دليل التوعية حول المخاطر السيبرانية

قوى الأمن الداخلي

شعبة العلاقات العامة

خدمة - ثقة - شراكة

الفهرس

الصفحة

١- مقدمة

ان التطور التقني الحاصل، لاسيما في مجال المعلوماتية والاتصالات، قد حوّل العالم الى قرية كونية من خلال شبكة الإنترنت التي سمحت بتطوير العديد من البرامج منها برامج الدردشة ومنصات التواصل الاجتماعي وغيرها من التطبيقات التي قلّصت المسافة بين الناس وسمحت بالتواصل فيما بينهم بشكل آني وسريع من خلال تبادل الرسائل والصور والبيانات، وأيضاً توفير الخدمات الإلكترونية المختلفة التي تساعد في إنجاز المعاملات الإلكترونية بكافة أشكالها.

في المقابل، برزت الى الواجهة أنواع جديدة من الجرائم، التي تقوم بإستغلال تكنولوجيا المعلومات من أجل إرتكاب جرائم مستجدة أو جرائم قديمة ولكن بأساليب وطرق حديثة. وباتت المخاطر السيبرانية تشكل مشكلة كبيرة لكونها تسببت في زيادة الجرائم المتعلقة باختراق البيانات الشخصية للأفراد والمؤسسات وسرقتها وأيضاً تهديد البنية التحتية المعلوماتية للأنظمة والشبكات الحيوية على مستوى الدولة. من هنا أصبح لزاماً علينا العمل لرفع مستوى الوعي حول المخاطر والتهديدات المتصلة بشبكة الانترنت ومنها سرقة الهويّات، كلمات المرور الخاصة بالحسابات، قرصنة البيانات، الإبتزاز الإلكتروني... بالإضافة الى اتباع أفضل الممارسات في الوقاية والحماية وتعزيز الإجراءات والتدابير الأمنية الضرورية الواجب إتخاذها عند التعرض لمثل هذه الحالات.

أمام هذ الواقع، فإنّه يقع على مؤسسة قوى الأمن الداخلي، من ضمن واجباتها ومسؤولياتها الوطنية، حماية أفراد المجتمع من كافة المخاطر التي تتهددهم، لاسيما الجرائم والهجمات السيبرانية، وهي على جهوزية تامة لتأدية هذا الواجب وتحمل هذه المسؤولية من خلال العمل على تأمين الحماية المطلوبة على شبكة الإنترنت وضمان أمن الفضاء السيبراني اللبناني وتوعية المواطنين، وأيضاً من خلال القيام بالتحقيقات اللازمة لكشف المجرمين السيبرانيين وتوقيفهم وإحالتهم الى المراجع القضائية المختصة مع المحافظة على سرية هذه التحقيقات وإحترام الخصوصية الفردية ومعايير حقوق الإنسان.

٢- الهدف

يهدف هذا الدليل الى رفع مستوى الوعي لدى أفراد المجتمع حول أبرز المخاطر والتهديدات والجرائم السيبرانية التي قد تواجههم وكيفية تأمين الحماية اللازمة منها وضمان توفير الخصوصية الفردية جراء استخدام تقنيات تكنولوجيا المعلومات والإتصال بشبكة الإنترنت.

بالإضافة إلى ذلك، يَعرُض هذا الدليل الخطوات والإجراءات الإحترازية والممارسات الفضلى الواجب إتباعها بشكل واضح بغية حماية المعلومات والبيانات الشخصية من السرقة، منع تعرض الأجهزة الإلكترونية للإختراق، تجنُّب الوقوع ضحية للإبتزاز الالكتروني، وحماية الأطفال وباقي أفراد العائلة أثناء إستخدام شبكة الإنترنت.

٣- أنواع الجرائم السيبرانية

مع إزدياد الإعتماد على الأجهزة الإلكترونية لاسيما الهواتف الذكية والأجهزة المحمولة للتواصل على شبكة الإنترنت والإستفادة من مختلف التطبيقات والخدمات الإلكترونية التي تؤمنها الشركات والمؤسسات الحكومية والخاصة على إختلافها، أصبحت هذه الأجهزة عرضة للمزيد من الهجمات الإلكترونية لعدة أهداف منها ما يتعلق بسرقة المعلومات، الإبتزاز، التخريب، تحقيق الكسب المادي، أو ضرب المصداقية أو السمعة. لذلك يجب على جميع أفراد المجتمع أن يكونوا حريصين على حماية هذه الأجهزة من القرصنة والهجمات الإلكترونية. وفيما يلي نعرض أبرز أنواع الجرائم الإلكترونية التي ظهرت مؤخراً:

٣.١- الابتزاز الإلكتروني Extortion

هو عملية تهديد وترهيب لضحية ما بنشر صور أو مواد مصورة، أو تسريب معلومات سرية خاصة بها أو بأحد أفراد عائلتها، مقابل إجبارها على دفع مبالغ مالية أو إستغلالها لغايات جنسية، غير اخلاقية، أو غير مشروعة لصالح المبتزين. ان الإبتزاز الالكتروني يؤثر بشكل رئيسي على الحالة النفسية والإجتماعية للضحايا، مما يجعل نسبة كبيرة منهم يترددون في تقديم الشكاوى خشية نشر مقاطع الفيديو العائدة لهم أو غيرها، أو خوفاً من نظرة المجتمع لهم فيعمدون إلى الرضوخ الى طلبات المبتز ويقومون بإرسال مبالغ مالية، أو إيذاء انفسهم، وقد يؤدي بهم الأمر في بعض الحالات الى الانتحار.

ونعرض فيما يلي بعض الأمثلة عن حالات الإبتزاز الإلكتروني:

١. الإحتفاظ بمقاطع فيديو وتسجيلات أو صور شخصية أو إباحية تم إلتقاطها خلال محادثات إلكترونية عبر الكاميرا والتهديد بنشرها لقاء المطالبة بمبالغ مالية أو خدمات جنسية أو غيرها...

٢. سرقة البيانات والصور الشخصية أو العائلية عن الهاتف أثناء صيانته وإبتزاز صاحبه.

٣. ايهام الضحية بمعرفة المواقع الإلكترونية التي تقوم بتصفحها وابتزازها من خلال التهديد بنشرها.

٣.٢- التصيد الاحتيالي عبر الانترنت Phishing:

هو نوع من تقنيات الخداع على شبكة الانترنت التي غالباً ما تستخدم لسرقة بيانات المستخدمين الشخصية مثل تفاصيل تسجيل الدخول وكلمات المرور، رقم الهاتف، بطاقات الائتمان، وغيرها. فعلى سبيل المثال، يقوم المجرمون السيبرانيون بإنشاء موقع إلكتروني مزيف يشبه الموقع الأصلي (موقع فايسبوك مزور مثلاً **faceb00k.com** بدلاً من **facebook.com**) ومن ثم إرسال رابط الموقع المزيف إلى الضحية من خلال البريد إلكتروني أو عبر وسائل التواصل الإجتماعي، على أساس أنها مرسلة من مصدر موثوق، (مثل الشركة أو البنك أو حتى الموقع الالكتروني الذي تتعامل معه)، ودفعه بأساليب مختلفة للضغط على الرابط المذكور. وفي هذه الحالة يتم توجيهه لإدخال معلومات شخصية هامة عنه، يمكن استخدامها من قبل المقرصن لاحقاً لغرض الإحتيال أو الدخول غير المشروع الى حسابات الضحيّة، أو يؤدي ذلك إلى تثبيت برامج خبيثة على أجهزة الضحيّة تساعد القراصنة في سرقة المعلومات أو في عمليات التخريب.

٣.٣- سرقة الهوية أو إنتحال الشخصية Identity Theft:

هي نوع من أنواع الغش التي تحصل عندما يستخدم شخص ما معلومات تعريف شخصية تعود لشخص آخر، مثل الاسم، رقم جواز السفر، بطاقة الهوية، رخصة السوق، بطاقة الائتمان، تفاصيل الحسابات الالكترونية أو صورته، دون إذنه، بغية إرتكاب أعمال إحتيالية، سرقة المال وبطاقات الائتمان، أو مجرد الحاق الضرر والإساءة الى السمعة.

ومن أبرز الأمثلة على سرقة الهوية ما يلي:

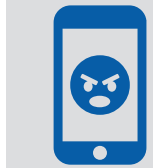
١. سرقة الحسابات الخاصة على مواقع التواصل الاجتماعي Facebook, Twitter, Instagram, Snapchat, LinkedIn ... بغية انتحال صفة الضحية وإلحاق الضرر بسمعتها من خلال التشهير بها ونشر معلومات مسيئة لها، أو مضايقة أصدقائها عبر استعمال حسابها للتنمر عليهم.

٢. سرقة الحسابات على خدمات البريد الالكتروني العامة والمراسلة الفورية (Instant Messaging).

٣. سرقة الحسابات على مواقع الألعاب الالكترونية.

٤. فتح حسابات مصرفية والحصول على قروض والقيام بأعمال غير مشروعة من خلال انتحال هوية الضحية بشكل كامل.

٥. استخدام حسابات بطاقات الائتمان العائدة للضحية بطرق غير مشروعة للقيام بعمليات شراء أو سحب مبالغ نقدية.



٣.٤- التنمر الإلكتروني Cyberbullying:

هو قيام شخص أو مجموعة من الاشخاص بمضايقة، سوء معاملة، أو السخرية تجاه شخص آخر مراراً وتكراراً من خلال رسائل البريد الإلكتروني، المواقع الاكترونية، نشر الفيديوهات والمدونات، أو بأي وسيلة إتصال أخرى بهدف إلحاق الضرر به.

ويشمل التنمر الإلكتروني الأمثلة التالية:

١. نشر رسائل إفتراء على مواقع التواصل الإجتماعي.

٢. نشر شائعات على شبكة الإنترنت.

٣. التحريض من خلال شبكة الإنترنت على إستبعاد شخص من مجموعة معيّنة أو استبعاده اجتماعياً.

