

وسائل التواصل سهلت إستفراد مجرم بأطفال ومراهقين الأمن العام كثف محاضرات التوعية السيبرانية

تكاد لا تحصى ايجابيات التطور التكنولوجي الهائل على حياة الناس في المجالات الاجتماعية، الاقتصادية وسواها. في المقابل، كانت له سيئات عدة، منها مثلا سهولة تواصل اخطر المجرمين المحنكين، بشكل مباشر وسري عبر وسائل التواصل، مع اطفال او مراهقين ابرياء لاستدراجهم الى افعال جرمية

امام حقائق ثابتة تفيد بأن وسائل التواصل اصحت امرا واقعا لا يمكن الغاؤه من حياة اولادنا، وبأن مرحلتي الطفولة والمراهقة تتميزان بالبراءة وقللة الخبرة مما يجعل اصحابها فريسة سهلة للمجرمين المحنكين. لا يمكن للاهل حماية اولادهم من مختلف الجرائم التي قد تطالهم عبر وسائل التواصل الاجتماعي، كتلك التي حصلت عبر ما اصبح يعرف بعصابة "التيك - توك" الشهيرة، الا عبر الرقابة الدائمة عليهم، تعزيز الحوار والصراحة معهم، وتوعيتهم بشكل متواصل. في سياق التوعية والتوجيه والتثقيف، تقوم المديرية العامة للامن العام منذ العام 2019، بالقاء محاضرات سيبرانية في مختلف المدارس والجامعات.

ما ابرز الجرائم التي تحصل عادة عبر مختلف وسائل التواصل الاجتماعي؟ ما ابرز قواعد ووسائل الحماية السيبرانية بالنسبة الى الاطفال والمراهقين او الراشدين؟ ماذا عن العقوبات على بعض ابرز تلك الجرائم؟ ما هي الانجازات التي تحققتها المديرية العامة للامن العام لتوعية الاطفال ومراهقي وشباب المدارس والجامعات وحمايتهم؟

ابرز الجرائم

كون الاتصال عبر مختلف وسائل التواصل الالكتروني يكون من بعد، فان كل انواع الجرائم التي لا تتطلب الحضور او الاتصال الجسدي بين اطرافها يمكن ان تحصل عبر تلك الوسائل. مع الاشارة الى انه في كثير من الاحيان، تبدأ العلاقة من بعد لتتحول الى حضورية مع الوقت. يمكن تصنيف مختلف انواع الجرائم التي قد تتم عن بعد عبر مختلف وسائل التواصل كالآتي:

اولا: جرائم تطاول الافراد، مثلا:

- جرائم القذف والذم. ان الكثير من افعال التنمر

عبر وسائل التواصل الاجتماعي تعتبر جرائم قذف او ذم عندما تتوافر فيها الشروط القانونية لأي من هاتين الجريمتين.

- تهديد الافراد سواء بشكل مباشر او غير مباشر كالتهديد بالقتل او بايقاع اذية ما بالشخص المعني او احد افراد عائلته.
- التحريض: كالتحريض المذهبي او الطائفي او غيره.

ثانيا: جرائم ضد المؤسسات:

- سرقة او تخريب انظمة وبرامج عمل مؤسسة ما على سبيل المثال.
- تشويه سمعتها عبر اخبار كاذبة او قذف وذم.
- ثالثا: جرائم ضد الاموال:
- الاستيلاء على حسابات مصرفية عن طريق الاحتيال مثلا.
- انتهاك حقوق الملكية الفكرية والادبية.

رابعا: جرائم ضد امن الدولة:

- التجسس على مؤسسات الدولة الامنية، السياسية، الدبلوماسية، وسواها لصالح اي جهة كانت.
- بث اخبار تثير النعرات الطائفية في البلاد.
- لكل جريمة طرق اثبات، اصول ملاحقة، عقوبات معينة، وسوى ذلك من التفاصيل القانونية. كما ان القانون يعاقب بالاضافة الى مرتكب الفعل الجرمي، كلا من المحرض والشريك والمتدخل في ذلك الفعل الجرمي.

