة المرور لمرة واحدة (OTP) الّتي يعطيكم إيّاها المصرف لأيّ شخص، حتّى لموظّف المصرف.
- تفادوا إدخال تفاصيل حسابكم المصرفيّ بعد الضّغط على رابطٍ في رسالة إلكترونيّة أو نصّيّة.
- تحقّقوا بانتظام من رصيد حسابكم المصرفيّ وبلّغوا مصرفكم عن أيّ دفعات غير مألوفة، وتذكّروا أنّ السّارقين قد يقومون بحوالاتٍ صغيرة على فترة طويلة ليتفادوا رفع الشّبهات.

٥,٢ تأمين التّسوّق على الإنترنت

- راجعوا القسم ٣,١ للنّظر إلى أفضل الممارسات الّتي يمكنكم اتّباعها عند اختياركم كلمات مرور قويّة لحسابات التّسوّق على الإنترنت.

- لا تتسوّقوا على الإنترنت إلّا من المواقع المعروفة ذات السّمعة الحسنة، وتأكّدوا من أنّ هذه المواقع تؤمّن اتّصالًا آمنًا ومشفّرًا– مثل SecureTPS
- احذروا روابط التّسوّق على الإنترنت الغريبة الّتي تعدكم بعروضات غير معقولة مثل "prada–at–awesome–price.com " و"the–bestonlineshopping.com " لأنّها قد تُستخدم للتّصيّد الاحتيالي (Phishing).
- احذروا مواقع التّسوّق الّتي تعرض مجموعة غريبة من الماركات، مثل المواقع الّتي تتخصّص ببيع الملابس لكنّها تبيع أيضًا قطع السّيّارات أو مواد البناء.
- احذروا المعلومات الغريبة لخدمات الزّبائن على متاجر الإنترنت، مثل "ebaysupport@gmail.com" بدلًا من support@ebay.com .
- احذروا متاجر الإنترنت الّتي تسوّق منتوجات بأسعار منخفضة جدًّا، مثل تلك الّتي تبيع هاتف iPhone 11 بسعر ١٥٠ دولار.
- تفادوا القيام بحوالاتٍ نقديّة للتّسوّق على الإنترنت من روابط البريد الإلكتروني، مثل رسالة تصيّد احتيالي تعرض عليكم فرصةً وهميّة لشراء منتج مرغوب به مع زرّ لشرائه مباشرةً بدلًا من أخذكم إلى موقع يسمح لكم برؤية العرض.
- تفادوا التّسوّق على الإنترنت على أجهزة مقاهي الإنترنت أو على الأجهزة المتّصلة بالواي–فاي في مكان عامّ.
- عند قيامكم بعمليّة شراء على الإنترنت، احذروا من نوع المعلومات الّتي تُطلب منكم لإكمال عمليّة التّحويل، ولا تعطوا سوى المعلومات الأساسيّة لإكمالها.
- عند قيامكم بعمليّة شراء على الإنترنت، اقرأوا مراجعات الزّبائن الآخرين اتتأكّدوا إذا كانت تجربتهم إيجابيّة أو سلبيّة على الموقع.
- استخدمو اختيارات الدّفع الآمنة، وتذكّروا أنّ بطاقات الائتمان هي الأكثر أمنًا عادةً.
- استخدموا بطاقة ائتمان عليها رصيد محدود أو بطاقة ائتمان مدفوعة مسبقًا من أجل القيام بحوالاتكم الماليّة عند التّسوّق على الإنترنت.
- احذروا من حفظ معلومات بطاقة ائتمانكم على مواقع التّسوّق على الإنترنت.

٥,٣ احموا بريد العمل الإلكتروني من الخطر

- اقرأوا كلّ الرّسائل الإلكترونيّة بحذر، لا سيّما تلك الّتي تطلب الحوالات الماليّة أو الّتي تطلب منكم القيام بأمور غير مألوفة من مدراء الشّركات.
- ضعوا إجراءات صارمة لتحويل الأموال تكون مبنيّة على طلبات البريد الإلكتروني، مثل:
  - التّأكّد دائمًا من الفاتورة
  - التّحقّق مرّتين من معلومات الدّفع مع المتلقّي.
  - التّحقّق مرّتين من أيّ طلب لتحويل أموال مع المدير التّنفيذي، أو المحامي، أو شركة التّأمين، أو شركة العقارات.