٣.٥- قرصنة الأجهزة والبيانات Hacking IT Systems:

و تتضمن إختراق أو محاولة اختراق البيانات الالكترونية الخاصة بالأفراد والمؤسسات الحكومية أو الخاصة بهدف سرقتها أو تخريبها.
وقد تحتوي هذه البيانات على معلومات حساسة متعلقة بالمواطنين، العملاء، الموظفين أو بأمور أخرى لا تقل أهمية مثل الملكية الفكرية.

٣.٦- برمجيات «الفدية» الخبيثة Ransomware و تشفير البيانات

يتسبب هذا النوع من البرمجيات بتشفير البيانات الهامة أو تشفير الجهاز بأكمله (جهاز كمبيوتر أو هاتف ذكي)، بحيث لا يستطيع المستخدم الوصول إلى بياناته. ومن ثم يقوم المقرصن بالطلب من الضحية مبلغًا ماليًا «فدية» عبر العملات الرقمية مثل Bitcoin، كونها صعبة التتبع، مقابل فكّ التشفير عن البيانات وإعادة الأمور لطبيعتها (وهذا ليس مضموناً أبداً ولا يُنصح به).

٣.٧- الإحتيال عبر البريد الالكتروني الخاص بالعمل
Business Email Compromise Fraud

هو نوع من عمليات الاحتيال التي تستهدف الشركات التي تجري عادة تحويلات مالية أو لديها موردين في الخارج. ويعتمد هذا النوع من الجرائم بشكل أساسي على الوصول إلى حسابات البريد الإلكتروني للمديرين التنفيذيين والمسؤولين عن التحويلات المالية في الشركة من خلال استحداث عناوين بريد إلكتروني مشابهة لها أو اختراق العناوين الأصلية بالإعتماد على تقنية التصيد الاحتيالي phishing أو على الهندسة الاجتماعية (Social Engineering) ومن ثم خداع الموظفين التابعين للشركة من خلال انتحال صفة الرئيس التنفيذي أو أي مسؤول تنفيذي مفوض بإعطاء الإذن لإجراء التحويلات المالية الى الخارج، من أجل القيام بتحويلات احتيالية معجلة، بما يؤدي إلى خسائر مالية كبيرة.

أي أنّه وبعد معرفة المجرم الإلكتروني بالإجراءات المتبعة، يعمد إلى استخدام حساب البريد الالكتروني الخاص بالمدير الذي تم تزويره من أجل تنظيم طلب تحويل أموال معجل. ويطلب من الموظف عدم إتباع المسار التقليدي المعتمد عادة لتصديق طلب التحويل. ليقوم الموظف بتحويل الأموال بسرعة الى حساب يديره المجرم في أحد البنوك غالباً ما يكون خارج نطاق الدولة التي تقع ضمنها الشركة. في هذه الحالة، سيكون المدير الحقيقي غير مدرك بفحوى الطلب وبأي إجابات ترد عبر البريد الالكتروني من قِبل الموظفين.

٤- الحماية من المخاطر والجرائم السيبرانية

بالرغم من تطور تقنيات الحماية الإلكترونية والأمن السيبراني بالتوازي مع تطوّر الهجمات الالكترونية، يبقى من الضروري اتخاذ بعض الاجراءات الضرورية واتباع أفضل الممارسات لتجنّب الوقوع ضحية للجرائم السيبرانية ودرء المخاطر الناتجة عنها.

٤.١- حماية الحسابات والتطبيقات من مخاطر الإنترنت

تشكل حماية البريد الإلكتروني، كلمات المرور، حسابات مواقع التواصل الإجتماعي، تطبيقات المراسلات النصية، والتجهيزات الالكترونية جزءاً أساسياً من حماية المجتمع من مخاطر الإنترنت. وينبغي لتحقيق هذا الغرض الالتزام بالإجراءات واتباع الإرشادات الواردة أدناه والعمل على تطبيقها بشكل تام.

٤.١.١- اختيار كلمة مرور قوية:

- استخدم كلمات مرور قوية ومعقدة تتضمن مزيج من الأحرف الكبيرة (A – Z) والصغيرة (a – z)، إضافة إلى الأرقام والرموز والعلامات الخاصة (!,&,@,%,$,#) على أن لا تقل عن ١٢ حرفاً.

- استخدم جملاً كاملة لكلمات مرور إذا أمكن (على سبيل المثال Th1515@5tr0ngP@55) مع استبدال بعض الأحرف برموز خاصة.

- تجنّب استخدام المعلومات الشخصية في كلمات المرور مثل الإسم، رقم الهاتف، عنوان السكن، تاريخ الميلاد، الخ.

- يجب ألا تتضمن كلمات المرور أية كلمات موجودة في القاموس حتى لا يسهل تخمينها.

- تجنّب استخدام حروف متسلسلة abcd١٢٣٤٥ ومتتاليات لوحة المفاتيح مثل qwerty asdzxcg.

- تجنب إستخدام نفس كلمة المرور لمختلف الحسابات والتطبيقات.

- إستخدم التطبيقات الخاصة والموثوقة بإدارة كلمات المرور Password Manager إذا أمكن للمساعدة في إنشاء كلمات المرور وإدارتها.

- تجنّب حفظ كلمات المرور جنباً الى جنب مع معلومات تفصيلية عن الحساب في أماكن غير آمنة مثل الهواتف المحمولة، أجهزة الكمبيوتر، أو الأوراق المكتوبة.

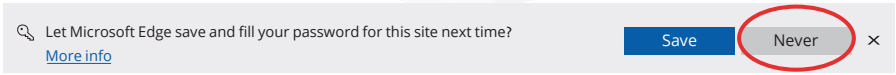
- لا تشارك كلمات المرور الخاصة بك ولا تقم بإدخالها بشكل مرئي أمام أي كان.

- قم بتغيير كلمة المرور بشكل فوري إذا اشتبهت بأن أي من حساباتك قد تعرض للقرصنة.

- قم بتغيير كلمة المرور الخاصة بحساباتك بشكل دوري واحرص على اختيار كلمة مرور جديدة مختلفة عن سابقاتها.

- كن حذراً عند اختيارك للأسئلة التذكيرية لكلمة المرور، التي تستخدمها بعض المواقع للمساعدة في تذكر كلمة المرور في حال نسيانها، بحيث لا تكون قابلة للتخمين بسهولة (اسم الأب مثلاً كجواب لسؤال التذكير).

- تجنّب حفظ كلمات المرور على أي من التطبيقات التي توفر ميزة «حفظ كلمة المرور».



٤.١.٢- حماية الحسابات على مواقع التواصل الاجتماعي (Facebook, Twitter, Instagram, Snapchat, LinkedIn, ...)

- الإلتزام بمعايير إختيار كلمات المرور الواردة آنفاً.
- توفير الحد الأدنى من المعلومات المطلوبة والضرورية لفتح حساب جديد على مواقع التواصل الاجتماعي.
- مراجعة خصائص الحماية الإضافية في مواقع التواصل الاجتماعي والحرص على تفعيلها من أجل زيادة مستوى الحماية المتعلقة بالحسابات. مثال تفعيل خاصية المصادقة الثنائية 2FA Two Factor Authentication الخاصة بصلاحية الدخول، الحد من الوصول الى تفاصيل الحساب Limit Access، تشديد خيارات الخصوصية الـ Privacy وتفعيل الإنذار بالطرق المناسبة Alerting عند حصول محاولات مشبوهة للدخول الى الحساب.
- التنبه إلى ما تقوم بنشره من معلومات شخصية مفصلة عنك وعن عائلتك لأنه يصعب التحكم بأية معلومة بعد نشرها.
- تجنّب المشاركة في أيّة أنشطة إلكترونية مؤذية وغير قانونية مثل الابتزاز، التشهير، الإستهانة بالمعتقدات الدينية أو الطائفية أو الإساءة إليها، توجيه التهديدات الى الآخرين والتسبب بالأذى لهم.
- الحرص على التواصل مع الأشخاص الموثوق بهم فقط، وأخذ الحذر من الغرباء والمتنمرين الذين يطلبون إضافتك كصديق لهم.

- عدم التجاوب مع أي محادثة ترد من مصدر غير معروف لا سيما أن البعض يعمد، عن قصد أو غير قصد، الى تغيير أو إخفاء هويتهم الحقيقية (العمر، الإسم، الجنس، والصورة) على مواقع التواصل الاجتماعي.
- تجنّب نشر أو إعادة نشر (share, retweet ...) معلومات غير صحيحة وغير موثوقة.
- تجنّب طلب صداقات أو قبول طلب صداقات من قبل أشخاص غير معروفين منك، والتحقق قبل قبول صداقتهم من الصور المنشورة على صفحتهم ولائحة صداقاتهم.
- تجنّب تبادل البيانات الخاصة بحساباتك على مواقع التواصل الاجتماعي أو السماح لأي كان استخدام حساباتك تحت أي ظرف من الظروف.
- اعتماد تسجيل الخروج من حساباتك على مواقع التواصل الاجتماعي عند الإنتهاء من استخدامها.
- التأكد من ربط الحسابات على مواقع التواصل الإجتماعي برقم الهاتف المحمول بهدف التحقق من بيانات الحساب عند الدخول إليه، وكذلك لتسهيل عملية استعادته في حال فقدانه.
- عدم النقر على أية روابط غير آمنة ترد ضمن وسائل التواصل الاجتماعي لأنها قد تحوي فيروسات خبيثة.

كيف تحمي نفسك على الإنترنت؟

لا تضغط على الروابط والمرفقات التي تردك من خلال الرسائل الالكترونية المجهولة المصدر

فكر جيداً قبل نشر أي صور أو فيديوهات تتعلق بك أو بعائلتك

حافظ على خصوصية معلوماتك الشخصية موقع منزلك وعملك وحساباتك ورقم هاتفك وكلمات المرور

لا تتواصل مع الغرباء بل فقط مع أشخاص موثوقين ومعروفين من قبلك

٤.١.٣- حماية حسابات البريد الإلكتروني (Gmail, Hotmail و Yahoo, ...)