امثلة عقوبات

على ضوء ما اثارته قضية ما يسمى بعصابة "التيك - توك" من ضجة واستنكار لدى الرأي العام اللبناني، بخاصة لناحية ما تداولته وسائل الاعلام حول استدراجها اطفالا ومراهقين واغتصابهم وسوى ذلك من الافعال، سنتوقف في هذا السياق باقتضاب وعلى سبيل

المثال عند رأي القانون يمثل تلك الافعال. بحسب المادة 586 من قانون العقوبات الصادر تحت الرقم 340 تاريخ 1 اذار 1943، المعدلة في 24 آب 2011، تعتبر افعال اجتذاب اي شخص بمختلف طرق التهديد او الترغيب او الاستغلال لضعفه او ما شابه، بهدف استغلاله جنسيا او في افعال دعارة او غيرها من الافعال التي عدتها تلك المادة، افعالا تؤلف جريمة الاتجار بالبشر. يعاقب مرتكبو جرائم الاتجار بالبشر تلك بعقوبة الاعتقال لمدة لا تقل عن خمس سنوات وبالغرامة من مئة ضعف الى مئتي ضعف الحد الادنى الرسمي للاجور بالحد الادنى، اي ان فترة الاعتقال ومقدار الغرامة يزيدان في حالات اخرى عدتها تلك المادة. استطرادا، تشدد العقوبات اذا ارتكبت افعال الدعارة او الاستغلال الجنسي بفعل شخصان او اكثر، وكذلك اذا تناولت الجريمة اكثر من مجنى عليه.

وسائل الحماية

يجمع علماء الامن السيبراني والتربية والنفس والاجتماع على وجود وسائل وتقنيات وقواعد عدة مخصصة لحماية الاشخاص، سواء الاطفال او المراهقين او الراشدين، من المخاطر السيبرانية، ابرزها بشكل عام نوعان اساسيان: الاول تربوي والثاني تقني.

الحماية التربوية

يقصد بعبارة الحماية التربوية - السيبرانية ابرز قواعد تربية الاطفال والمراهقين في ما خص علاقتهم بالعالم السيبراني، بحيث ينصح علماء النفس والاجتماع بالآتي:

- عدم تسليم الطفل او المراهق جهازا متصلا بالانترنت بشكل دائم، الى ان يصبح ناضجا وواعيا نوعا ما.

- تعيين وقت محدد لاستخدامه وسائل التواصل او الاجهزة السيبرانية وجعله يعتاد على الالتزام به.
- تعزيز الحوار الصادق معه بشكل يومي وفي شتى المواضيع.
- الاشتراك معه في مناقشة كل ما يهمه او يصادفه او يحبه او يجب ان يعرفه بالنسبة الى اجهزة العالم السيبراني وتطبيقاته.
- اعلامه، بحسب الطريقة المناسبة لعمره، بابرز اخطار العالم السيبراني والامور او الاشخاص غير الصادقين الذي قد يصادفهم وبضرورة ابلاغ اهله عن اي علاقات جديدة مشوقة او تواصل متكرر مع اي كان.
- اقتاعه بضرورة عدم اجابة احد عن اي سؤال يتعلق بافراد عائلته وعدم اعطائه ايا كان صور اي مستندات او بطاقات مصرفية او ارقام هواتف تخص ايا كان في المنزل، وما شابه من افعال.

- متابعته بشكل دائم، لحظة بلحظة، في ما خص العالم السيبراني. تماما كما تتم متابعة طفل ما لحظة بلحظة بالنسبة الى الاشياء التي يمكن للانسان ان ياكلها وتلك التي تعتبر سموم او نفايات او اوساخ يجب عليه الابتعاد عنها.

الحماية التقنية

تتمثل من جهة اولى برفع مستوى الثقافة السيبرانية للفرد بهدف تمكينه من استخدام مختلف اجهزة وبرامج وتطبيقات العالم السيبراني بشكل آمن. من جهة ثانية، اعتماده برامج وتطبيقات حماية وتجديدها بشكل دوري، وما شابه من تقنيات الكترونية. في هذا السياق، سنتوقف على سبيل المثال التوضيحي عند بعض الامثلة عن ابرز الوسائل التقنية - العملائية التي تساعد المواطنين على حماية انفسهم واجهزتهم الالكترونية من الجرائم السيبرانية، وذلك عبر الآتي:

كلمة المرور (Password)

كلمة المرور (Password) هي الية 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



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 المتوفرة على متجرى 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 الموثوق بمصدرها.
- عدم الضغط على الروابط الا اذا كنت متاكدا من مصدرها والوجهة التي تاخذك اليها.
- عدم تحميل اي برنامج من جهة غير موثوق بها.
- تحديث برامج مكافحة القرصنة والفيروسات دوريا.
- ضبط الاذونات لكل تطبيق (permissions) ◀



