قضية

المحامي منير الشدياق
mounirchidiac2014@gmail.com

بعد استحداثه قبل سنوات شُعبًا متخصّصة بمكافحتها

الأمن العام يطلق حملة توعية للحماية من الجرائم السيبرانية

نطاق سيادة الدولة كان مقتصرا في الماضي على ثلاثة عناصر: الارض والبحر والفضاء المادي. لكن عصرنا الالكتروني فرض وجود عنصر سيادي رابع هو الفضاء السيبراني الذي اصبح مسرحا للمعلومات والمحاولات الجرمية التي لا يمكن حمايتها والتصدي لها بالاسلحة التقليدية، بل حصرا عبر الثقافة الشخصية وبرامج الحماية وقوى امنية الكترونية كالتي استحدثها الامن العام

في ايار 2019، اطلقت المديرية العامة للامن العام حملة توعية على مخاطر الفضاء السيبراني تحت شعار "حتى ما تكون ضحية". الحملة ستشمل في المرحلة المقبلة محاضرات يلقيها ضباط من الامن العام في مختلف المدارس والجامعات، مع حملة اعلامية عبر مختلف وسائل الاعلام، واقامة نشاطات متنوعة بالتعاون مع مختلف هيئات المجتمع المدني والادارات الرسمية المعنية، تهدف الى توعية المواطنين، المستخدمين لأي من الوسائل الالكترونية كالهواتف الذكية والكومبيوتر وغيرها، على ابرز تقنيات ووسائل حماية انفسهم واجهزتهم من كل الجرائم السيبرانية، كسرقة الاسرار الشخصية، الابتزاز الالكتروني، تجارة المخدرات والسلاح، الاتجار بالبشر، تجنيد العملاء، الارهاب الالكتروني وسواها.

سبق وعرضنا في "الامن العام" (عدد رقم 59) وعلى الموقع الالكتروني الخاص بالمديرية العامة للامن العام كل الاطر التاريخية والواقعية والقانونية والامنية، المحلية والدولية للجرائم السيبرانية. اليوم، سنتوقف عند ابرز الوسائل التقنية - العملانية التي تساعد المواطنين على حماية انفسهم واجهزتهم الالكترونية من تلك الجرائم، وفقا للآتي:

كلمة المرور (Password)

كلمة المرور (Password) هي آلية تعريف للمستخدم (User). تعد من اهم وسائل حماية البيانات كونها تعتبر القفل على الخزينة الالكترونية لما تقوم به من حماية للمعلومات وانظمة التشغيل الخاص بالمستخدم.

مميزات كلمة المرور القوية: طويلة - معقدة - غير شخصية - عملية - سرية - سهلة الحفظ. لتحقيق هذه المميزات يجب اتباع الخطوات التالية:

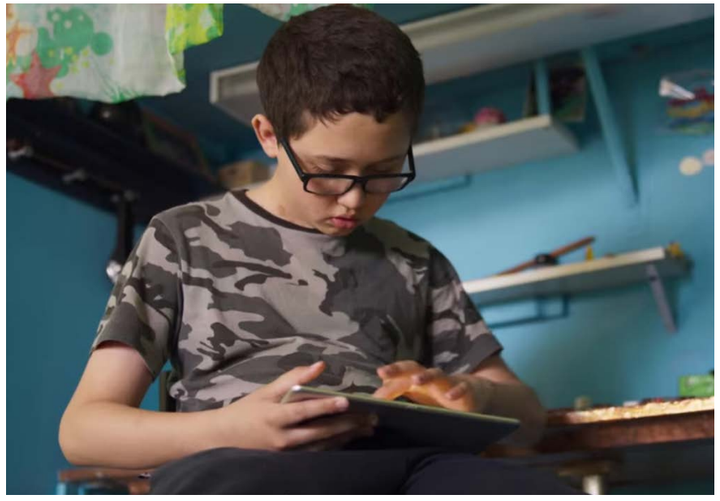
- اختر كلمات مرور قوية تتألف من مجموعة من الاحرف الابجدية الصغيرة والكبيرة، اضافة الى الرموز والارقام مثل: k@b2oL3z.
- تغيير كلمة المرور التابعة لحساباتك الشخصية دوريا (كل ثلاثة اشهر تقريبا او اقل).
- عدم الافصاح عن كلمة المرور الخاصة بك لأي كان.
- عدم استخدام كلمة مرور واحدة لحسابات عدة.
- تجنب استخدام كلمات من حروف متسلسلة او مكررة مثل: 12345678- 222222- abcdefg.
- تجنب استخدام كلمات من معلومات شخصية مثل الاسم وتاريخ الميلاد، او معلومات مماثلة: مثلا سعيد 1990/9/23.