- اقرأوا بحذر الرّسائل الّتي تطلب منكم أيّ شيء غير اعتياديّ، لا سيّما إذا كانت تعطيكم مهلة محدّدة وقصيرة من الوقت، ومن الأفضل أن تطرحوا الكثير من الأسئلة عن أيّ أمر تجدونه غير اعتياديًّا.
- تحقّقوا من حساب مرسل البريد الإلكترونيّ– فغالبًا ما يقوم المجرمون السّيبرانيّون بتغيير حرفٍ واحد في البريد الإلكترونيّ أو بإضافة رموزٍ عليه.
- تأكّدوا من طلبات تغيير تعليمات الدّفعات عبر التّواصل مع الطّرف الآخر على رقم الهاتف الّذي كنتم تستخدمونه وليس على رقم الهاتف الجديد في البريد الإلكتروني.
- اطلبوا من المرسل إرسال تعليمات الدّفع الجديدة مرفقةً بعلامات الشّركة الرّسميّة وتحقّقوا من صحّتها.
- تحقّقوا من أيّ تغييرات في معلومات الدّفع للبائع من خلال التّواصل مع شخصٍ آخر من موظّفي الشّركة.

٦. التّعامل مع المشاكل السّيبرانيّة الشّائعة

ستساعدكم المبادئ التّوجيهيّة والنّصائح التّالية على تخفيف أثر حوادث الأمن السّيبراني أو خرق البيانات. احرصوا على القيام بالخطوات التّالية مباشرةً لتفادي حدوث أيّ ضرر إضافيّ.

٦,١ الهواتف الذّكيّة المسروقة أو الضّائعة

إليكم الخطوات الّتي يمكنكم اتّباعها إذا لاحظتم أنّ جهازكم مسروق أو ضائع. قد تعتمد بعض هذه الخطوات على إعدادت الأمن الّتي مكّنتموها على هاتفكم الذّكيّ بناءً على التّوصيات الموجودة في كتيّب الاستعمال.

- حاولوا الاتّصال بهاتفكم أوّلًا فإذا كان قريبًا، ستسمعونه يرنّ أو يهتزّ.
- حاولوا استخدام تطبيق العثور على الهاتف (مثل تطبيقات Find My iPhone، أو Google Find My Device، أو Samsung Find My Mobile).
- تحقّقوا من موقع جهازكم على تطبيق العثور على الهاتف وشغّلوا المنبّه من التّطبيق إذا كان قريبًا منكم.
- إذا كان هاتفكم في مكانٍ لم تزوروه أو إذا كان يتحرّك، يمكنكم التّأكّد من أنه مع شخصٍ آخر. وإذا لم يستجب ذلك الشّخص لاتّصالاتكم، فإنّه على الأغلب مسروق.
- من المحبّذ ألّا تذهبوا إلى الموقع الّذي يظهره التّطبيق إذا لم تميّزوه حتّى إذا كان بإمكانكم تتبّعه. في هذه الحال، من المحبّذ أن تتّصلوا بالشّرطة (يمكنكم إلعثور على معلومات إضافيّة عن ذلك في الأسفل).
- بمجرّد أن تكتشفوا أنّ شخصًا آخر يملك هاتفكم، تصبح أولويّتكم التّأكّد من أنّه لا يستطيع الوصول إلى محتوى الهاتف. ومن أجل فعل ذلك، يمكنكم إقفال الهاتف عن بعد.
- بعد القيام بذلك، يمكنكم القيام بمسح كلّ بيانات جهازكم عن بعد عبر تطبيق العثور على الهاتف (Find My Device). ومن المحبّذ أن تكونوا قد نسختم بيانات الهاتف (back up) لتتأكّدوا من أنّكم لم تفقدوا أيّ معلوماتٍ مهمّة عند قيامكم بعمليّة المسح.
- إذا قام شخصٌ ما بسرقة هاتفكم واستطاع الدّخول إلى الجهاز، من الممكن أن يزيد مصاريف الاتّصال والرّسائل والإنترنت بشكلٍ ملحوظ.. من هنا، يفضّل أن تتّصلوا بخدمة زبائن مزوّد هاتفكم مباشرةً لتطلبوا إيقاف رقم هاتفكم أو تعليق خدمتكم.
- غيّروا كلمة مرور أيّ حسابات مربوطة بهاتفكم، ويفضّل أن تغيّروا كلمة مرور متجر التّطبيقات لكي لا يقوم السّارق بأيّ عمليّة شراء داخل التّطبيقات.