- الإلتزام بمعايير إختيار كلمات المرور الواردة آنفاً.
- إنشاء حساب البريد الإلكتروني الجديد من قبلكم شخصياً، والتنبّه في حال السماح لأحد ما بمساعدتكم كون ذلك يجعله قادراً على إستعادة كلمة المرور لاحقاً حتى ولو قمت بتغييرها.
- مراجعة خصائص الحماية الإضافية في الحسابات الخاصة بكم والحرص على تفعيلها من أجل زيادة مستوى الحماية المتعلقة بعناوين البريد الإلكتروني. مثال على ذلك إعتماد خاصية المصادقة الثنائية 2FA Two Factor Authentication، تفعيل الحماية من الرسائل الإلكترونية التطفلية Spam Protection، واستخدام فلاتر البريد الإلكتروني Email Filter، إلخ...
- مشاركة عنوان بريدك الالكتروني فقط مع الأشخاص الموثوقين.
- التحقق من خانات المرسل اليهم TO و CC و BCC عند ارسال البريد الالكتروني للتأكد من عدم إضافة أشخاص غير مرغوبين.
- إنشاء عنوان بريد الكتروني إضافي لإستخدامه من أجل إستعادة حساب بريدك الالكتروني الأساسي في حال تعرضه للقرصنة أو السرقة.
- تجنّب استخدام بريدك الالكتروني للمشاركة في مسابقات أو ألعاب إلكترونية مشكوك في صحتها.

- التنبه من مسترقي النظر عند ضرورة فتح بريدك الالكتروني أمام الآخرين أو في مكان عام.
- تجاهل رسائل البريد الالكتروني التي ترد من مصادر مجهولة أو غير معروفة والتي قد تطلب منك إدخال بياناتك الشخصية مثل اسم الحساب وكلمات المرور أو غيرها.
- التنبّه من فتح الروابط داخل البريد الإلكتروني الوارد إلى صندوق بريدك أو فتح أي مرفقات به قبل التأكد من المصدر، لتفادي تحميل برمجيات ضارة أو خبيثة قد تهدف إلى قرصنة الحساب والجهاز لأعمال التجسس أو التخريب.
- حذف الرسائل الالكترونية التطفلية Spam بشكل فوري وتجنّب التفاعل معها أو الرد عليها كون ذلك من شأنه أن يعرّضك لمزيد من الرسائل التطفلية.
- عدم ترك عنوان البريد الإلكتروني مرئيّاً للجميع في شبكات التواصل الإجتماعي وغيرها من المواقع، وعدم تزويده إلا للأشخاص المعروفين من قبلك.
- الحذر من الرسائل الالكترونية التي لا تتوجه إليك باسمك وتستخدم عبارات عامة لإلقاء التحية مثل «عزيزي المستخدم»، و«عزيزي مستخدم البريد الالكتروني» لأنها قد تكون محاولات لتنفيذ عملية التصيد الإحتيالي phishing.

- الحرص على الإتصال بالإنترنت من خلال بروتوكول https الآمن إذا أمكن، والذي يسبقه عادة رمز القفل 🔒 ، لضمان سلامة المعلومات أثناء التواصل مع مزوّدي خدمات البريد الإلكتروني.

- التنبه من الرسائل الالكترونية التي توحي بوجود حالة طوارئ ما خاصة بك (مثلاً لقد تخطيت حصة الرسائل الالكترونية الخاصة بك، لقد وقعت ضحية لعملية اصطياد احتيالي، أو حساب بريدك الالكتروني على وشك الإغلاق...) كونها يمكن أن تكون محاولة لخرق الخصوصية أو قرصنة الحساب.

- التنبّه من مشاركة المعلومات الحساسة الخاصة بك (مثل بطاقة الائتمان العائدة لك) أو غيرها من المعلومات الهامة عبر البريد الالكتروني.

- تجنّب التفاعل مع الرسائل المغرية التي تزعم أنك ربحت جائزة أو مبلغاً من المال، فهذه الرسائل غالباً ما تكون عبارة عن رسائل تهدف الى تنفيذ عملية تصيد إحتيالي.

- الإحتفاظ بشكل دائم ودوري بنسخ احتياطية عن الرسائل الالكترونية الهامة في صندوق البريد.

- إعتماد تسجيل الخروج من حساب البريد الالكتروني عند الإنتهاء من استخدامه.

- افتح بريدك الالكتروني بشكل دوري حتى لا تنتهي صلاحيته في حال عدم استخدامه كون ذلك يدفع الشركة إلى استرداده ومن ثم قد يقوم شخص آخر بالحصول عليه ومن خلاله يمكنه قرصنة حساباتك الالكترونية.

٤.١.٤- حماية تطبيقات المحادثات النصية (... WhatsApp, Skype, Signal, Telegram)

- الالتزام بمعايير إختيار كلمات المرور الواردة آنفا في حال وجدت.
- قم بمراجعة خصائص الحماية الإضافية Advanced Security Settings في تطبيقات المحادثات النصية واحرص على تفعيلها من أجل زيادة مستوى الحماية المتعلقة بهذه التطبيقات. مثال عى ذلك إعتماد خاصية المصادقة الثنائية Two Factor Authentication من أجل صلاحية الدخول، تشفير الرسائل، والاحتفاظ بنسخ إحتياطية Backup عن الرسائل المهمة...
- إحذر من الرسائل مجهولة المصدر التي تطلب معلومات خاصة أو شخصية، وتجنّب فتح الروابط أو المرفقات التي تحتويها، لأنها قد تؤدي الى تحميل برمجيات ضارة وخبيثة تهدف الى سرقة المعلومات والبيانات الشخصية وقرصنة الجهاز.
- قم بالإبلاغ عن الرسائل التطفلية Spam فور إستلامها لدى إدارة التطبيق Report as spam.
- قم بحظر المستخدمين غير المرغوب فيهم Block لمنعهم من التواصل معك بشكل مباشر.
- لا تنجذب للروابط التي تردك عبر تطبيقات الدردشة مهما بلغ حجم الإغراءات لأنها قد تحوي فيروسات ضارة.
- تجنب الدخول في مجموعات الدردشة التي تروج معلومات ذات جانب عدائي أو تشكل تهديداً بالنسبة إليك.
- عدم الرد والتجاوب مع أي دردشة ترد من مصدر غير معروف.

- عدم التواصل أو تبادل الصور الخاصة من خلال مكالمات الفيديو مع أي شخص كان لتجنب الوقوع ضحية لعمليّات الإبتزاز بكافة أشكاله.
- قم بإلغاء حسابات الدردشة الخاصة بك في مختلف التطبيقات ومحو البيانات المتعلقة بها عن هاتفك الخليوي قبل التخلي عنه لأي سبب.
- تعزيز خصائص الحماية من خلال إستخدام رقم سري Pin لفتح تطبيقات الدردشة.
- قم بتحميل كافة التطبيقات من المتاجر الرسمية فقط (مثل Apple Store أو Google Play Store).
- تجنّب إرسال أية بيانات سرية أو تفاصيل الحسابات المصرفية أو كلمات المرور أو غيرها من الوثائق والمستندات الحساسة عبر هذه التطبيقات.

٤.٢- حماية الأطفال على الإنترنت

- ينبغي دوماً النقاش مع أفراد العائلة في مسألة التهديدات الالكترونية التي تحصل على مواقع التواصل الاجتماعي وتطبيقات المحادثة النصية لاسيما التنمر السيبراني Cyberbullying والابتزاز الجنسي Sextortion.
- ينبغي مراقبة استخدام الأطفال للإنترنت، ولهذا ينصح إبقاء الأجهزة الإلكترونية على إختلافها في مكان مرئي في المنزل وليس في مكان معزول، كغرفة الجلوس بدل غرف النوم مثلاً.
- يجب أن تقضي بعض الوقت مع أطفالك على الانترنت لكي تعلّمهم كيفية التصفح الآمن وتكون على إطلاع بكيفية إستخدامهم للإنترنت.
- إحرص على محاورة أطفالك والتحدث إليهم بصراحة ووضوح حول المعلومات الشخصية وعن السبب في خصوصيتها، إذ يمكن إستخدام هذه المعلومات في تحديد هويتهم أو أماكن سكنهم والأماكن التي يرتادونها أو الأنشطة التي يشاركون فيها واستغلالها لإلحاق الأذى بهم.

- إنصح أولادك بأن يكونوا حذرين جداً عند نشر صور أو فيديوهات خاصة بهم على الإنترنت ومواقع التواصل الإجتماعي لأنه بمجرد نشرها يمكن للجميع الوصول إليها بسهولة، ويمكن أن تُستخدم لغرض سيء.
- حذّر أولادك بعدم التّواصل مع أشخاص غرباء أو غير معروفين، وعدم مشاركتهم أيّة صور أو بيانات أو فيديوهات أو معلومات شخصية (عنوان السكن، رقم الهاتف، عنوان البريد الإلكتروني) وعدم استخدام محادثات الفيديو للتواصل معهم وعدم القبول بلقاء هؤلاء الأشخاص مهما اقتضى الأمر.
- علّم أطفالك على ضرورة التحدث معك وابلاغك عن أي مشكلة أو تهديد أو إبتزاز قد يواجهونه على الإنترنت مهما كان حجمه.
- إستكشف مع أطفالك المواقع المفضلة لديهم وساعدهم على القيام بعملية الإشتراك والتسجيل فيها عبر إختيار اسم مستعار وأن لا يكشفوا عن أية معلومات حول هويتهم الشخصية.
- ضع مجموعة من القواعد للأطفال وتأكد من معرفتهم بماهية المعلومات التي يمكن مشاركتها مع الآخرين وتحديد أنواع المواقع الإلكترونية التي يمكن زيارتها والألعاب الالكترونية التي يمكن الدخول إليها والتي تناسب أعمارهم.
- قم بتحديد الوقت المسموح به للأطفال بالاتصال بشبكة الإنترنت والإلتزام به كونهم بحاجة إلى توازن في الأنشطة للتمتع بطفولة صحية، وقم باتخاذ الاجراءات المناسبة لذلك مثل إطفاء جهاز «الراوتر» للإتصال اللاسلكي أثناء وقت النوم أو غيرها.

