المديريّة العامّة للأمن العام اللّبناني

تضحية . خدمة

أمن المعلومات والتوعية من المخاطر

المديريّة العامّة للأمن العام

أمن المعلومات والتوعية من المخاطر

"سوف نبقى سداً منيعاً في وجه كل المخاطر التي تهدّد حاضر

ومستقبل وطننا ومنها مخاطر العالم الإفتراضي

فاحذروا فخ هذا العالم، لأنه سلاح ذو حدّين

ولا تكونوا أداة للتكنولوجيا لمصلحة أعدائنا بل استخدموا هذه الأداة

بهدف مقاومتهم لما فيه إعلاء كلمة الحق وصون لبنان الوطن."

مدير عام الأمن العام
اللواء عباس إبراهيم

أمن المعلومات

- كلمة المرور
- الأجهزة الإلكترونية
- متصفح الإنترنت
- البريد الإلكتروني
- حماية المعلومات
- الحسابات المصرفية
- التطبيقات
- شبكة الواي فاي

مخاطر الإنترنت

- تجنيد العملاء لصالح العدو الإسرائيلي
- الإرهاب والتطرف
- تجارة السلاح
- تجارة المخدرات
- الابتزاز الإلكتروني
- الإتجار بالبشر
- إنترنت آمن للأطفال

كيف تحمي نفسك من مخاطر العالم الإفتراضي؟

سؤال لا بدّ من طرحه والإجابة عنه والتوعية بشأنه انطلاقاً من مسؤوليتنا تجاه المواطن وتجاه مجتمعنا، في عالم أضحت فيه الجريمة بمختلف أنواعها هاجسنا الوحيد، بعد أن أصبحنا نعيش في قرية كونية واحدة بسبب الإنترنت.

هجمات إلكترونية، سرقة بيانات وحسابات مصرفية، عمليات نصب واحتيال، تجنيد عملاء لصالح العدو الإسرائيلي، تجنيد لصالح الإرهاب التكفيري، إضافة إلى الإتجار بالبشر والإتجار بالمخدرات والسلاح، كلها جرائم باتت تمثّل خطراً محدقاً على كافة شرائح المجتمع اللبناني، لسهولة التواصل بين مختلف الدول، إذ لم تعد المسافات عائقاً أمام العلاقات الاجتماعية والاقتصادية والسياسية.

يزوّد هذا الكتيّب القرّاء من مختلف الفئات العمرية بالمعلومات الضرورية البسيطة التي تجنّب الاستخدام الخاطئ لشبكة الإنترنت حتى لا يكونوا ضحية أي فعل جرمي يعاقب عليه القانون.

إضافة إلى ذلك، يقدّم الكتيّب توعية شاملة حول الاستخدام الآمن لشبكة الإنترنت من خلال شرح المفاهيم الأساسية التي تساهم في الحفاظ على الخصوصية الرقمية وحماية المعلومات.

أمن المعلومات

أصبحت الوقاية من الجرائم التي تُرتكب على الإنترنت محطّ اهتمام جميع الجهات المختصة، التي تعمل بدورها على التصدي لها ومكافحتها ولا سيّما بعد كثرة عمليات الاحتيال والابتزاز واختراق مواقع حكومية أو خاصة وذلك عبر اتخاذ عدة تدابير أساسية

- كلمة المرور
- الأجهزة الإلكترونية
- متصفح الإنترنت
- البريد الإلكتروني
- حماية المعلومات
- الحسابات المصرفية
- التطبيقات
- شبكة الواي فاي

الأمن المعلوماتي

كلمة المرور (Password)

كلمة المرور (Password) هي آلية تعريف للمستخدم (User). تُعدّ من أهم وسائل حماية البيانات، فهي تُعتبر القفل على الخزينة الإلكترونية لما تقوم به من حماية للمعلومات وأنظمة التشغيل الخاصة بالمستخدم.

مميزات كلمة المرور القوية:

- طويلة
- معقدة
- غير شخصية
- عملية
- سرية
- سهلة الحفظ

لتحقيق هذه المميزات اتّبع الخطوات التالية:

- اختر كلمات مرور قوية تتألف من مجموعة من الأحرف الأبجدية الصغيرة والكبيرة، بالاضافة الى الرموز والأرقام مثل: K@b2oL3Z.
- تغيير كلمة المرور التابعة لحساباتك الشخصية دورياً (كل ثلاثة أشهر تقريباً).
- عدم الإفصاح عن كلمة المرور الخاصة بك لأي شخص آخر.
- عدم استخدام كلمة مرور واحدة لعدة حسابات.
- تجنّب استخدام كلمات متكهّنة وكلمات من حروف متسلسلة أو مكرّرة مثل: ~~12345678~~، ~~222222~~، ~~abcdefg~~.
- تجنب استخدام كلمات من معلومات شخصية مثل الاسم وتاريخ الميلاد، أو معلومات مماثلة: مثل ~~سعيد~~، ~~23\9\1990~~.