اللواء البيسري: بناء الانسان الصالح هدفا اولا، دائما، وابدا



- شخصية - عملية - سرية - سهلة الحفظ. لتحقيق هذه المميزات يجب اتباع الخطوات التالية:
- اختر كلمات مرور قوية تتألف من مجموعة من الاحرف الابدجية الصغيرة والكبيرة، بالاضافة الى الرموز والارقام مثل: k@b2oL3z.
- تغيير كلمة المرور التابعة لحساباتك الشخصية دوريا (مثلا 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 متكهنه وكلمات من حروف متسلسلة او مكررة مثل: -12345678- abcdefg 222222.
- تجنب استخدام كلمات من معلومات شخصية مثل الاسم وتاريخ الميلاد، او معلومات مماثلة: مثلا سعيد، 1990/9/23.

UNITED FOR A HEALTHIER WORLD

Supporting Lebanese Businesses
Since 1990



◀ لناحية التحكم في الامكانات او المعلومات التي يمكن للتطبيق الوصول اليها.

فيسبوك Facebook

كي تحمي حسابك من الاختراق، اليك الخطوات الآتية:

- 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 الى خمسة من اصدقائك المقربين، ارسل اليهم رمز وعنوان URL من الشركة، لتتمكن من استرداد حسابك في حال تم اختراقه.
- عدم قبول اي طلب صداقة قبل التأكد بان الشخص حقيقي وان الصور الموجودة في حسابه حقيقية وغير 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 التنبيه الى ضرورة تسجيل الدخول الدوري الى البريد الالكتروني حتى لا يتم الغاؤه او خرقه).

- تفعيل ميزة " التحقق بخطوتين Two-step Verification" التي تضمن انه اذا تم الدخول الى حسابك عبر متصفح جديد، ان يطالبك بـ "رمز التحقق" يرسله الى هاتفك للتحقق من المتصفح.

الامن العام: حماية وتوعية

في موازاة المهمات والانجازات الامنية التي تحققتها المديرية العامة للامن العام على مختلف الصعد الامنية - السيبرانية، كتوقيف العديد من الشبكات الاجرامية المنظمة التي تنشط عبر مختلف وسائل التواصل الاجتماعي في مجال تجارة المخدرات، الدعارة، الاحتيال وسواها. كذلك رصد المواقع الالكترونية التي تقوم بارتكاب

جرائم سيبرانية ضد المواطنين وابلغ القضاء عنها بهدف حجبها من التداول وسواها من الافعال المماثلة غير المنظورة للعموم كونها امنية وغالبا ما تبقى طي الكتمان بقرار من القضاء. المديرية، وبهدف توعية وتثقيف وحماية مختلف المواطنين عموما، لاسيما الاطفال والمراهقين والشباب خصوصا كونهم العنصر الاضعف بسبب قلة خبرتهم وتركيز الشبكات الاجرامية عليهم بشكل كبير، اطلقت منذ عدة سنوات حملة توعية على مخاطر الفضاء السبراني تحت شعار "حتى ما تكون ضحية". تضمنت الحملة عدة برامج توعية وحماية سيبرانية من ابرزها اصدار تعاميم توعية بشكل دوري وتعميمها عبر مختلف وسائل الاعلام وكل المنصات والمواقع والبرامج الاعلامية التابعة للمديرية. وكذلك انجاز محاضرات في الامن السبراني في مختلف المدارس والجامعات اللبنانية بهدف توعية وحماية الطلاب.

من آخر تلك المحاضرات التي انجزت خلال الاشهر القليلة الفائتة نذكر على سبيل المثال لا الحصر، محاضرات في كل فروع جامعة القديس يوسف (USJ)، سلسلة مدارس المصطفى، ثانوية راهبات الوردية، مدارس المبرات، ثانوية الصرند، ثانوية مار ميخائيل - زوق مكابيل، مدارس الابرار، جامعة المدينة في طرابلس، وسواها. يأتي كل ذلك تطبيقا لنهج وطني تعتمده المديرية العامة للامن العام ويمكن اختصاره بما اكد ويؤكد عليه مديرها العام بالانابة اللواء الياس البيسري خلال لقاءاته مع الاعلاميين والعسكريين عبر قوله ما مفاده: "ان بناء مستقبل افضل للوطن يبدأ عبر حماية وتوعية واعداد اطفاله ومراهقيه وشبابه بشكل افضل منذ الان. عندما نبني طفل او شاب صالح سيكون عندنا في المستقبل موظف صالح، تاجر صالح، ومسؤول صالح. فبناء الانسان الصالح يجب ان يكون هدفنا اولا، دائما، وابدأ".