الاجهزة الالكترونية (Electronic Devices)

ثمة طرق عدة تمكن المخترقين من الوصول الى اجهزة الضحية، وتهدف الى خرق البيانات الشخصية السرية والاطلاع عليها. في ما يلي بعض الحلول الوقائية لتفادي الوقوع ضحية المخترق (Hacker):

- وضع كلمة سر قوية لتشغيل الجهاز، كتلك التي اشرنا اليها انفا.
- عدم الاتصال بشبكة واي فاي مفتوحة.
- استخدام برامج مضادة للفيروسات (Antivirus) لكشفها والقضاء عليها.
- القيام بعملية المسح الالكتروني للجهاز دوريا (Scansystem).
- تحديث البرامج المضادة للفيروسات دوريا (Update).

الفضاء السيبراني من عناصر سيادة الدولة.



دور الاهل اساسي في حماية اطفالهم.

- عدم الاعتماد على برامج مضادة للفيروسات منتهية الصلاحية.
- الحذر من الاجهزة المشتركة او العامة المستخدمة من جميع المواطنين.
- تفعيل خاصية اغلاق الهاتف اوتوماتيكيا بعد بضع دقائق.
- عدم ادخال اي حافظة (Flash Memory) او كابل USB مجهول المصدر في الجهاز.
- الحرص على ايقاف تشغيل خدمة الواي فاي (Wi-fi) في حال عدم الاتصال بشبكة موثوق بها.
- تجنب الاتصال بشبكات الواي فاي العامة (الفنادق، المطارات، المقاهي...)، اي (Public Wi-fi).
- عدم الاتصال بجهاز بلوتوث (Bluetooth) غير موثوق به.
- الحرص على ايقاف تشغيل برنامج البلوتوث في حال عدم استخدامه.
- القيام باعادة ضبط المصنع (Factory Reset) قبل بيع اي جهاز والتأكد من مسح جميع البيانات (clear data).
- التأكد من ايقاف تشغيل خاصية تحديد الموقع (Location/GPS) في حال عدم استخدامها.
- تفعيل ميزة تحديد مكان الهاتف في حال فقدانه او سرقته.

> **توجيهات اللواء ابراهيم قضت باعطاء اهتمام استثنائي لحماية الاطفال**

(findmyiphone-android device manager)

متصفح الانترنت (Web Browser)

على الرغم من اهمية متصفحات الانترنت firefox,chrome وغيرها، الا انها ليست آمنة بما يتناسب مع حساسية المعلومات المتبادلة وخصوصيتها. لذلك نقدم ابرز خطوات الحماية:

- تحقق دائما من اعدادات متصفح الانترنت لديك وقم بتحديثه باستمرار.
- عند استخدامك المتصفح شغل private browsing كي لا تترك اثرا بعد الانتهاء.
- اختر دائما اشارة (x) الموجودة على زاوية النوافذ المنبثقة (pop-up screen)، ولا تضغط ابدا على نعم او قبول او حتى الغاء، لانها قد تكون خدعة لتحميل برامج خبيثة على جهازك.
- قبل ادخال معلومات حساسة على صفحة الويب، تأكد من وجود اشارة القفل على المتصفح او كلمة https التي تعني ان الموقع رسمي ومحمي، وليس كلمة http التي تعني ان الموقع غير رسمي وغير محمي.
- الضغط على رمز القفل للتأكد من الصلاحية (Certificate).