الأمن المعلوماتي

الأجهزة الإلكترونية (Electronic Devices)

هناك عدة طرق تُمكّن المخترقين من الوصول إلى أجهزة الضحية وجميعها تهدف لخرق البيانات الشخصية السرية والاطلاع عليها، فيما يلي بعض الحلول الوقائية لتفادي الوقوع ضحية المخترق (Hacker) :

- وضع كلمة سر قوية لتشغيل الجهاز.
- عدم الاتصال بشبكة "واي فاي" مفتوحة.
- استخدام برامج مضادة للفيروسات (Antivirus) لكشف الفيروسات والقضاء عليها.
- القيام بعملية المسح الإلكتروني للجهاز دورياً (Scansystem).
- تحديث البرامج المضادة للفيروسات دورياً (Update).
- عدم الاعتماد على برامج مضادة للفيروسات منتهية الصلاحية.
- الحذر من الأجهزة المشتركة أو العامة المستخدمة من قبل جميع المواطنين.
- تفعيل خاصية إغلاق الهاتف أوتوماتيكياً بعد بضع دقائق.
- عدم إدخال أي حافظة (Flash Memory) أو كابل USB مجهول المصدر في الجهاز.
- الحرص على إيقاف "واي فاي (Wi-fi)" في حال عدم الاتصال بشبكة موثوقة.
- تجنّب الاتصال بشبكات "واي فاي" عامة (الفنادق، المطارات، المقاهي...) أي (Public Wi-fi).
- عدم الاتصال بجهاز بلوتوث (Bluetooth) غير موثوق.
- الحرص على إيقاف البلوتوث في حال عدم استخدامه.

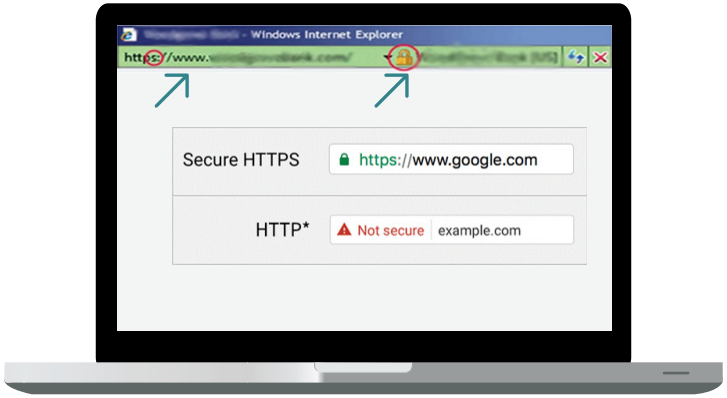
- القيام بإعادة ضبط المصنع (Factory Reset) قبل بيع أي جهاز والتأكد من مسح جميع البيانات (clear data).
- التأكد من إيقاف تشغيل خاصية تحديد الموقع (Location\GPS) في حال عدم استخدامها.تفعيل ميزة تحديد مكان الهاتف في حال فقدانه او سرقته (findmyiphone, android device manager).

الأمن المعلوماتي

متصفح الإنترنت (Web Browser)

بالرغم من اهمية متصفحات الإنترنت (.../chrome/firefox) الا انها ليست آمنة بما يتناسب مع حساسية وخصوصية المعلومات المتبادلة عبرها. لذلك نقدّم أبرز خطوات الحماية:

- تحقق دائماً من إعدادات متصفّح الإنترنت لديك وقم بتحديثه باستمرار.
- عند استخدامك المتصفّح شغّل "private browsing" كي لا تترك أثر بعد الانتهاء.
- اختر دائماً إشارة (X) الموجودة على زاوية النوافذ المنبثقة (pop-up screen)، ولا تضغط أبداً على "نعم" أو "قبول" أو حتى "إلغاء" لأنها قد تكون خدعة لتحميل برامج خبيثة على جهازك.
- قبل إدخال معلومات حساسة على صفحة الويب، تأكد من وجود إشارة القفل على المتصفح أو كلمة https في عنوان المتصفح كدلالة على أنك محمي.
- الضغط على رمز القفل للتأكد من الصلاحية (Certificate).



الأمن المعلوماتي

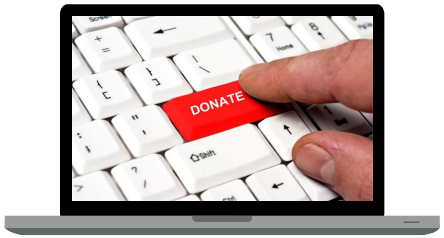
البريد الإلكتروني (Email)

يزداد استخدام البريد الإلكتروني يوماً بعد يوم بهدف نقل الرسائل النصية، إرسال المستندات وتبادل المعلومات التي تعتبر حساسة وغاية في الأهمية. إلا ان البريد الإلكتروني كغيره من وسائل الاتصال، عرضة أيضاً للكثير من الثغرات الأمنية.بالتالي يجب رفع مستوى أمن البريد الالكتروني عبر إتخاذ عدة خطوات أساسية للحماية؛ ابرزها:

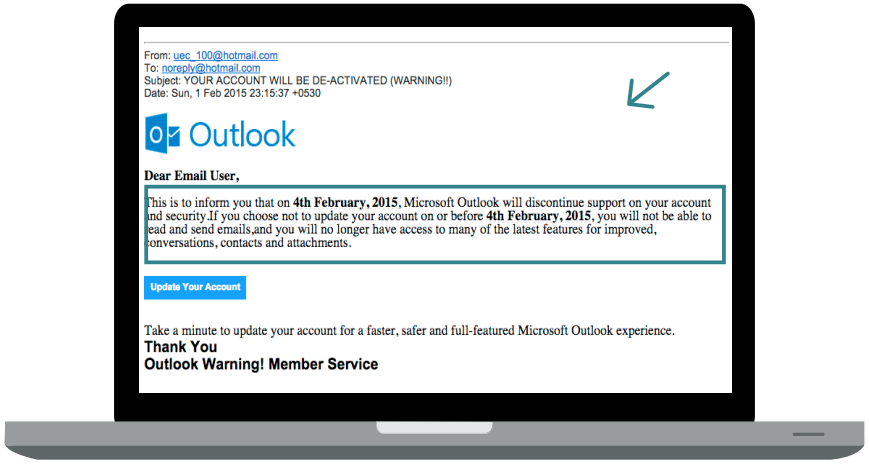
- الاعتماد على خاصية التوثيق بخطوتين لحماية البريد الإلكتروني (Two Factor Authentication).
- عدم فتح أي رسالة إلكترونية أو ملف مجهول المصدر(spam).
- حذف أو عدم الرد على الرسائل الملتبسة أوالرسائل التي تطلب ادخال البريد الالكتروني وكلمة المرور.
- الحرص على الدخول إلى حسابك الشخصي دورياً (مرة كل أسبوع على الأقل).

عروض خادعة لزيارة أماكن سياحية في العالم

طلبات تبرع لجمعيات خيرية



رسائل منبّهة وتحذيرات حول إغلاق حساب معيّن



وعود بالحصول على مبالغ مالية من دون أي جهد يُذكر أو مقابل عمل بسيط.

عروض بشأن بعض الوظائف

الأمن المعلوماتي

حماية المعلومات (Data Privacy)

يعتمد أمن المعلومات الشخصية وحمايتها على مجموعة مبادئ أساسيّة لا بدّ من الالتفات إليها، وهي:

- نسخ احتياطي (backup) للمعلومات المهمة على مخزّن (harddisk\flash memory) غير موصول على الإنترنت (offline).
- عدم مشاركة معلومات أكثر من المطلوب.
- عدم نشر معلومات شخصية على الإنترنت.
- عدم مشاركة عنوان بريدك الإلكتروني الأساسي أو اسمك الخاص بالرسائل الفورية، إلا مع الأشخاص الموثوق بهم.
- عدم إدراج عنوان بريدك الإلكتروني أو اسمك على دلائل الإنترنت أو على مواقع وظائف العمل غير الموثوق بها.
- مراقبة ما يكتبه الآخرون عنك على مواقع التواصل الاجتماعي.
- عدم السماح للآخرين بنشر صور تعود لك او لعائلتك من دون موافقتك.
- عدم مشاركة أي حافظة (USB)، إلا إذا كانت للقراءة فقط (read-only) أي إنها غير قابلة للتعديل.
- تجنّبْ استخدام أي حافظة، إلا إذا كنت واثقاً من المصدر.

الأمن المعلوماتي

الحسابات المصرفية (Banking Accounts)

على الرغم من إجراءات الأمان والتأمين التي تعمل البنوك على تطبيقها، إلا أنها دائماً ما تكون هدفاً وعرضةً للمخترقين والقراصنة الذين يسعون جاهدين بكل الاساليب للحصول على المال بطرائق غير شرعية. لذلك يتوجب على المستخدم الالتزام بالتالي:

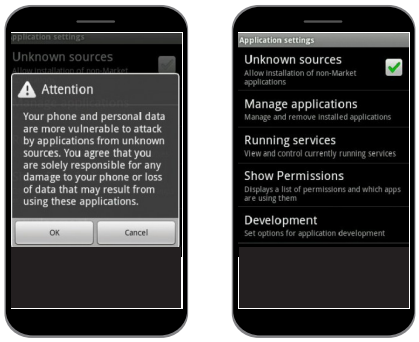
- المحافظة على سرية رقم حسابك، اسم المستخدم وكلمة المرور.
- التنبّه من عمليات الاحتيال الإلكترونية وتجاهل الرسائل الإلكترونية التي تطلب منك رقم حسابك أو كلمة المرور.
- تغيير كلمة المرور التابعة لمصرفك الإلكتروني وبطاقاتك المصرفية (visa card-master card) دورياً بهدف منع اختراقها.
- تحديث تطبيقات الخدمات المصرفية الإلكترونية.
- تجنب استخدام كلمة السر نفسها في المواقع المصرفية ومواقع التواصل الاجتماعي.
- عند إجراء عمليات الشراء عبر الإنترنت، تأكّد من قراءة سياسة الخصوصية الإلكترونية (license) للشركة.
- عدم مناقشة بياناتك الشخصية أو المصرفية خلال أي مكالمة مريبة تصلك.
- تفادي إجراء أي معاملة مالية إلكترونية، إلا عند الضرورة.