- شجّع أطفالك على إستخدام خصائص الحماية والأمان Security and Privacy Settings في البرامج والتطبيقات بهدف الحرص على حمايتهم.

- اعمل على إنشاء حساب إلكتروني عائلي خاص بالأمور الترفيهية يمكن إستخدامه للمشاركة في المسابقات وغيرها من الأنشطة.

- إنصح أولادك بعدم نشر معلومات أو فيديوهات أو صور مسيئة للآخرين على الإنترنت كون ذلك يعرضهم للملاحقة القانونية.

- شجّع أولادك بعدم الرد على المنشورات السلبية التي لا تعجبهم وعدم التواصل مع أي شخص يقوم بإرسال رسائل فيها إساءة لهم على الإنترنت.

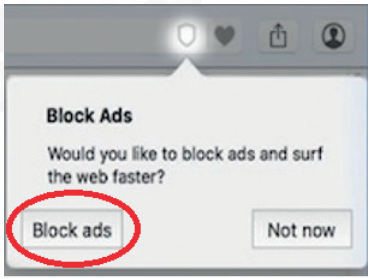
- إنصح أولادك بعدم تحميل نسخ غير قانونية من البرامج والتطبيقات أو تنزيل الموسيقى أو الأفلام بطرق غير شرعية بالإضافة الى الالتزام بنوعية الألعاب التي تناسب أعمارهم.

- إنصح أولادك بعدم الضغط على الأزرار والدعايات التي تقوم بترويج الإعلانات أو المباريات أو الجوائز على الإنترنت كون معظمها يحتوي على برامج ضارة أو يساهم في نشر محتوى سيء.

- ينبغي عدم فتح رسائل البريد الإكتروني مجهولة المصدر التي تحتوي على مرفقات أو بداخلها روابط لأنها قد تكون نوع من أنواع التصيد الإحتيالي أو قد تحوي على فيروسات ضارة.

- إنصح أولادك بإستخدام محركات بحث خاصة بهم ومناسبة لأعمارهم مثل Kiddle.co و kidrex.org وغيرها.

- إعمل على إعداد خصائص الأمان في متصفح الإنترنتBrowser كتفعيل ميزة حظر الإعلانات Ad Blocking واستخدام الفلاتر Web Filtering.



- ينبغي الكشف بشكل دوري على الحسابات الخاصة بأولادك على مواقع التواصل الاجتماعي والسؤال «هل يمكن لأي شخص غريب أن يستغلّ هذه المعلومات؟»

- ينبغي التحقق بشكل دوري من سجل متصفح الإنترنت History للاطلاع على المواقع والعناوين الإلكترونية التي يتصفحها أولادك.

- ينبغي عدم إعطاء الأولاد رقم بطاقة الإئتمان حرصاً على عدم قيامهم بعمليات شراء ودفع غير عادية ومن دون علمك المسبق.

- إحرص على إستخدام برامج المراقبة Filtering and Parental Control التي تسمح بمراقبة وحجب البرامج والمواقع غير المرغوبة وتتيح للأهل التحكم بنشاط الأطفال على شبكة الانترنت ومنعهم من الدّخول إلى المواقع غير المناسبة لأعمارهم.

- قم بتوعية الأطفال حول عدم مسح الرّسائل المسيئة لهم والحفاظ عليها كأدلّة احتياطيّة عند الحاجة إليها.

٤.٣- إجراءات حماية الأجهزة الإلكترونية

في سبيل تعزيز تدابير الأمان والحماية، يمكن للمستخدمين اتباع بعض الإجراءات التي تساعد في حماية الأجهزة الإلكترونية من القرصنة أو الإختراق وفقاً لما يلي:

٤.٣.١- إجراءات حماية أجهزة الكومبيوتر الثابتة (Desktops) والمحمولة (Laptops)

- الإلتزام بمعايير إختيار كلمات المرور الواردة آنفاً.

- التأكد من تفعيل جدار الحماية Firewall الحديثة المدمجة في أنظمة التشغيل ويندوز وماك Windows & Mac لتحديد منافذ الإنترنت الضرورية فقط.

- تفعيل قفل الشاشة/الجهاز Lock تلقائياً بعد فترة قصيرة من عدم الإستخدام.

- الحرص على تفعيل خاصية التحديث الأوتوماتيكي Automatic Updates لكافة البرمجيات/التطبيقات، وأنظمة التشغيل Operating System بهدف سد الثغرات الأمنية التي يتم اكتشافها والتي ينفذ من خلالها مجرمي الانترنت.

- القيام بتعطيل خاصية الوصول الى جهاز الكمبيوتر الخاص بك عن بعد Remote Access وتفعيلها عند الحاجة فقط.
- الحرص على إستخدام برنامج موثوق للحماية من الفيروسات والبرمجيات الخبيثة Antivirus & Antimalware واعتماد نسخ أصلية له والقيام بتحديثه باستمرار.
- الحرص دائماً على تغطية الكاميرا في الحاسوب المحمول في حال عدم إستخدامها.
- إطفاء وسائل إتصال الجهاز بالشبكة (Bluetooth ,NFC ,WiFi) في حال عدم إستخدامها.
- عدم تنزيل أية برامج أو ألعاب من مواقع غير موثوقة والعمل دائماً على تحميلها من مواقعها الأصلية.
- ضرورة تجاهل الرسائل والإعلانات Ads & Popups التي تدعوك لتنزيل برمجيات معينة تدعي أنها قادرة على تنظيف جهاز الحاسوب الخاص بك من الفيروسات والبرامج الضارة.
- تجاهل طلبات تحميل/تنزيل أية برامج أو تطبيقات لتقديم خدمات معينة عند ورودها من مصادر غير موثوقة.
- أخذ الحذر من العروض المجانية لتنزيل الموسيقى والالعاب لأنها طرق رائجة لنشر البرمجيات الخبيثة.
- التحقّق جيداً من الصلاحيات التي تستوجبها التطبيقات والبرامج ومدى الحاجة إليها قبل القيام بتحميلها.

- حذف Uninstall التطبيقات والبرمجيات التي لست بحاجة إليها.
- تجنّب العمل على الأجهزة المحمولة، في الأماكن المكتظة التي لا تتمتع بالخصوصية (مثل المقهى والفندق وغيرها)، لتجنّب استراق النظر إليها وخاصة عند العمل على بيانات ومعلومات خاصة أو حساسة.
- الحرص على عدم إستخدام حافظة المعلومات USB أو غيرها من وسائل التخزين الخارجية قبل فحصها والتأكد من خلوها من برمجيات خبيثة.
- ضرورة تسجيل الخروج من كافة حساباتك، وتنظيف سجل المتصفح History & Cookies، في حال اضطرارك للاتصال بشبكة الانترنت في الأماكن العامة (مثلاً في مقهى للإنترنت، المكتبة، أو في الفندق).
- الحرص دائماً على الإحتفاظ بنسخ إحتياطية من محتوى جهازك وبياناتك على أقراص CD ,DVD أو أقراص صلبة خارجية Hard Disk أو السحابة Cloud بهدف تقليل الأضرار التي قد تنتج عن الإصابة بأي نوع من الفيروسات والبرامج الخبيثة المطالبة بفدية أو التي قد تنتج عن تداعيات سرقة الحاسوب المحمول، تعطله أو فقدانه، والتأكد من إمكانية استرجاعها باستمرار.
- القيام بمسح البيانات الحساسة والشخصية (Wipe) من جهاز الكمبيوتر قبل التخلص منه لأي سبب كان.
- عدم استخدام أسم مستخدم ذات صلاحيات عالية Admin Rights للأعمال اليومية.

٤.٣.٢- إجراءات حماية الهواتف الذكية والأجهزة اللوحية

- تفعيل خصائص الأمان المتقدمة Advanced Security Settings على الهاتف الذكي والأجهزة اللوحية Tablets مثل كلمات المرور القوية والمعقدة، ميزة التحقق البيومتري (مثل التعرف على الوجه، بصمات الأصابع، وبصمة العين)، وكذلك استخدام الأنماط Patterns المعقّدة لتشديد الحماية على هذه الأجهزة.

- تفعيل ميزة تعقب الجهاز Find my Phone والإقفال التلقائي Autolock لتأمين حماية الجهاز وسهولة إيجاده في حالة الفقدان أو السرقة.

- تفعيل ميزة إقفال الجهاز تلقائياً بعد فترة قصيرة من عدم الإستخدام.

- تفعيل خاصية التحديث الأوتوماتيكي أو الدوري Automatic Update لكافة البرامج/التطبيقات، وأنظمة التشغيل OS، من أجل سد الثغرات الأمنية في البرمجيات التي قد يجري إستغلالها لإختراق جهازك.

- تجنّب التلاعب بإعدادات المصنع الخاصة بهاتفك (مثلاً: Jailbreaking أو Rooting).

- إغلاق وسائط إتصال الجهاز بشبكة الاتصالات (مثل Bluetooth, NFC, WiFi) في حال لم تكن تستخدمها.

- لا تمنح أذونات permissions للتطبيقات أو البرمجيات على الجهاز المحمول أو الهاتف الذكي إذا بدا لك أنها مبالغ فيها أو غير منطقيّة.

- تحميل التطبيقات، التي تحتاج إليها فعلياً فقط، من متاجرها الرسمية (مثل Apple Store أو Google Play Store) لتجنب إصابة الجهاز بالبرمجيات الضارة.

- إحرص على مراجعة آراء المستخدمين حول (Rating & Reviews) أداء وفعالية ومصداقية التطبيق الذي تنوي إستخدامه قبل تنزيله.

- تحميل برنامج لمكافحة الفيروسات Antivirus & Antimalware موثوق على الجهاز الهاتفي وتحديثه بشكل دوري.

- استخدام شبكة موثوق بها للإتصال بالإنترنت وتجنّب شبكات الواي فاي العامة والمجانية Public WiFi الا عند الضرورة.

- تجنّب حفظ كلمات المرور أو المعلومات الحساسة على الهاتف الذكي أو الجهاز المحمول.