٦,٢ الابتزاز

إذا وصلتكم رسالة ابتزاز أو استلاب، من الأفضل ألّا تتولّوا معالجة الأمر بمفردكم. إليكم الخطوات الّتي ننصحكم باتّخاذها:

- خذوا صورة (screenshot) واحتفظوا بكلّ دليلٍ أو اتّصالات يمكن أن تكون مفيدة.
- اطلبوا المساعدة من صديقٍ موثوق أو فردٍ تثقون به من العائلة في عمليّة توثيق الأدلّة.
- أوقفوا أيّ تواصل مع المبتزّين أو المستلبين السّيبرانيّين.
- لا تدفعوا لهم أيّ جزء من الفدية ولا تحاولوا التّفاوض معهم.
- بلّغوا عن الابتزاز أو التّنمّر لموقع التّواصل الاجتماعي الّذي تحدث المشكلة عليه.
- عزّزوا إعدادات الأمان على حسابات التّواصل الاجتماعي الّتي تستخدمونها.
- تواصلوا مع الشّرطة (يمكنكم إلعثور على معلومات إضافيّة عن ذلك في الأسفل)

٦,٣ حسابات التّواصل الاجتماعي المخترقة

قد يكون من الصّعب عليكم أحيانًا أن تعرفوا إذا تعرّض حسابكم على التّواصل الاجتماعيّ للخطر، لا سيّما إذا كان المجرمون السّيبرانيّون يقومون بتغييرات صغيرة أو يرسلون رسالة واحدة بين الفينة والأخرى. إليكم بعض العلامات الّتي قد تثبت أنّ حسابكم قد تعرّض للخطر:

- أن تتلقّوا إعجابات (likes) أو متابعين (follows) مجهولين.
- أن يتلقّى أصدقائكم رسائل نصّيّة خاصّة (قد يكون من الصّعب عليكم معرفة ذلك إلّا إذا قاموا بإبلاغكم).
- أن تتلقّوا أيّ رسائل إلكترونيّة أو إخطارات من الشّبكة الاجتماعيّة، مثل التحذيرات الّتي تبلغكم أنّ بريدكم الإلكترونيّ تغيّر.
- أن تظهر على حسابكم تحديثات أو تويتات (tweets) لم تقوموا بها.
- أن يتمّ تغيير صوركم على صفحة التّواصل الاجتماعيّ.

إذا كنتم تظنّون أنّ حسابكم على التّواصل الاجتماعيّ قد تعرّض للخرق، يمكنكم اتّخاذ الخطوات التّالية لتحدّوا من أثر الخرق وتستعيدوا حسابكم:

- إذهبوا إلى صفحة الدّعم على موقع حساب التّواصل الاجتماعيّ (support) واضغطوا على "حساب معرّض للخطر" (Account Compromised) أو "حساب مخترق" (Account Hacked)، أو تواصلوا مع فريق الدّعم إذا لم تجدوا الرّابط إلى صفحة الموقع.
- غيّروا كلمة المرور على حساب التّواصل الاجتماعيّ.
- اختاروا عمليّة التّوثيق القائمة على عاملين (two-factor authorization).
- تواصلوا مع أصدقائكم أو متابعينكم على حسابكم وأعلموهم بأنّ حسابكم تعرّض للخرق، إذ قد تساعدونهم على تجنّب التّعرّض للخرق بدورهم.
- إذا قام شخصٌ ما بإنشاء حسابٍ باسمكم من دون علمكم، بلّغوا عن ذلك للموقع واطلبوا أن تتمّ إزالته.

٦,٤ البرامج الخبيثة على الجهاز (Malware)

قد تلاحظون أحيانًا أنّ جهازكم أصبح بطيئًا، أو أنّه صار يتوقّف فجأةً عن العمل، أو أنكم صرتم تتلقّون عشوائيًّا العديد من الإخطارات المنبثقة على متصفّح الإنترنت، أو أنّ بعض التّطبيقات غير المألوفة صارت تنطلق تلقائيًّا. كلّ هذه الأمور تدلّ على أنّ جهازكم تعرّض لبرنامج خبيث.