الأمن المعلوماتي

التطبيقات (Applications)

بالرغم من أهمية التطبيقات الذكية المستخدمة يوميا لاهداف متعددة، إلا انه ينبغي الحذر وأخذ الاحتياطات للحماية من مخاطر استخدامها بطريقة غير سليمة:

- عدم تحميل تطبيقات من مصادر غير موثوقة، والاعتماد فقط على التطبيقات المتوفرة على متجريّ (playstore/appstore).
- عدم استخدام وسائل التراسل الفوري لمناقشة معلومات سرية أو شخصية أو أمنية.
- الحذر من البرمجيات الخبيثة خلال استخدام برامج التراسل الفوري.
- تحديث برامج التراسل الفوري وتغيير كلمة السر دورياً.
- استخدام برامج مرخصة قانونياً.
- تحديث البرامج دورياً.
- عدم فتح المرفقات (صور/مقاطع فيديو..)، إلا موثوقة المصدر .
- عدم الضغط على الروابط، إلا إذا كنت متأكداً من مصدرها والوجهة التي تأخذك إليها.
- عدم تحميل أي برنامج من جهة غير موثوقة.
- تحديث برامج مكافحة القرصنة والفيروسات دورياً.
- ضبط الأذونات لكل تطبيق (permissions) لناحية التحكم في الإمكانات أو المعلومات التي يمكن للتطبيق الوصول إليها.

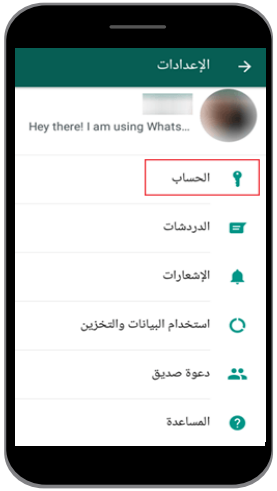


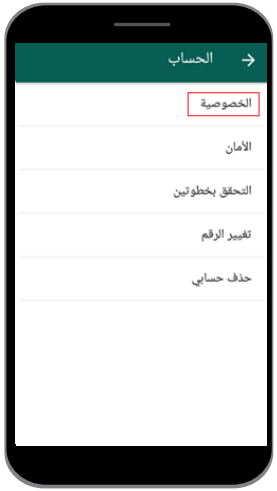
ثمة تطبيقات هاتفية أكثر استخداماً من غيرها. يجب اعتماد خطوات حماية خاصة لكلّ منها، أبرزها:

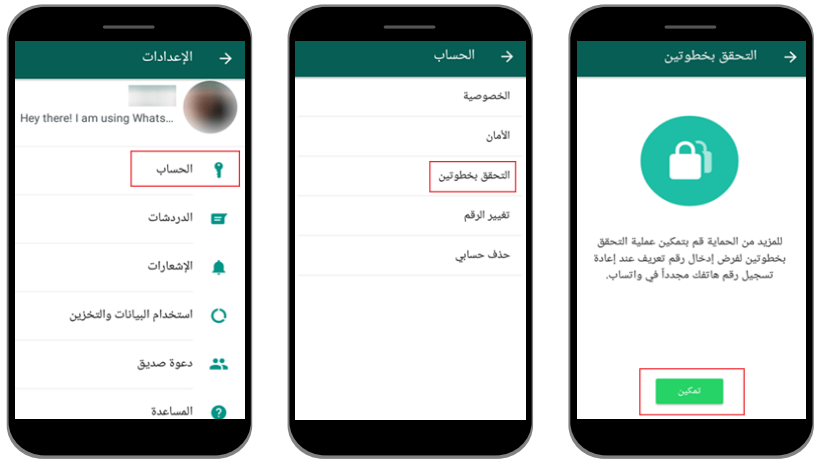
Whatsapp

في إعدادات الخصوصية:

- إيقاف تشغيل خاصيّة الموقع الحالي (live location).
- عدم فتح التطبيق على متصفح الإنترنت إلا عند الحاجة.
- عدم إظهار الحالة (status) إلا لجهات الاتصال (contacts) لدى المستخدم.
- عدم إظهار الصورة الشخصية (profile picture) إلا لجهات الاتصال (contacts) لدى المستخدم.
- تفعيل ميزة "التحقق بخطوتين Two-step Verification " والتي تطلب من المستخدم "رمزاً" يضمن له عدم إمكانية تفعيل حسابه من جهاز آخر.



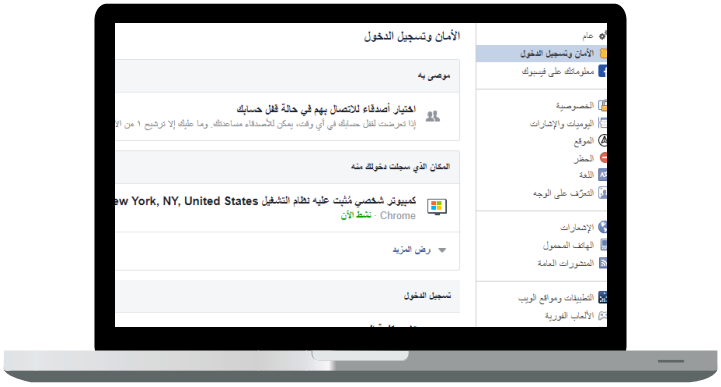




Facebook

يعدّ "فيسبوك" من أكثر المواقع استخداماً على مواقع التواصل الاجتماعي في كافة أنحاء العالم ومن مختلف الفئات العمرية. إلا أن "فيسبوك" يسهّل بشكل كبير للمخترقين الوصول الى أي معلومة حول الافراد، إليك الخطوات التالية كي تحمي حسابك من الاختراق:

- تتبّع نشاط فتح الحساب: يظهر لك معلومات عن الحساب الناشط الآن وكذلك عن المرة السابقة بحيث يعرض بعض التفاصيل مثل الوقت والمكان، إضافة إلى نوع الجهاز والمتصفّح المستخدم.