البريد الالكتروني (Email)

يزداد استخدام البريد الالكتروني يوما بعد يوم بهدف نقل الرسائل النصية، ارسال المستندات وتبادل المعلومات التي تعتبر حساسة وغاية في الاهمية. الا ان البريد الالكتروني كغيره من وسائل الاتصال عرضة ايضا للكثير من الثغر الامنية. لذا يجب رفع مستوى امنه عبر اتخاذ خطوات اساسية للحماية، ابرزها:

- الاعتماد على خاصية التوثيق بخطوتين لحماية البريد الالكتروني (Two Factor Authentication).
- عدم فتح اي رسالة الكترونية او ملف مجهول المصدر (spam).
- حذف او عدم الرد على الرسائل الملتبسة او الرسائل التي تطلب منك ادخال البريد الالكتروني وكلمة المرور.
- الحرص على الدخول الى حسابك الشخصي دوريا (مرة كل اسبوع على الاقل).

حماية المعلومات (Data Privacy)

يعتمد امن المعلومات الشخصية وحمايتها على مجموعة مبادئ اساسية لا بد من الالتفات اليها، وهي:

- نسخ احتياطي (backup) للمعلومات المهمة على مخزّن (harddisk/flash memory) غير موصول على الانترنت (offline).
- عدم مشاركة معلومات اكثر من المطلوب.
- عدم نشر معلومات شخصية على الانترنت.
- عدم مشاركة عنوان بريدك الالكتروني الاساسي او اسمك الخاص بالرسائل الفورية، الا مع الاشخاص الموثوق بهم.
- عدم ادراج عنوان بريدك الالكتروني او اسمك في دلائل الانترنت او في مواقع وظائف العمل الموثوق بها.
- مراقبة ما يكتبه الاخرون عنك على مواقع التواصل الاجتماعي. ◄

- عدم السماح للاخرين بنشر صورك او صور عائلتك من دون موافقتك.
- عدم مشاركة اي حافظة (USB) الا اذا كانت للقراءة فقط (read-only) اي انها غير قابلة للتعديل.
- تجنب استخدام اي حافظة، الا اذا كنت واثقا من المصدر.

الحسابات المصرفية (Banking Accounts)

على الرغم من اجراءات الامان والتامين التي تعمل المصارف على تطبيقها، الا انها دائما ما تكون هدفا وعرضة للمخترقين والقراصنة الذين يسعون جاهدين، بكل الاساليب، للحصول على المال بوسائل غير شرعية. لذلك يتوجب على المستخدم التزام التالي:
- المحافظة على سرية رقم حسابك، اسم المستخدم وكلمة المرور.
- التنبه من عمليات الاحتيال الالكترونية، وتجاهل الرسائل التي تطلب منك رقم حسابك او كلمة المرور.
- تغيير كلمة المرور التابعة لمصرفك الالكتروني وبطاقاتك المصرفية (visa card- master card) دوريا بهدف منع اختراقها.
- تحديث تطبيقات الخدمات المصرفية الالكترونية.
- تجنب استخدام كلمة السر نفسها في المواقع المصرفية ومواقع التواصل الاجتماعي.
- عند اجراء عمليات الشراء عبر الانترنت، تأكد من قراءة الخصوصية الالكترونية (licence) للشركة.
- عدم مناقشة بياناتك الشخصية او المصرفية خلال اي مكالمة مريبة تصلك.
- تفادي اجراء اي معاملة مالية الكترونية الا عند الضرورة.