في هذه الحال، يمكنكم اتّخاذ بعض الخطوات لتنظيف جهازكم واسترجاع حالته الأساسيّة.

- احرصوا على الاحتفاظ بنسخ احتياطيّة (back up) عن كلّ وثائقكم وملفّاتكم قبل أن تبدأوا بإزالة البرنامج الخبيث. يمكنكم القيام بذلك عبر الاحتفاظ ببياناتكم الأساسيّة على قرصٍ خارجيّ (external drive)، أو على قرص DVD أو CD، أو على جهاز الذّاكرة الومضيّة (USB) أو على خدمة التّخزين على السّحابة (cloud).
- ضعوا حسابكم على الوضع الآمن (Safe Mode).
- احرصوا على تنظيف القرص (Disk Cleanup) وعلى إلغاء الملفّات مؤقّتًا للحرص على تسهيل عمليّة المسح وتبسيطها.
- امسحوا جهازكم باستخدام برنامج مكافحة الفيروسات (antivirus) وخذوا النّصائح الّتي يعطيكم إيّاها بالاعتبار.
- إذا لم يتمكّن برنامج مكافحة الفيروسات من إزالة البرنامج الخبيث، حاولوا استرجاع البيانات من نقطة استرجاع صالحة أو حاولوا إعادة إطلاق جهازكم (format).
- استرجعوا البيانات الّتي احتفظتم بها من تاريخ آخر نسخة جيّدة.

٦,٥ برامج الفدية (Ransomware)

إذا تعرّض جهازكم لخطر برنامج الفدية، من المحبّذ أن تتفادوا دفع أيّ فدية مقابل استرجاعه. فإذا قمتم بدفع فدية:

- لا شيء يضمن لكم أنّكم ستستطيعون الوصول من جديد إلى بياناتكم أو جهازكم.
- سيظلّ كمبيوتركم مؤثّرًا بخطر البرنامج إلّا إذا قمتم باتّباع الخطوات اللّازمة لتنظيفه.
- قد يفترض المعتدّون بأنّكم مستعدّون لدفع فدياتٍ إضافيّة في المستقبل.
- ستكونون دعمتم مجموعات إجراميّة ماديًّا.

يمكنكم اتّباع الخطوات التّالية لتنظيف جهازكم وإرجاعه إلى حالته الأساسيّة.