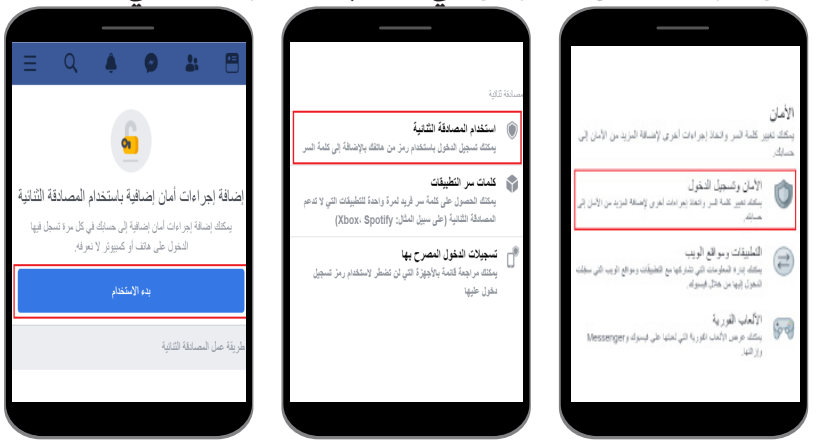


- تفعيل تلقّي التنبيهات (alerts): يمكن تلقّي التنبيهات عبر البريد الإلكتروني أو الهاتف أو رسالة ماسنجر، في حال تم تسجيل الدخول إلى حسابك من أي جهاز جديد غير الذي تستخدمه دورياً.

- اختيار ثلاثة إلى خمسة من أصدقائك المقرّبين، أرسلْ إليهم رمز وعنوان URL من قبل الشركة، لتتمكّن من استرداد حسابك في حال تم اختراقه.

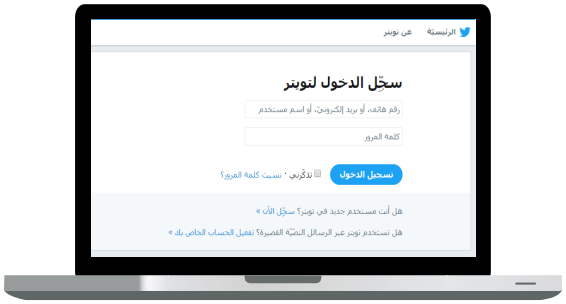
- عدم قبول أي طلب صداقة قبل التأكد بأن الشخص حقيقي وأن الصور الموجودة في الحساب حقيقية وغير مزيّفة.
- إدارة إعدادات الخصوصية (Privacy) لحظر المستخدمين غير المرغوب فيهم بالاطلاع أو الوصول إلى معلوماتك.
- التأكد من ربط الحساب برقم الهاتف أو بالبريد الإلكتروني (مع التنبه إلى ضرورة تسجيل الدخول الدوري إلى البريد الإلكتروني حتى لا يتم إلغاؤه أو خرقه).
- تفعيل ميزة "التحقق بخطوتين Two-step Verification" والتي تضمن أنه إذا تمّ الدخول إلى حسابك عبر"متصفّح جديد" أن يطالبك بـ "رمز تحقق" يرسله إلى هاتفك للتحقق من المتصفّح.

يتم تفعيل ميزة "التحقق بخطوتين" في حساب "فيسبوك" كالآتي:

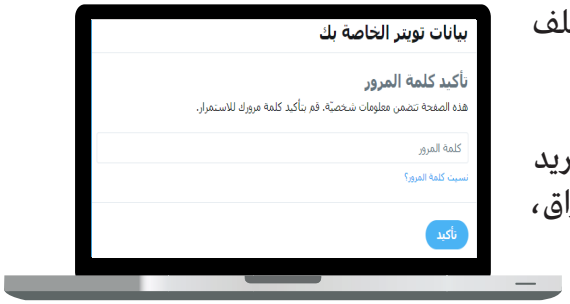


Twitter

يعد "تويتر" أيضاً من أشهر تطبيقات التواصل الاجتماعي ، كونه يسمح لمستخدميه بمشاركة الآخرين «تغريدات» (مقالات/صور...) يمكن قراءتها مباشرة من صفحتهم الرئيسية أو من خلال زيارة ملف المستخدم الشخصي. بالتالي هو عرضة لخطر القرصنة الالكترونية ولحمايته يجب اتباع الخطوات التالية:



- إنشاء الحساب بشكل آمن.



- إنشاء بريد إلكتروني جديد، مختلف عن المعتمد عادةً من المستخدم، لاستخدامه عند فتح حساب "تويتر"، وذلك بهدف تجنيب البريد الإكتروني الأساسي عملية الاختراق، إذا حاول المخترق أن يستخدم خاصية "نسيت كلمة المرور".

- إدخال كلمة سر قوية تحتوي على أحرف كبيرة وصغيرة وأرقام ورموز لا يقل عددها عن عشرة.
- تغيير كلمة السر دورياً (كل 3 أشهر مثلاً).
- استخدام كلمة سر مختلفة عن كلمة السر التي تستخدمها لحساباتك الأخرى.