التطبيقات (Applications)

على الرغم من اهمية التطبيقات الذكية المستخدمة يوميا لاهداف متعددة، الا انه ينبغي الحذر واخذ الاحتياطات اللازمة للحماية من مخاطر استخدامها بطريقة غير سليمة:
- عدم تحميل تطبيقات من مصادر غير موثوق بها، والاعتماد فقط على التطبيقات المتوافرة على متجري appstore و playstore.
- عدم استخدام وسائل التراسل الفوري لمناقشة معلومات سرية او شخصية او امنية.
- الحذر من البرمجيات الخبيثة خلال استخدام برامج التراسل الفوري.
- تحديث برامج التراسل الفوري وتغيير كلمة السر دوريا.
- استخدام برامج مرخصة قانونيا.
- تحديث البرامج دوريا.
- عدم فتح المرفقات (صور، مقاطع فيديو...)، الا الموثوقة المصدر.
- عدم الضغط على الروابط، الا اذا كنت متأكدا من مصدرها والوجهة التي تأخذك اليها.
- عدم تحميل اي برنامج من جهة غير موثوق بها.
- تحديث برامج مكافحة القرصنة والفيروسات دوريا.
- ضبط الاذونات لكل تطبيق (permissions) لناحية التحكم في الامكانات او المعلومات التي يمكن للتطبيق الوصول اليها.

ثمة تطبيقات هاتفية اكثر استخداما من غيرها. يجب اعتماد خطوات حماية خاصة لكل منها، ابرزها:

Whatsapp

في اعدادات الخصوصية:
- ايقاف تشغيل خاصية الموقع الحالي (live location).

علينا اعتماد كلمة مرور طويلة، معقدة، سرية وسهلة الحفظ.

- عدم فتح التطبيق على متصفح الانترنت الا عند الحاجة.
- عدم اظهار الحالة (statut) الا لجهات الاتصال (contacts) لدى المستخدم.
- تفعيل ميزة التحقق بخطوتين Two-step Verification، تطلب من المستخدم رمزا يضمن له عدم امكان تفعيل حسابه من جهاز آخر.

Facebook

كي تحمي حسابك من الاختراق، اليك الخطوات الاتية:
- تتبع نشاط فتح الحساب: يظهر لك معلومات عن الحساب الناشط الان وكذلك عن المرة السابقة بحيث يعرض بعض التفاصيل مثل الوقت والمكان، اضافة الى نوع الجهاز والمتصفح المستخدم.
- تفعيل تلقي التنبيهات (alerts): يمكن تلقي التنبيهات عبر البريد الالكتروني او الهاتف او رسالة مسنجر، في حال تم تسجيل الدخول الى حسابك من اي جهاز جديد غير الذي تستخدمه دوريا.
- اختيار ثلاثة او خمسة من اصدقائك المقربين وارسل اليهم رمز وعنوان URL من الشركة، لتتمكن من استرداد حسابك في حال تم اختراقه.
- عدم قبول اي طلب صداقة قبل التأكد من ان الشخص حقيقي وان الصور الموجودة في حسابه حقيقية وليست مزيفة.

- ادارة اعدادات الخصوصية (Privacy) لحظر المستخدمين غير المرغوب فيهم بالاطلاع او الوصول الى معلوماتك.
- التأكد من ربط الحساب برقم الهاتف او البريد الالكتروني (مع التنبه الى ضرورة تسجيل الدخول الدوري الى البريد الالكتروني حتى لا يتم الغاؤه او خرقه).
- تفعيل ميزة التحقق بخطوتين Two-step Verification تضمنان انه اذا تم الدخول الى حسابك عبر متصفح جديد، ان يطالبك برمز التحقق ويرسله الى هاتفك للتحقق من المتصفح.