- اكتشفوا ما هو نوع برنامج الفدية على كمبيوتركم وتأكّدوا إذا أصبتم ببرنامج فدية مشفّر، أو ببرنامج يقفل الشّاشة أو ببرنامج يدّعي أنّه برنامج فدية فقط. وتحقّقوا من أنّكم ما زلتم قادرين على الوصول إلى ملفّاتكم على الشّاشة الرّئيسيّة (desktop) أو على صفحة الملفّات (My Documents).
- إذا لم تستطيعوا الخروج من رسالة الفدية على شاشتكم، يعني ذلك أنّ كمبيوتركم تعرّض لبرنامج فدية يقفل الشّاشة.
- إذا كنتم لا تزالون قادرين على تصفّح الأدلّة أو التّطبيقات لكنّكم لم تتمكّنوا من فتح ملفّات برنامج office العاديّة، أو الأفلام أو الصّور أو البريد الإلكترونيّ، يعني ذلك أنّ كمبيوتركم تعرّض لبرنامج فدية مشفّر.
- إذا كنتم قادرين على التّنقّل عبر النّظام وقراءة أغلبيّة ملفّاتكم، فيعني ذلك أنّكم ترون برنامجًا مزيّفًا تمّ تحميله لدفعكم إلى دفع الفدية، وبالتّالي يمكنكم تجاهل رسالة الفدية ومحاولة إغلاق متصفّح الإنترنت الّذي تستخدمونه.
- باعتبار أنّ برامج الفدية المشفّرة هي أكثر أنواع برامج الفدية شيوعًا وأكثرها أذيّةً، من المحبّذ معالجتها أوّلًا. يمكنكم إذًا اتّباع الخطوات التّالية بالتّرتيب حتّى وإن كنتم قد نسختم ملفّاتكم مؤخّرًا، ثمّ يمكنك إيقاف العمليّة بمجرّد أن تسترجعوا كلّ ملفّاتكم.
  - افصلوا جهازكم عن أيّ أجهزةٍ أخرى وعن أيّ أقراصٍ خارجيّة.
  - استخدموا هاتفًا ذكيًّا أو كاميرة لأخذ صور رسالة الفدية الّتي ظهرت على الشّاشة, ومن المحبّذ أن تعلموا الشّرطة بعد اتّخاذ كلّ هذه الخطوات.
  - استخدموا برامج مكافحة الفيروسات (antivirus) لإزالة برنامج الفدية عن جهازكم.
  - تفحّصوا إمكانيّة استرجاع ملفّاتكم الملغاة، إذ إنّ العديد من برامج الفدية المشفّرة تقوم بنسخ ملفّاتكم وتشفير النّسخ بعد محو الملفّات الأصليّة. من حسن حظّكم أنّكم ستكونون على الأغلب قادرين على استرجاع الملفّات الملغاة بسهولة بواسطة أدوات مثل برنامج ShadowExplorer المجّانيّ.
  - حاولوا معرفة نوع برنامج الفدية المشفّر الّذي أصاب هاتفكم. في حال لم يُظهر برنامج الفدية اسمه، يمكنكم محاولة استخدام أداتي Crypto Sheriff وID Ransomware اللّتان تسمحان لكم بتحميل ملفّات مشفّرة ثمّ تعلمانكم إذا كان بإمكانكم عكس التّشفير.
  - تأكّدوا إذا كانت أدوات فكّ التّشفير متوفّرة، وإذا كنتم تعرفون اسم برنامج الفدية، ابحثوا عن لائحة أدوات فك التشفير على موقع "nomoreransom.com" لتتأكّدوا من وجود أداة ملائمة لفكّ التّشفير.
  - إذا لم تنجحوا في فكّ تشفير ملفّاتكم، من الأفضل أن تعيدوا تعيين إعدادات المصنع (factory reset) على جهازكم، وتعيدوا تحميل نظام التّشغيل (operating system) قبل أن تستعيدوا الملفّات الّتي احتفظتم بنسخها.
  - قدّموا تقريرًا للشّرطة (يمكنكم العثور على معلومات إضافيّة عن ذلك في الأسفل). إذ إنّ السّلطات قادرة على مساعدتكم على تتبّع معدّلات الإصابة والانتشار.

٦,٦ بطاقة ائتمان مسروقة

إذا كنتم تشكّون أنّ أحدًا قام بسرقة بطاقة ائتمانكم أو استخدامها من دون إذنكم أو موافقتكم، يمكنكم اتّخاذ بعض الخطوات للتّخفيف من خسارتكم.

- تواصلوا مباشرةً مع الجهة المصدّرة لبطاقة الائتمان للتّبليغ عن فقدان بطاقتكم أو سرقتها.
- حضّروا المعلومات الّتي قد تحتاجون إليها مثل بطاقة الهويّة، واسمكم، وعنوانكم، وغيرها من المعلومات الشّخصيّة.
- قد تسألكم الجهة المصدّرة أسئلةً مثل: متى فقدتم بطاقتكم؟ أو متى تمّت سرقتها؟ ومتى قمتم باستخدامها آخر مرّة؟ كما قد تراجع آخر الحوالات للتّأكّد من إذا ما كانت تبدو احتياليّة أم لا.
- ستقوم الجهة المصدّرة بإلغاء حسابكم وسترسل إليكم بطاقةً جديدة عليها رقم بطاقة ائتمان جديد.
- احرصوا على تحديث محفظتكم الإلكترونيّة على هاتفكم (mobile wallet) إذا كانت تتضمّن بدورها البطاقة المفقودة كإحدى وسائل الدّفع.
- احرصوا على مراقبة بيانات بطاقة ائتمانكم بانتباه بعد التّبليغ عن فقدانها.
- إذا لاحظتم أيّ رسومٍ تبدو لكم احتياليّة أو غير مألوفة، اتّصلوا بشركة بطاقة الائتمان مباشرةً.

٦,٧ الاحتيال المصرفي على الإنترنت

إذا كنتم تشكّون أنّكم وقعتم ضحيّةً للاحتيال المصرفيّ، يمكنكم اتّخاذ بعض الخطوات للتّخفيف من خسارات حسابكم.