- الحرص دائماً على الإحتفاظ بنسخ إحتياطية من محتوى جهازك وبياناتك الهامة (مثل جهات الاتصال، الرسائل النصية، الملفات، الصور الخاصة والفيديوهات، ودردشات برامج المراسلة وغيرها) على أقراص CD, DVD أو أقراص صلبة خارجية Hard Disk أو السحابة Cloud بهدف تقليل الأضرار التي قد تنتج عن الإصابة بأي نوع من الفيروسات والبرامج الخبيثة المطالبة بفدية أو التي قد تنتج عن تداعيات سرقة الهاتف أو الجهاز المحمول أو فقدانه.

- الحرص على محو شبكات الواي فاي العامّة التي اضطررت الى إستعمالها في فترات معينة.

- الحرص على بقاء جهازك دوماً تحت مرأى نظرك في الأماكن العامة وعدم تركه خارج متناول يديك ولو لفترة قصيرة.

- الحرص على الإحتفاظ بالرقم التسلسلي IMEI لجهاز الهاتف المحمول الخاص بك.

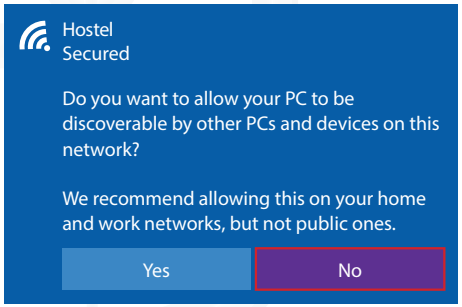
- إعادة ضبط الهاتف الذكي أو الجهاز اللوحي الخاص بك على إعدادات المصنع Wipe Data / Factory Reset قبل الإستغناء عنه لأي سبب كان.

٤.٤- إجراءات حماية شبكة الواي فاي والأجهزة المتصلة بها

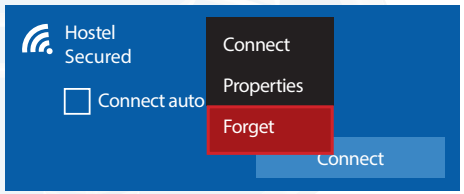
٤.٤.١- الواي فاي العامة

- تجنب الاتصال بشبكات Wi-Fi العامة: المقاهي والمطاعم والفنادق وما إلى ذلك. يبقى الإنترنت عبر الهاتف المحمول أكثر أمانًا.

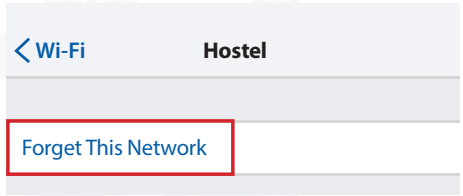
- ومع ذلك، إذا كان من الضروري لك الاتصال بشبكة Wi-Fi عامة، فاحرص على إتباع الإجراءات التالية:
  - لا تسمح للأجهزة الأخرى باكتشاف جهاز الكمبيوتر الخاص بك أثناء الاتصال.



- تجنب الاتصال التلقائي عن طريق حذف Forget شبكات Wi-Fi التي لا تنوي الاتصال بها من قائمة الشبكات الموثوقة في المستقبل.
- مثال: حذف شبكة Wi-Fi على نظام التشغيل Windows :



- مثال: حذف شبكة Wi-Fi على iPhone :



٤.٤.٢- الواي فاي الخاصة:

- الإلتزام بمعايير إختيار كلمات المرور الواردة آنفاً وتطبيقها للإتصال بشبكة الواي فاي الخاصة بك.
- مراجعة إعدادات الأمان على جهاز الواي فاي أو الراوتر Router الخاص والعمل على تغيير إسم التعريف الخاص بالواي فايSSID ، وتغيير إسم المستخدم وكلمة المرور المحددِيْن من قِبل المصنّع وتطبيق التحديثات التلقائية Automatic Updates للبرنامج الخاص بجهاز الراوتر WiFi Router.
- ضرورة تفعيل خاصية تشفير التواصل عبر شبكة الواي فاي الخاصة من خلال أحدث أنواع التشفير (حالياً WPA2/3) لحماية البيانات الصادرة والواردة من كل جهاز وتجنب سرقتها.
- إعتماد خاصية المصادقة الثنائية Two Factor Authentication على الأجهزة الإلكترونية والحسابات المتصلة بالإنترنت إذا أمكن.
- إطفاء جهاز الـ wifi Router في حال عدم استخدامه منعاً لمحاولة قرصنته.

٤.٥- إجراءات حماية المعاملات الإلكترونية والمالية

نعرض فيما يلي بعض الإرشادات والإجراءات التي تساعد المستخدمين في الحفاظ على سلامة أموالهم وبطاقاتهم الائتمانية وحماية معاملاتهم المالية والإلكترونية على شبكة الإنترنت.

٤.٥.١- إجراءات حماية المعاملات المصرفية الالكترونية

- إنجاز العمليات المصرفية الإلكترونية من خلال أجهزة حواسيب وأجهزة محمولة آمنة مزودة بأحدث البرامج Antivirus لكشف وتصحيح الثغرات الأمنية في التطبيقات وأنظمة التشغيل المثبتة عليها.
- تجنب إجراء العمليات المصرفية الإلكترونية في حال كنت متصلاً بالإنترنت بواسطة واي فاي عامة أو في حال عدم استخدام مواقع الإتصال لبروتوكول https.
- عدم الكشف عن تفاصيل حساباتك أو بطاقاتك المصرفية إلا أمام أشخاص موثوقين (مثلاً ممثلين عن المصارف، الفنادق، الخ) وكن متنبهاً للمعلومات التي تكشفها أمامهم.
- التنبّه للمعلومات التي تشاركها عبر الهاتف مع أي متصل يطلب منك تفاصيل حول حساباتك وبطاقاتك المصرفية أو عملياتك المالية.
- لا تقم بمشاركة كلمات المرور PIN وتلك التي تعطى لمرة واحدة من قبل المصرف OTP: One Time Password مع أي شخص كان حتى لو كان موظفاً في البنك وكن متأكداً ان موظف البنك لن يسألك أبداً بأية وسيلة عن الرموز الخاصة بحسابك أو بطاقتك الائتمانية.
- التأكد من حجب لوحة الأرقام عن الآخرين عند إدخال رمز المرور PIN في أجهزة الصرف الآلي أو نقاط البيع وتجنّب الكشف عنها أو إعطاءها لأي كان.

- الحذر من عملية نشل بطاقة الإئتمان الخاصة بك عندما تكون في مكان مزدحم.

- العمل على إتلاف بطاقات الإئتمان منتهية الصلاحية عبر تقطيعها الى قطع صغيرة والتأكد من تلف الشريط المغناطيسي Magnetic Stripe والشريحة Chip.

- مراجعة حساباتك المصرفية وبخاصة تلك المرتبطة ببطاقاتك الإئتمانية من وقت لآخر للتأكد من دقة وصحة العمليات المالية المنفذة وإبلاغ مصرفك عن أي معاملات أو مدفوعات مشبوهة لم تنفذها أو حتى عمليّات سحب مبالغ صغيرة من المال من حساباتك بشكل مستمر.

- ضرورة إجراء التدقيق والمصادقة الإضافية للعمليات (مثلاً معاودة الإتصال بالجهة الطالبة) بشأن أي مدفوعات تتخطى السقف المحدد.

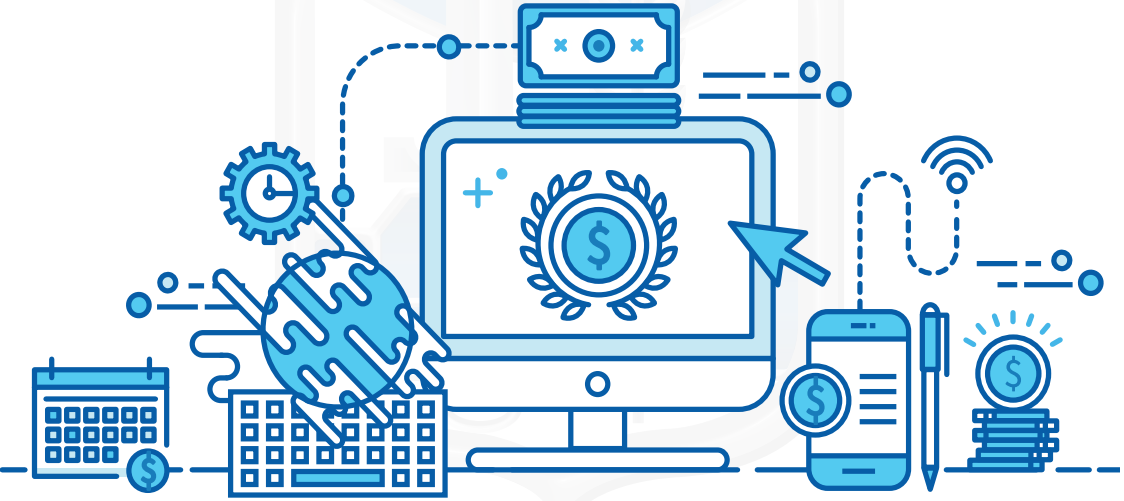
- تجنّب إدخال تفاصيل تتعلق بحسابك المصرفي بعد الضغط على رابط في رسالة الكترونية أو نصية أو بريد إلكتروني كون ذلك يمكن أن يؤدي الى سرقة بياناتك ومعلوماتك الشخصية والمصرفية.

- لا ترد مطلقا على أي بريد إلكتروني يدعي أنه من "المصرف" أو أي شركة تطلب حسابك أو معلوماتك السرية مثل كلمات المرور أو أرقام بطاقات الائتمان أو أرقام التعريف الشخصي أو أرقام التعريف الضريبية.