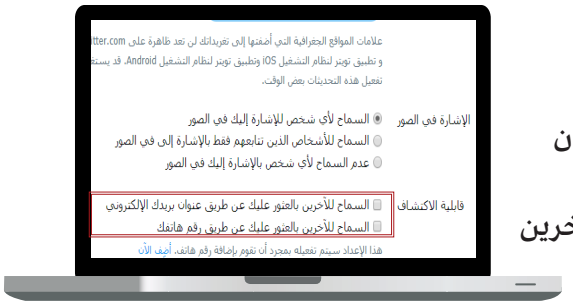
في خانة الإعدادات لحسابك

↓

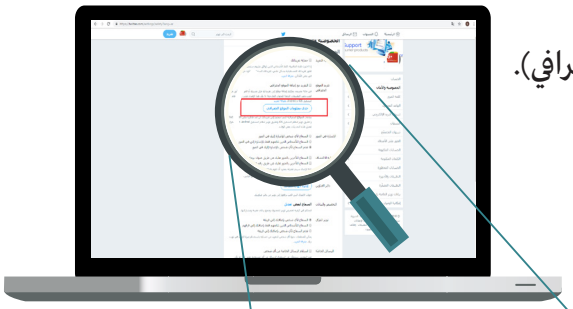
الذهاب إلى خانة الخصوصية والأمان

↓

إزالة علامة الصح عن (السماح للآخرين بالعثور عليك عن طريق عنوان بريدك الإلكتروني



- إزالة علامة الصح عن (التغريد مع إضافة الموقع الجغرافي).



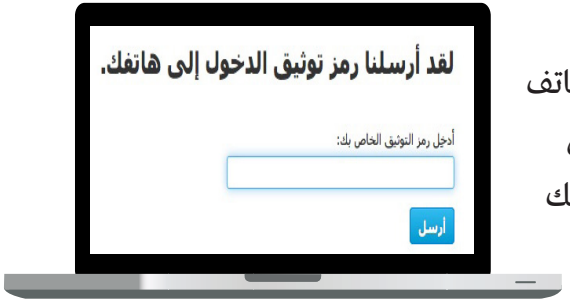
- ربط الحساب بالهاتف :

الإعدادات - الهاتف- أدخل رقم هاتفك

← اتبع الإرشادات التي يعرضها تويتر (تختلف باختلاف مشغّل خدمة الهاتف الذي تستخدمه).

- العودة مرة أخرى إلى قائمة الحساب ثم وضع علامة صح على الخيارات التالية:

- التأكد من ربط حسابك برقم الهاتف لتلقّي رسالة تتضمّن رمز التوثيق للدخول إلى الحساب، ما يتيح لك أيضاً معرفة محاولة اختراق حسابك عبر اي شخص آخر في حال لم تكن أنت المستخدم.



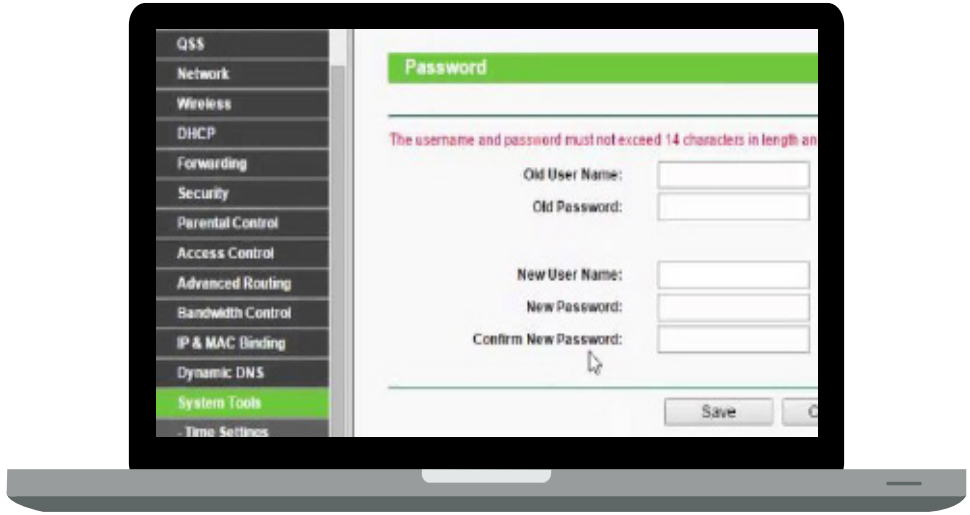
الأمن المعلوماتي

شبكة الواي فاي (WIFI)

لحماية شبكة الواي فاي من الاختراق يجب اتخاذ الإجراءات التالية:

تغيير كلمة المرور الخاصة بالموزع (Router)

إن "اسم المستخدم وكلمة السرّ" الافتراضية في الإعدادات الأساسية للموزع (Router) غالباً ما تكون: "Admin" ما يسهّل اختراقها في حال اعتمادها. لذلك على المستخدم تغييرها واعتماد اسم جديد وكلمة سر قوية.