- تواصلوا مباشرةً مع مصرفكم.
- احرصوا على توثيق تاريخ تقرير الاحتيال أو اكتشافه بالإضافة إلى وقت حدوثه والتّفاصيل المرفقة به.
- دوّنوا كلّ الملاحظات والإجراءات الّتي تمّ اتّخاذها.
- اكتبوا بالتّفصيل الخطأ الّذي تشكّون بحدوثه، بما في ذلك الأجوبة الّتي تجيب عن الأسئلة التّالية: ما هو الفعل الّذي تمّ ارتكابه؟ من هو المتّهم؟ هل ما زال نشاطه مستمرًّا؟ متى حدثت عمليّة الاحتيال؟ ما هي قيمة الخسارة الحقيقيّة أو المفترضة؟
- حدّدوا كلّ الأدلّة المتّصلة بالفعل مثل الفواتير، والعقود، وطلبات الشّراء، والشّيكات، إلخ.

٧. قوى الأمن الدّاخلي متوفّرة لمساعدتكم

٧,١ اطلبوا المساعدة من مكتب مكافحة الجرائم السّيبرانيّة التّابع لقوى الأمن الدّاخلي (ISF (Counter Cybercrime Bureau

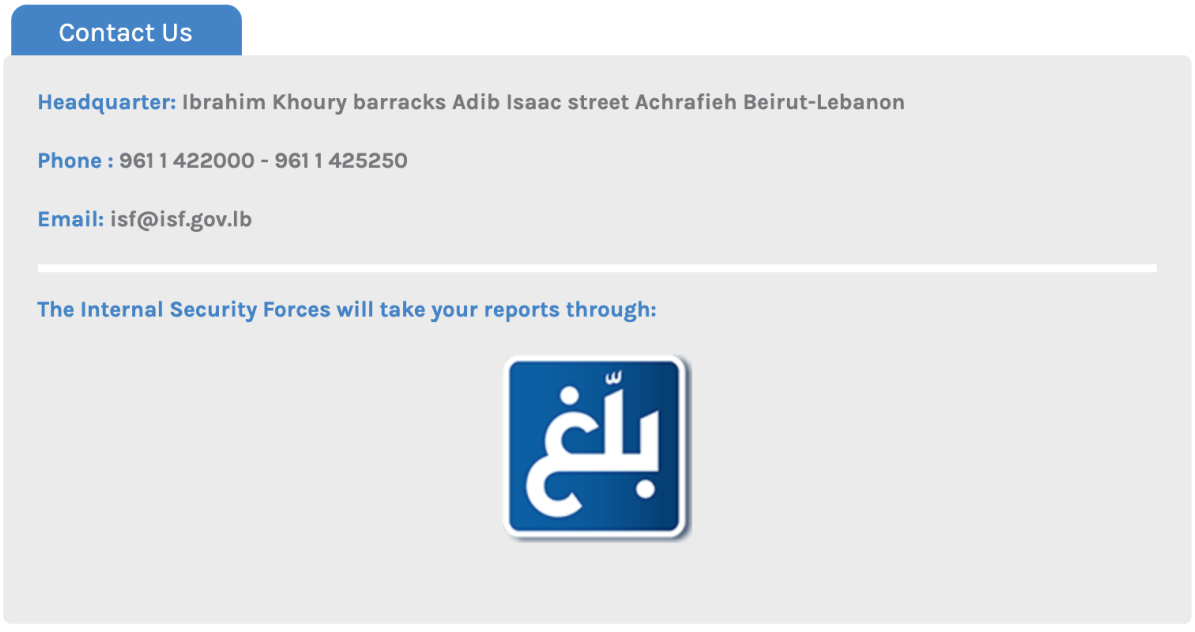
إذا لم تكن التّوجيهات المذكورة أعلاه كافية، من الأفضل أن تطلبوا المساعدة من أحد خبراء قوى الأمن الدّاخليّ.

- يمكنكم أيضًا التّواصل بالخطّ السّاخن لمكتب مكافحة الجرائم السّيبرانيّة ومكتب حماية الملكيّة الفكريّة على الرّقم: ٢٩٣ ٢٩٣– ٠١ المتوفّر ٢٤/٢٤.
- يمكنكم أيضًا إرسال بريد إلكتروني إلى مكتب مكافحة الجرائم السّيبرانيّة ومكتب حماية الملكيّة الفكريّة على: cybercrime@isf.gov.lb .