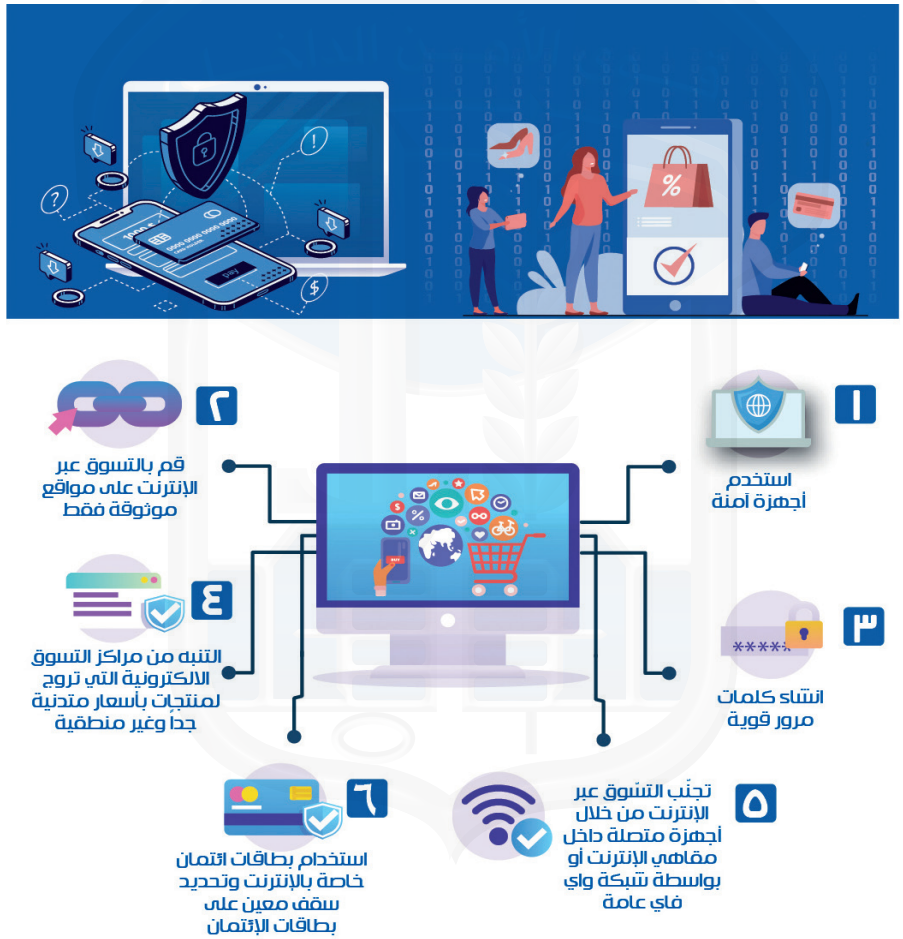
- سجل خروجك Logout فور الانتهاء من استخدامك للخدمات المصرفية عبر الإنترنت.

حماية الأموال والمعاملات الإلكترونية والمصرفية

- ✓ استخدم أجهزة آمنة لاجراء معاملاتك الالكترونية والمصرفية
- ✗ عدم إجراء العمليات المصرفية الإلكترونية في حال كنت متصلاً بالإنترنت من خلال شبكة واي فاي عامة
- ✗ لا تشارك عبر الهاتف أو في رسالة الكترونية أو رسالة نصية أو روابط الكترونية أي تفاصيل حول حساباتك وبطاقاتك المصرفية أو عملياتك المالية
- ✓ احرص على استخدام الموقع الالكتروني الرسمي الحقيقي للمصرف (انتبه الى الروابط المشبوهة التي قد تردك وتوهمك بأنها تعود اليه)
- ✓ انشاء كلمات مرور قوية
- ✗ لا تجاوب على الرسائل أو الاتصالات المشبوهة
- ✗ لا تقم بمشاركة كلمات المرور أو اسم المستخدم أو رمز PIN
- ✓ إجراء التدقيق والمصادقة الإضافية للعمليات المالية



٤.٥.٢- إجراءات التسوق الآمن عبر الانترنت
Online Shopping



- لا تقم بالتسوق عبر الإنترنت سوى على مواقع موثوقة وتتضمن توفير إمكانية تأمين اتصالاً آمناً ومشفراً بالإنترنت (https أو علامة القفل 🔒 .)
- التنبه من وسائط الاتصال المريبة الخاصة بخدمة الزبائن في مراكز التسوق الالكترونية (مثلاً عنوان البريد الالكتروني الخاص بخدمة الزبائن supportcompany@gmail.com بدلاً من support@company.com).
- التنبه من مراكز التسوق الالكترونية التي تروج لمنتجات بأسعار متدنية جداً وغير منطقية مما يرجح أنها تستعمل للقيام بعمليات إحتيال، ومن عناوين التسوق الالكتروني المثيرة للريبة مثل «brands-at-awesome-price.com» إذ قد يكون هدفها تنفيذ عمليات التصيد الاحتيالي.
- تجنّب القيام بعمليات التسوق عبر الإنترنت من خلال روابط معينة ترد ضمن بريد الكتروني (مثلاً رسالة الكترونية هدفها التصيد الاحتيالي تتضمن عرضاً وهمياً لمنتج مرغوب مع زرّ «اشترِ الآن»).
- تجنّب التسّوق عبر الإنترنت من خلال أجهزة متصلة داخل مقاهي الإنترنت أو بواسطة شبكة واي فاي عامة.
- إحذر من توفير معلومات تتخطى المعلومات الضرورية لإنجاز عملية الشراء عبر الانترنت.
- ينبغي التمعّن في الآراء الواردة من قبل المستهلكين السابقين الذين مرّوا بتجربة إيجابية أو سلبية لدى تعاملهم مع نفس الموقع أو البائع أو المنتج.
- ضرورة تحديد سقف معين على بطاقات الإئتمان للمبالغ المسموح سحبها أو الشراء بها في وقت واحد. ومن الممكن استخدام بطاقات ائتمان خاصة بالإنترنت (Internet credit card) أو مسبقة الدفع (Prepaid).
- ينبغي عدم حفظ أي تفاصيل تتعلق ببطاقات الإئتمان الخاصة على مواقع التسوق الالكتروني.

٤.٥.٣- إجراءات الحماية من الإحتيال المالي عبر البريد الالكتروني الخاص بالعمل Business Email Compromise

- ضرورة القيام بتحليل دقيق لمختلف الرسائل الالكترونية لاسيما تلك التي تتعلق بطلبات التحويل المالي والطلبات غير المألوفة الصادرةعن المدراء التنفيذيين.
- ضرورة وضع آليات وتدابير صارمة خاصة بالتحويلات المالية التي ترد من طلبات عبر البريد الالكتروني قبل إرسال أي بيانات أو تحويل اي أموال مثلاً:
  - التحقق دوماً من الفاتورة.
  - التحقق والتثبت من تفاصيل الدفع الخاصة بالمرسل إليه.
  - التأكد من المدير التنفيذي، أو المحامي أو شركة التأمين... بخصوص أي طلب يتعلق بتحويلات مالية.
- التدقيق في الرسائل الالكترونية التي تتضمن اخطاء إملائية أو طلبات غير معتادة لاسيما إذا كانت المهلة المعطاة للدفع أو التحويل قصيرة.
- التحقق جيداً من عنوان البريد الاكتروني الخاص بالمرسل كونه في معظم الأحيان يكون البريد الالكتروني الخاص بالمقرصن يتضمن حرفاً مغايراً أو حرفاً إضافياً.
- التثبت من طلبات تعديل الدفع عبر الاتصال بالطرف المعني من رقم هاتف معروف سابقاً وليس ذاك المشار اليه في عنوان البريد الاكتروني الذي يتضمن الطلب.
- الطلب إلى المرسل إرسال التعديلات المتعلقة بطريقة الدفع الجديدة بواسطة رسالة تحمل شعار الشركة والتثبت من صحة هذا الشعار.
- التحقق من أي تغييرات في تفاصيل الدفع الخاصة بالبائع من خلال استخدام توقيع ثانٍ لأحد موظفي الشركة.

0- كيفية التعامل مع الجرائم السيبرانية

نعرض فيما يلي كيفية التصرف في حال التعرّض لخطر أو جريمة سيبرانية:

0.1- كيفية التصرف عند سرقة أو فقدان الهواتف الذكية والأجهزة المحمولة

في حال سرقة أو فقدان جهازك المحمول أو هاتفك الذكي، بإمكانك اتخاذ سلسلة من الخطوات الهامة، بعضها مرتبط بما تم إتخاذه من إجراءات الأمان على الأجهزة المحمولة وفقاً لما ورد سابقاً في هذا الدليل.

في هذه الحالة:

- حاول بداية الاتصال بالهاتف المحمول من رقم آخر، لتحديد ما إذا كان بالإمكان سماع صوت الرنين.

- اذا قمت سابقاً بتفعيل ميزة تعقب الجهاز Find My Device (على الروابط android.com/find للأندرويد أو icloud.com/find للأيفون)، قم بما يلي:

أ. تحقق من موقع الجهاز على التطبيق وشغل التنبيه (alarm) في حال كان الموقع قريباً
ب. لا تذهب الى موقع الجهاز في حال كان بعيداً بل بلغ قوى الأمن الداخلي على الفور.

ج. إستخدم ميزة تأمين الجهاز Lock Device أو Secure Device، التي تمكنك من إقفال هاتفك عن بعد كي لا يتمكن احد من الوصول إلى محتويات الهاتف. ولهذه الغاية، يمكنك عرض رسالة من اختيارك على شاشة القفل توضح ان الجهاز مفقود.

- إذا كنت تحتفظ ببيانات بطاقاتك الائتمانية داخل المتصفح أو في أحد التطبيقات الموجودة على الهاتف؛ يجب عليك الاتصال فوراً بالمصرف لإخباره بمنع التعامل بهذه البطاقات وإصدار غيرها ، وإذا كنت تستخدم خدمات الإنترنت المصرفي من الهاتف فعليك أن تطلب التغيير الفوري لكلمات المرور إذا لم يكن في مقدورك فعلها بنفسك.

- ينبغي تغيير كل كلمات المرور العائدة لمختلف الحسابات المرتبطة بهاتفك ولعل الأهم تغيير كلمة المرور الخاصة بمتاجر التطبيقات كي لا يتمكن أحد من القيام بعمليات شراء مختلفة.