Twitter

لحمايته يجب اتباع هذه الخطوات:
- انشاء الحساب بشكل آمن.
- انشاء بريد الكتروني جديد، مختلف عن المعتمد عادة من المستخدم، لاستخدامه حصرا لحساب تويتر بهدف تجنيب البريد الالكتروني الاساسي عملية الاختراق، اذا حاول المخترق ان يستخدم خاصية نسيت كلمة المرور.
- ادخال كلمة سر قوية تحتوي على احرف كبيرة وصغيرة وارقام ورموز لا يقل عددها عن العشرة.
- تغيير كلمة السر دوريا (كل 3 اشهر مثلا).
- استخدام كلمة سر مختلفة عن كلمة السر التي تستخدمها لحساباتك الاخرى.
- في خانة الاعدادات لحسابك، الذهاب الى خانة الخصوصية والامان وازالة علامة الصح عن السماح للاخرين بالعثور عليك عبر عنوان بريدك الالكتروني.
- ازالة علامة الصح عن التغريد مع اضافة الموقع الجغرافي.
- ربط الحساب بالهاتف: الاعدادات، الهاتف... ادخل رقم هاتفك واتبع الارشادات التي يعرضها تويتر (تختلف باختلاف مشغل خدمة الهاتف الذي تستخدمه).
- العودة مرة اخرى الى قائمة الحساب ثم وضع علامة صح على خيارات الحماية المتنوعة التي تظهر لك.
- التأكد من ربط حسابك برقم الهاتف لتلقي رسالة تتضمن رمز التوثيق للدخول الى الحساب، ما يتيح لك ايضا معرفة محاولة اختراق حسابك عبر اي شخص آخر في حال لم تكن انت المستخدم.

شبكة الواي فاي WIFI

لحماية شبكة الواي فاي من الاختراق يجب اتخاذ هذه الاجراءات:
- تغيير كلمة المرور الخاصة بالموزع (Router): اسم المستخدم وكلمة السر الافتراضية في الاعدادات الاساسية للموزع (Router)، غالبا ما يكونا Admin ما يسهل اختراقهما في حال اعتمادهما. لذلك على المستخدم تغييرها واعتماد اسم جديد وكلمة سر قوية.
- اختيار تصفية عناوين الـ MAC: لكل جهاز كومبيوتر وهاتف ذكي عنوان MAC خاص به وفريد، لذا يمكن استخدام عناوين الماك الموثوق بها ومنع بقية عناوين الماك غير المعروفة من الوصول الى شبكة واي فاي. في الامكان تحقيق ذلك عبر: اعدادات الموزع (Router) واختيار DHCP تظهر قائمة من عناوين MAC وتصفية عناوين ماك MAC Adress Filter، اضافة الى عناوين الماك الموثوق بها.
- تقليل مدى اشارة واي فاي: تتيح بعض اجهزة الموزع (Router) التحكم في قوة بث الاشارة ومداها، لذلك يستطيع المستخدم تقليل مدى بثها لكي لا تتجاوز حدود المنزل على سبيل المثال، وذلك من خلال تعديل MAC TX Rate وتخفيضها لتقليل قوة الاشارة خارج المنزل او المركز.
- اخفاء اسم شبكة واي فاي: يكون اسم شبكة واي فاي ظاهرا بشكل افتراضي لسرعة اتصال المستخدمين به، لكن في حال اخفائه فانها تطلب من المستخدم: كتابة اسم الشبكة يدويا واختيار نوع التشفير وكلمة المرور.

لحماية الشبكة ايضا، ينبغي اتباع الخطوات التالية: دخول الاعدادات واختيار Wireless واخفاء SSID او تعطيلها.


عدم فتح اي رسالة الكترونية او ملف مجهول المصدر.

اطفالنا اولوية

حرصت المديرية العامة للامن العام خلال حملة التوعية، بتوجيهات واضحة من مديرها العام اللواء عباس ابراهيم، على اعطاء الاولوية للشق المتعلق بالاطفال كونهم يشكلون العنصر الاضعف والاكثر استهدافا من شبكات الاجرام المنظم. لكن دور الاهل في هذا المجال يبقى هو الاساس، ويرتكز على حمايتهم ومراقبتهم لكل ما يتصل بعلاقة اولادهم بالادوات الالكترونية، كاستخدام برمجيات الحماية بهدف حصر المواقع المسموح لاطفالهم زيارتها، وحظر المواقع الخطرة. كذلك تشجيع الاطفال على الحوار ومناقشة ذويهم حول اية مشكلة يواجهونها في اثناء استخدام الانترنت، وغيرها من الواجبات التي يستطيع الاهل وحدهم القيام بها.