٧,٢ بلّغوا عن الجرائم السّيبرانيّة لقوى الأمن الدّاخلي

إذا أردتم التّبليغ عن جريمة سيبرانية لقوى الأمن الدّاخليّ، يمكنكم اتّباع الخطوات التّالية:

- زوروا موقع قوى الأمن الدّاخليّ (http://isf.gov.lb)
- اضغطوا على الصّورة الظّاهرة أدناه
- املأوا الاستمارة أو اطلبوا رقم الهاتف الموجود أو أرسلوا رسالةً عبر البريد الإلكتروني.



٨. يومٌ سيّء في حياة موظّف أعمال

٩. يومٌ جيّد في حياة موظّف أعمال

١٠. المرفق: تعاريف ومصطلحات

- **تهديد بريد العمل الإلكتروني (Business Email Compromise– BEC)**: شكل من أشكال الجرائم السّيبرانيّة يعتمد على استخدام الاحتيال على البريد الإلكتروني بغية تحقيق الرّبح المادّي.
- **الأمن السّيبراني**: حماية أنظمة المعلومات والتّواصل من الضّرر والاستخدام والتّغيير غير المشروعين.
- **التشفير**: عمليّة تحويل المعلومات أو البيانات إلى شيفرة لا يمكن قراءتها لا سيّما بهدف تفادي الوصول إليها من دون إذن.
- **إعادة تعيين إعدادات المصنع (Factory Reset)**: إعادة جهازكم إلى حالته الأساسيّة من خلال إلغاء كلّ المعلومات المخزّنة عليه.
- **الخرق (Hacking)**: الدّخول غير المشروع إلى نظام أو كمبيوتر.
- **IOT**: اختصار لعبارة Internet of Things، وهو نظام الأجهزة الّتي تتّصل بالإنترنت (الحوسبة، والمجال الميكانيكي، والمجال الرّقمي، والأشياء، والألعاب، إلخ).
- **البرنامج الخبيث (Malware)**: أيّ برنامج يهدّد عمل النّظام من خلال القيام بفعل أو عمليّة غير مشروعين.
- **التّصيّد الاحتيالي (Phishing)**: اللّجوء إلى الخداع (بشكل رقمي) للتّلاعب بالأفراد ودفعهم إلى الإفصاح عن معلومات سرّيّة أو شخصيّة يمكن استخدامها لأهداف احتياليّة.
- **عبارة المرور**: مجموعة كلمات يجب استخدامها للوصول إلى نظام كمبيوتر أو إحدى خدماته.
- **برنامج الفدية (Ransomware)**: أحد أشكال البرامج الخبيثة المصمّمة لمنع الوصول إلى نظام كمبيوتر إلّا إذا تمّ دفع مبلغ من المال مقابل فكّ التّشفير.
- **الخداع (Scam)**: الخداع هو آليّة مستخدمة للحصول على معلومات متعلّقة بالشّخص أو للوصول إلى معلومات الدّفع. ويمكن أن يحصل على البريد الإلكتروني، أو مواقع التّواصل الاجتماعي، أو الصّيرفة، أو بطاقة الائتمان.
- **التّصيّد الاحتيالي الموجّه (Spear Phishing)**: محاولة تصيّد احتيالي موجّهة لأفراد معيّنين. وخلافًا للتّصيّد الاحتيالي العاديّ، يقوم المعتدون في هذه الحالة عادةً بتجميع معلوماتٍ شخصيّة عن هدفهم من حساباته على مواقع التّواصل الاجتماعيّ من أجل زيادة فرصهم بالنّجاح.
- **انتحال الشّخصيّة (Spoofing)**: يعني فعل الإقناع بأنّ محادثةً أو عمليّة تواصل غير معروفة جاءت من مصدر معروف وموثوق به.
- **عمليّة التّوثيق القائمة على عاملين (Two–factor Authentication)**: طريقة للتّأكّد من صحّة هويّة المستخدم من خلال استخدام عاملين مختلفين: ١) شيءٌ يعرفونه، أو ٢) شيءٌ يملكونه، أو ٣) هويّة شخصيّة.