- إبلاغ سلطات إنفاذ القانون المحلية بفقدان الجهاز أو سرقته واعطائهم الرقم التسلسلي للجهاز IMEI في حال تم طلب ذلك.

- إحرص على الإتصال بمركز خدمة الزبائن لدى شركة الهاتف لوقف العمل برقم هاتفك وتعليق كافة الخدمات.

- العمل على تسجيل الدخول من خلال جهاز آخر تملكه إلى كافة الخدمات والحسابات التي سبق واستخدمتها من هاتفك المسروق واحرص على الضغط على خيار تسجيل الخروج من جميع الأجهزة الأخرى "Logout from all other devices" من أجل تعطيلها على الجهاز المسروق.

٥.٢- كيفية التصرف عند التعرض لعمليات الإبتزاز الإلكتروني

في حال التعرّض لعملية ابتزاز وعدم التأكّد مما يجب القيام به، عليك باتباع هذه الخطوات:

- التزام الهدوء وعدم اتخاذ أي قرار منفرداً. تحدّث إلى شخص تثق به، أحد الأصدقاء أو أحد أفراد العائلة.
- لا تقم بإيذاء نفسك أو الآخرين أبداً، لأن أجهزة الشرطة موجودة للمساعدة وتعمل على الحدّ من الجرائم ومعاقبة مرتكبيها.
- قم بتصوير وحفظ كافة الأدلة ومضمون المراسلات ورسائل البريد الإلكتروني ذات الصلة بعملية الإبتزاز بحيث يمكنك إظهار الأدلة للشرطة في وقت لاحق.
- عدم التواصل مع الشخص المبتز، حتى عند التعرض للضغوطات الشديدة.

- عدم الرضوخ لطلبات المبتز مثل تحويل أي مبالغ ماليّة، الإفصاح عن رقم بطاقة البنك، أو تلبية أي طلب كان إذ قد يؤدي ذلك الى زيادة الضغوط لتلبية طلبات إضافية.
- تجنّب المشادات مع المبتز وقم بالإبلاغ عن محاولات الابتزاز أو التنمّر التي تتعرض لها عند وقوعها لدى جهات إنفاذ القانون دون أن توجه للمبتز أي تلميح عن رغبتك في القيام بذلك.
- الاستمرار في التواصل مع المبتز للعمل على تعقب مكانه أو لجمع دليل اضافي لعملية الابتزاز إذا طُلِب منك ذلك.

٥.٣- كيفية التعامل مع التنمر الإلكتروني Cyberbullying

- إحرص على عدم الإنتقام وعدم الإستجابة.
- قم بتجميع كافة الأدلة وإحتفظ برسائل الهاتف المحمول ورسائل البريد الإلكتروني أو دردشات شبكات التواصل الإجتماعية، وقم بالحديث إلى شخص تثق به، أحد أفراد الأسرة أو أحد الأصدقاء.
- قم بالإبلاغ عن حادثة التنمّر واتبع نصائح الشرطة في ما خصّ:
  - حجب الشخص الذي يقوم بالتنمر وتغيير إعدادات الخصوصية لديك من أجل الحدّ من امكانية الوصول الى بياناتك ومنشورات حساباتك من قبل الغرباء.
  - الإبلاغ عن الإساءة من خلال الخدمة المخصصة لذلك على التطبيق.

٥.٤- كيفية التعامل مع الحسابات المسروقة لمختلف مواقع التواصل الاجتماعي، تطبيقات المراسلة النصية، أو مزودي الخدمات

يعمد المجرم السيبراني أحياناً إلى إحداث بعض التغييرات من حين إلى آخر على الحسابات العائدة لمواقع التواصل الإجتماعي (Facebook, YouTube, Instagram, Twitter, WhatsApp, Gmail, Snapchat,...) التي يصعب ملاحظتها بسهولة من قبل المستخدم والتي تدعو إلى الريبة. ومثال ذلك:

- عدم التمكن من تسجيل الدخول بواسطة كلمة المرور الخاصة بك.
- إضافة/حذف صداقات أو طلبات متابعة أو إعجابات أو خيارات لم تقم بها.
- تحديث الحالة Status أو إجراء تغريدات/بوستات لم تقم بها.
- تحميل صور دون علمك.
- توجيه رسائل إلكترونية خاصة ومزعجة إلى أصدقائك.
- تعديل صفحة التعريف الرئيسية (البروفايل أو الصور) الخاصة بحساباتك دون علمك.
- تلقي رسائل الكترونية أو إشعارات غير منتظرة من قبل إدارة مواقع التواصل الاجتماعي مثال على ذلك أنه قد تم تغيير عنوان بريدك الالكتروني.

يمكنك في حال حدوث اي من الحالات السابقة، القيام بالخطوات التالية للحد من الأضرار التي يمكن للقراصنة أن يتسببوا بها والعمل على استعادة حسابك المسروق:

- حاول تسجيل الدخول باستخدام جهاز آخر لتعرف إذا كنت قد فقدت إمكانية الدخول بالفعل، واحرص أيضاً على التحقق عدة مرات من كلمة المرور التي تقوم بإدخالها.

- حاول التأكد من وصول أي تحذير على شكل بريد إلكتروني من المواقع والخدمات الإلكترونية بشأن حدوث نشاطات مريبة في حسابك (مثل محاولة شخص ما تسجيل الدخول الى أحد حساباتك من حاسوب غير مألوف أو من مكان غير مألوف، أو قيام شخص ما بتغيير إسم المستخدم أو كلمة المرور الخاصة بك).

- قم بالدخول إلى صفحة الدعم المخصصة للمساعدة عبر الموقع الرسمي (Snapchat, Gmail, Instagram) .كما يمكن أيضاً إرسال بلاغ لمشكلة الحساب التي تواجهها وطلب المساهمة في حظره (Twitter, Facebook).

- إتبع التعليمات التي يقدمها الموقع أو الخدمة لإسترداد الحساب. وفي هذه الحالة قد تضطر لتأكيد رقم هاتفك، أو عنوان البريد الإلكتروني الإحتياطي، أو الإجابة عن الأسئلة الشخصية لكي تثبت أنك صاحب الحساب الحقيقي.

- إذا تم سرقة حساب (WhatsApp, Telegram, Signal,..) قم بحذف التطبيق من جهازك، وأعد تحميله من جديد مع المصادقة من خلال الرسالة النصيّة أو الاتصال. وبذلك سوف يتم تعطيل الحساب من جهاز المقرصن، ويتفعل الحساب في جهازك من جديد.

- بعد أن تتمكن من تسجيل الدخول الى حسابك مرة أخرى، قم مباشرة بتغيير كلمة المرور الخاصة به والتأكد من كافة المعلومات الشخصية والإعدادات الأخرى لعدم حدوث اي تغيير في رقم الهاتف، وعنوان البريد الإلكتروني الاحتياطي، والأسئلة الشخصية...

- الحرص على عدم استخدام أي كلمة مرور مستخدمة سابقاً.

- العمل على تغيير كلمات المرور العائدة للحسابات الأخرى إن كنت تستخدم كلمة المرور القديمة للدخول الى حسابات متعددة، علماً ان هذا الأمر لا ينصح به على الاطلاق.

- قم بعد ذلك بتسجيل الخروج من كافة جلسات الإتصال الأخرى بإستثناء جلسة الإتصال الحالية التي تستخدمها (Logout From All Other Sessions).

- قم بمراجعة وتفعيل خصائص الحماية الإضافية في حساباتك مثل خاصية المصادقة الثنائية (كلمة مرور + رمز يتم إرساله الى هاتفك الخليوي) Double Factor Authentication بالإضافة الى ميزات الأمان الأخرى التي صممت لمنع التعرض للهجمات (مثال: يتيح لك فايسبوك إضافة قائمة من الأصدقاء الموثوقين الذين يمكنهم تأكيد صحة هويتك في حال تعرض حسابك للإختراق من جديد).

- إذا لم تستطع إسترداد حسابك، تواصل مع أصدقائك وكافة جهات الاتصال على حسابك وأبلغهم بأن حسابك قد تعرض للقرصنة أو للإبتزاز محذراً إياهم من عدم قبول أي رسالة منه أو الدخول الى أي رابط يصلهم منه، والإبلاغ عن الحساب المسروق من خلال إدارة الموقع مما يساهم في حظر الحساب.

0.0- كيفية التصرف عند الإصابة بالبرمجيات الخبيثة Malware

هناك مجموعة من المشاكل التي تطرأ على عمل أجهزة الكمبيوتر وتوحي بأنها أصيبت بفيروسات وبرمجيات خبيثة ومنها البطئ الشديد، استهلاك شحن الجهاز بسرعة كبيرة، الخروج عن السيطرة، حذف الملفات، عدم وجود الملفات بالترتيب المعتاد ، تعطل بعض الخدمات والوظائف في الجهاز، عمل بعض التطبيقات بشكل تلقائي وغير إعتيادي.

في هذه الحالة، ينبغي اتخاذ الإجراءات التالية لمعالجة المشكلة.

- في حال عدم توفر نسخة إحتياطية، قم بنقل البيانات والملفات الهامة الخاصة بك على ذاكرة تخزين يو إس بي (USB) أو قرص صلب خارجي، مع الأخذ بعين الإعتبار أن هذا قد يصيب القرص الصلب أو ذاكرة تخزين USB التي استخدمتها لتخزين الملفات التي قد تكون مصابة بدورها.
- قم بفصل الجهاز عن شبكة الإنترنت.
- مستخدماً جهاز آخر، قم بتغيير جميع كلمات المرور لحساباتك على الإنترنت.
- قم بوضع جهازك في وضعية نظام الآمان Safe mode واعمل، من خلال نظام التشغيل على فحص القرص Check Disk وتنظيفه Disk Cleanup
- قم بمسح شامل وتنظيف جهازك بواسطة برنامج مضاد للفيروسات Antivirus واتبع النصائح والإرشادات التي يقدمها لك.