اختيار تصفية عناوين ال MAC

لكل جهاز كمبيوتر وهاتف ذكي عنوان MAC خاص به وفريد، لذلك يمكن استخدام عناوين الماك الموثوقة ومنع باقي عناوين الماك غير المعروفة من الوصول الى شبكة ال واي فاي. بإمكان تحقيق ذلك عبر:

إعدادات الموزع (Router) ← اختيار DHCP ← تظهر قائمة من عناوين MAC ← تصفية عناوين ماك " MAC Address Filter " ← إضافة عناوين الماك الموثوقة.

تقليل مدى إشارة واي فاي

تتيح بعض أجهزة الموزع (Router) التحكم في قوة بث الإشارة ومداها، لذلك يمكن للمستخدم تقليل مدى بثها لكي لا تتجاوز حدود المنزل على سبيل المثال، وذلك من خلال:

- تعديل Max TX Rate وتخفيضها لتقليل قوة الإشارة خارج المنزل أو المركز.

إخفاء اسم شبكة واي فاي

يكون اسم شبكة واي فاي ظاهراً بشكل افتراضي لسرعة اتصال المستخدمين به، لكن في حال إخفائه فإنها تطلب من المستخدم:

كتابة اسم الشبكة يدوياً ← اختيار نوع التشفير ← كلمة المرور.

لحماية الشبكة أيضاً، اتّباع الخطوات التالية:

دخول الإعدادات ← اختيار "Wireless" ← إخفاء SSID أو تعطيلها .

الجرائم الإلكترونية

يشهد العالم ثورة في مجال تكنولوجيا المعلومات والاتصالات وهي تشكل المحرك الأساسي في التطوّر في جميع المجالات. وقد نتج عن هذا التطور ظواهر إجرامية جديدة أو ما يُسمى بجرائم الكمبيوتر والإنترنت، أو الجرائم الالكترونية. إن هذه الظواهر تنذر بالخطر لكونها جرائم ذكية تحدث في بيئة إلكترونية ورقمية.

غالباً ما تهدف الجريمة الإلكترونية إلى :

- تجنيد عملاء
- الإرهاب الإلكتروني
- تجارة السلاح
- تجارة المخدرات
- الابتزاز الالكتروني
- الاتجار بالبشر

الجرائم الإلكترونية

تجنيد العملاء لصالح العدو الاسرائيلي

تفشّت في الآونة الأخيرة ظاهرة تجنيد العملاء لصالح العدو الإسرائيلي كما ارتفعت نسبة التجنيد بشكل ملحوظ مقارنةً بالسنوات الماضية. إنها من أخطر الظواهر التي تواجه مجتمعنا اليوم، نظراً إلى تأثيرها السلبي على جميع الجوانب الاجتماعية والاقتصادية والسياسية، حيث تقوم جهة معادية بتجنيد فئة من السكان المحليين كعملاء لها، ينصاعون لأوامرها ويعملون على تحقيق أهدافها، ويقدّمون خدمات لها تسهم في إلحاق الضرر بمصالح شعبهم، وتفكيك وحدته ومنظومته السياسية والاجتماعية.

ما هي العوامل التي تسهم في نجاح عملية تجنيد العملاء؟

- نقص الدافع الوطني وضعف العقيدة .
- الحاجة إلى العمل أو السفر إلى الخارج .
- ضعف الشخصية وفقدان الثقة بالذات.
- حب الانتقام لأقارب لهم قُتلوا بسبب العمالة أو الثأر .
- الفقر والحاجة إلى المال.

ما هي أساليب تجنيد العملاء؟

بهدف تجنيد العملاء تقوم أجهزة العدو الإسرائيلي باستخدام وسائل التواصل المختلفة بغية التحليل النفسي للضحية لمعرفة نقاط الضعف كخطوة أولى ومن ثم:

الترغيب

- بالمال أو بالنساء (ترغيب جنسي).
- الادّعاء بأن غالبية المجتمع من العملاء .
- إقناع الضحية بأن التعامل هو الطريق الأسهل لتحقيق الأماني والأحلام .
- الادعاء بأن المخابرات الاسرائيلية قادرة على حماية عملائها .

التحايل والابتزاز

- دفع الأشخاص إلى ارتكاب ما هو مخالف للقانون والمجتمع، ومن ثم ابتزازهم بما ارتكبوه (تعاطي المخدرات).
- التضييق الاقتصادي على الضحية ومساومتها من أجل الحصول على تصريح بالعمل أو تصريح بالسفر .
- إحضار الوثائق أو الصور أو التسجيلات الصوتية أو المعلومات التي تمكّنهم من استغلال الضحايا بهدف الضغط عليهم (جنس، مخدرات، أعمال منافية للقانون).

الترهيب

- تعذيب الضحية وتلفيق التُهم الخطرة ضدها.
- التهديد بالقتل أو بإيذاء أفراد عائلة الضحية.
- الإساءة إلى السمعة أو المركز.

الإقناع

- إقناع الشخص بأن مصلحته الشخصية هي الهدف الأعلى الذي يجب العمل من أجله .
- إن الارتباط لا يشكل ضرراً عليه بل ينقذه من المصائب ويلبّي رغباته .
- الاعتماد على مبدأ غسل الدماغ والتحفيز على ضرورة التعاون عبر نشر مقاطع فيديو مغرية لأعمال وتقنيات أمنية متطورة لاستقطاب الراغبين.