في حال لم ينجح البرنامج المضاد للفيروسات بإزالة ومحو البرمجيات الخبيثة عليك بما يلي:

- قم بإجراء عملية (Format) لجهاز الكمبيوتر المصاب وإعادة تنزيل نسخة أصلية من نظام التشغيل مثل ويندوز Windows، أو لينوكس Linux أو ماك macOS ، وبهذه الطريقة، تكون متأكداً من أن جهازك أصبح خال من الملفات الخبيثة.
- قم بتحميل وتنصيب برنامج مكافحة فيروسات موثوق وقوي ومن مصدره.
- قم بتحديث نظام التشغيل وقاعدة بيانات برنامج مكافحة الفيروسات Antivirus Updates وتأكد من أن التحديث قد تم بنجاح قبل فحص البيانات من أحدث عملية نسخ احتياطية في حال وجودها أو تلك التي قمت بنقلها إلى القرص الخارجي أو ذاكرة تخزين اليو إس بي في الخطوة الأولى.
- قم بنقل البيانات مجدداً الى جهازك.
- قم بفحص الجهاز وبياناتك باستخدام مضاد الفيروسات المحدث دوريّاً.

0.1- كيفية التصرف عند إصابة الأجهزة ببرمجيات «الفدية» الخبيثة Ransomware

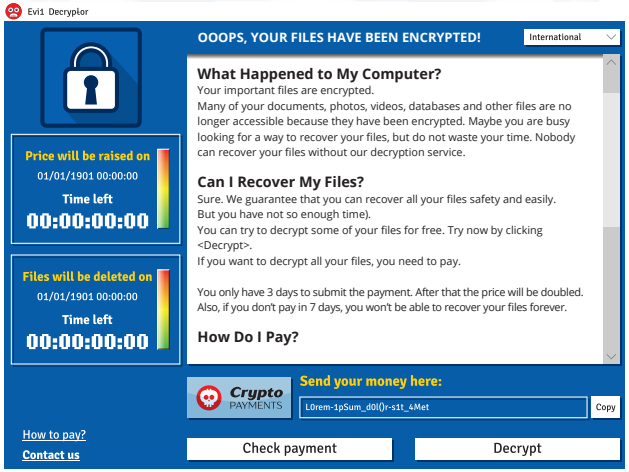
عند إصابة جهاز الكمبيوتر أو الهاتف الذكي بهذا النوع من البرمجيّات، ننصح بعدم تنفيذ تعليمات القراصنة بدفع المبلغ المطلوب أو الفدية كونه:

- لا يوجد ضمانات على الإطلاق بأنك ستسترجع بياناتك لأن هدف منتجي هذه البرامج هو جمع المال فقط.
- سيبقى جهازك مصاباً بالفيروس الخبيث ما لم تقم بعملية مسح وتنظيف شاملة للجهاز.
- سيستمر القراصنة بإبتزازك وطلب المزيد من المال أو سيعمدون الى محاولة مهاجمتك مجدداً لحملك على دفع فديات أخرى في المستقبل.
- ستساهم بشكل أو بآخر بتمويل الجماعات الإجرامية.
- سوف تساهم في تشجيع هؤلاء المجرمين على تطوير هذه البرمجيات وربما إستهدافك بها مرة أخرى.

بل يُنصح في هذه الحالة القيام ببعض الخطوات لتنظيف الجهاز وإعادته إلى وضعه الطبيعي على الشكل التالي:

- حاول تحديد نوع فيروس الفدية فإما أن يكون فيروس إقفال الشاشة Blocker/Locker ، أو فيروس تشفير الملفات Cryptor.
- في حال كنت غير قادر على تخطي الإشعار الظاهر على الشاشة أمامك الذي ينذر بوجود فيروس، ستكون على الأرجح مصاباً بفيروس إقفال الشاشة، أما اذا تخطيته ولم تستطع الولوج الى بعض أو كل الملفات الخاصة بك تكون مصاباً بفيروس تشفير الملفات.

- في حال كنت قادراً على تصفح النظام وقراءة معظم الملفات دون أي مشكلة، ستكون عندها أمام محاولة لإيهامك بأنك ضحية لكي يتم إجبارك على دفع مبلغ من المال وذلك من خلال وضع صورة معيّنة على خلفية الشاشة Desktop Background.
- في حال الإصابة بفيروس تشفير الملفات،
  - إفصل جهازك عن الأجهزة الأخرى وعن أي أقراص خارجية.
  - استخدم كاميرا لتصوير الإنذار بوجود فيروس الذي يظهر على الشاشة وإبلاغ الشرطة بذلك.
  - حاول استرداد بعض الملفات المشفرة باستخدام برامج فك تشفير مجانية التي من الممكن ان تكون مفيدة مع انواع معينة من فيروسات الفدية.
  - استخدم برنامج مضاد للفيروسات وقم بمسح Scan لمحاولة التخلص من فيروس الفدية من جهازك. مع هذا الحل ربما لن تستطيع إسترجاع ملفاتك المشفرة، ولكنك ستكون متأكداً من عدم وجود أي برمجيات خبيثة.



- تحقق إذا كنت قادراً على استعادة الملفات التي تم مسحها. فبعض أنواع الفيروسات المشفرة تقوم بنسخ ملفاتك وتشفير النسخ ومن ثم تلغي الملفات الأصلية. في هذه الحالة ممكن استعادة الملفات الممسوحة باستخدام تطبيقات مجانية مثل ShadowExplorer.

- حاول استخدام بعض التطبيقات التي تساعد في تحديد نوعية وإسم الفيروس المشفر الذي تقوم بالتعامل معه مثال Crypto Sheriff أو أداة ID Ransomware أو غيرها...

- تحقق من وجود أداة لفك التشفير وذلك من خلال البحث على موقع "nomoreransom.org".

- في حال لم تنجح في تعطيل وفك فيروس الفدية، قم بإرجاع جهازك إلى آخر نسخة تم أخذها Restore Point وفي حال فشل ذلك إرجاعه إلى إعدادات المصنّع Restore Factory Settings وقم بتحميل نظام التشغيل من جديد ومن ثم استعادة ملفاتك من النسخ الاحتياطية التي أنشأتها سابقاً.

- أما بالنسبةِ لفيروس إقفال الشاشة Screen-locker، فإن عملية إسترجاع أو إستعادة النظام ستكون كافية للوصول إليه من جديد. اما إذا لم ينجح ذلك، فالحل سيكون باستخدام قرص قابل للتشغيل قبل إقلاع الجهاز (Rescue CD) والقيام بعملية مسح (Scan).

٥.٧- كيفية التصرف عند سرقة أو فقدان البطاقة الإئتمانية

عند الشك في حصول سرقة أو فقدان أو إختراق لبطاقتك الائتمانية أو استخدامها دون موافقتك أو علمك، ينبغي إتباع الإجراءات التالية:

- الاتصال مباشرة بالجهة التي أصدرت بطاقة الإئتمان من خلال قنوات التواصل الموثوقة مثل الإتصال بخدمة العملاء هاتفياً والإبلاغ عن سرقة أو فقدان بطاقتك لكي تتخذ الإجراءات اللازمة لتجميدها وطلب إستبدالها.
- مراجعة كشف حساب البطاقة لضمان عدم إدراج أي عمليات غير نظامية لا يفترض تحملها، والتأكد من عدم وجود أي رسوم أو تكاليف إضافية على العمليات غير النظامية. وفي حال لوحظ وجود أي تكاليف غير اعتيادية ينبغي تقديم إعتراض للجهة المصدرة للبطاقة في أسرع وقت ممكن للقيام بالإجراءات اللازمة لإسترداد المبلغ.
- إستلام بطاقة الإئتمان الجديدة من الجهة التي أصدرتها وإتخاذ إجراءات الأمان والحماية المذكورة آنفاً.
- العمل على تحديث حافظتك المحمولة Mobile Wallet وجميع حساباتك على مواقع التسوق عبر الإنترنت في حال كانت البطاقة المفقودة تستخدم كوسيلة للدفع.

٥.٨- كيفية التصرف في حال التعرّض للإحتيال المصرفي على الإنترنت

عند الشك في أنك وقعت أو كدت تقع ضحية أي عملية إحتيال مصرفي أو مالي، ينبغي القيام بالخطوات التالية:

- الإبلاغ فوراً عن ذلك من خلال الإتصال بالجهة المعنية بعمليات الاحتيال في المصرف الذي تتعامل معه لإتخاذ الإجراءات اللازمة.
- تغيير كلمة سر حسابك المصرفي في الموقع أو في تطبيق الهاتف.
- توثيق تاريخ وزمان اكتشاف/إبلاغ عن وقوع عملية الاحتيال، وغيرها من الملاحظات ذات الصلة.
- مراقبة الحساب المصرفي وتوثيق أي عملية مصرفية مشبوهة تتم على حسابك وذلك للاثبات القانوني.
- حاول أن تسجّل ما الذي قد حصل؟ من هو منفذ هذا العمل؟ هل لا تزال العملية متواصلة؟ متى حصل ذلك؟ ما هي قيمة الخسائر أو الخسائر المحتملة؟
- قم بتحديد مختلف الأدلة المرتبطة بالعملية فضلاً عن الفواتير والعقود وأوامر الشراء والشيكات، الخ.

٦- الإتصال بقوى الأمن الداخلي لطلب المساعدة

إنّ قوى الأمن الداخلي تحرص على الحفاظ على السرية التامّة في التحقيقات التي تجريها في الجرائم السيبرانية، ولن توفّر أيّ جهد لمساعدتك في حلّ المشكلة التي تواجهها.

بلّغ قوى الأمن الداخلي عن أيّ جريمة سيبرانية، أو أيّ تهديد أو خطر سيبراني قد تواجهه من خلال إحدى الوسائل الآتية:

- مكتب مكافحة جرائم المعلوماتية وحماية الملكية الفكرية:
  ٠١/٢٩٣٢٩٣
- خدمة **بلّغ** على موقع قوى الأمن الداخلي الالكتروني:
  www.isf.gov.lb

قوى الأمن الداخلي

شعبة العلاقات العامة

خدمة - ثقة - شراكة

اعداد:
لجنة دراسة المخاطر السيبرانية وتأمين وسائل الحماية منها
تشرين الثاني ٢٠٢٠

مشروع ممول من الاتحاد الأوروبي