أماكن تجنيد العملاء

بفعل التطوّر التكنولوجي وتطوّر وسائل الاتصال أصبحت شبكة الإنترنت ومواقع التواصل الاجتماعي المكان الأساسي لتجنيد العملاء كونها الطريق الاسهل للتواصل والتأثير.

كيف تحمي نفسك من فخ التجنيد؟

- تجنّب المواقع والصفحات المشبوهة التي تدعو إلى التعاون مع العدو الإسرائيلي بشكل مباشر أو غير مباشر.
- تجنّب رفاق السوء والمشبوهين على مواقع التواصل الاجتماعي.
- تجنّب الوقوع ضحية الاستغلال في سوق العمل مثل العروضات المغرية حول وظائف مشبوهة
بأجور مرتفعة.
- تجنّب القيام بأي أعمال غير أخلاقية تسهم في الوقوع ضحية الابتزاز، مثل: صور إباحية،....
- الوعي والمسؤولية في استخدام مواقع التواصل الاجتماعي.
- رفض فكرة التطبيع مع العدو الإسرائيلي بش كل مطلق وتجنّب جميع المواقع الإلكترونية التي
تحثّ على ذلك.
- إعلام الأهل والجهات الأمنية المختصة في حال التعرض لمحاولات التجنيد أو عند ملاحظة أي أعمال مشبوهة.
- تجنّب مشاركة وإبداء آرائك في مختلف الامور (السياسة، المجتمع، الثقافة، الاقتصاد..) سواء تتعلّق بمجتمعك أو بأي بلد آخر.

مراجعة الاساليب الوقائية عبر مواقع التواصل الاجتماعي التي تمّ تقديمها في الصفحات السابقة.

الجرائم الإلكترونية

الإرهاب

لا يقل الإرهاب التكفيري خطورةً عن العدو الإسرائيلي من ناحية تجنيد العملاء، فهما وجهان لعملة واحدة، هدفها التأثير سلباً على أمن المجتمع وتفكيكه.

ومع انتشار شبكات التواصل الاجتماعي اليوم، أصبح لدى الجماعات الإرهابية أساليب عديدة لنشر الفكر التكفيري الارهابي وتجنيد الشبان خدمة لمصالحها، فالتجنيد بوجهه الإلكتروني يعتمد على التطرف الفكري والديني بهدف جذب الناس بالعاطفة لإقناعهم بالانضمام إلى تلك الجماعات، خصوصاً
الشبان منهم.

ما هي الدوافع المؤدية إلى تجنيد الإرهابيين؟

- الرغبة في الظهور وحب الشهرة، التي تتولّد بسبب فقدان الثقة والحرمان.
- نقمة الشخص على المجتمع الذي يعيش فيه نتيجة ما يراه من ظلم وهدر لحقوقه وانتشار البطالة والفقر.
- غياب الفكر المعتدل المواجه لنشاط هذه الجماعات التكفيرية المتطرّفة البارزة على مواقع وتطبيقات التواصل (... Facebook,Twitter,Telegram).
- غياب الرقابة الذاتية والأسرية.
- غياب الخلفية الثقافية والعلمية .
- الظاهر في خطابهم المبني على أصول قد يتفق الجميع عليها، مثل رفع الظلم ونُصرة الأمة والمستضعفين، وإنكار مظاهر الفساد.

ما هي أساليب التجنيد والإقناع؟

- توجيه رسائل دينية حماسية تشجّع على العنف والانسلاخ عن المجتمع وتكفير الحكومات وتأييد التطرف ورموزه.
- انتشار المواقع الإلكترونية المنتمية إلى التيارات الفكرية التي تقوم بترويج الفتاوى والكتب التي تحضّ على الإرهاب والتكفير.
- تشغّل التنظيمات الإرهابية عشرات الآلاف من الحسابات على مواقع التواصل الاجتماعي، وتديرها بأسماء نساء تحت مسمّى المجاهدات والأخوات، بهدف تجنيد عناصر جدد، وترغيبهم جنسياً.
- يقوم عناصر هذه الجماعات بتأويل الآيات القرآنية والأحاديث النبوية بشكل يدعو إلى العنف والقتل، بما يتماشى مع رغباتهم وأهدافهم.

للحماية من التجنيد الإرهابي، يجب:

- تجنّب الحسابات والمواقع المؤيّدة للفكر الإرهابي على مواقع التواصل وإبلاغ الجهات الأمنية المختصة عنها.
- الاستفسار عن أية معلومات يتلقّاها الشخص ويعتبرها مثيرة للشكّ.
- تجنّب المواقع التي تعمل على مبدأ الإغراء بالسلاح.
- تجنّب المواقع الدينية المتشددة التي تكفّر جميع الأديان.
- عدم تصديق كل ما يُتداول ويُنشر على مواقع التواصل الاجتماعي.
- التصرف بمسؤولية ووعي مع جميع الأطراف في المجتمع .
- تجنّب الإغراءات المالية مقابل أعمال مشبوهة.

الجرائم الإلكترونية

تجارة السلاح

بات الإنترنت سوقًا كبيراً لتجارة مختلف أنواع الأسلحة، وهو ما أثار قلقاً عالمياً لنمو وازدهار هذه التجارة الحساسة بهذا الشكل. إن أكثر الطرق شيوعاً لبيع الأسلحة هو عبر الإنترنت المظلم (Dark Web) ومواقع التواصل الاجتماعي.

أسباب انتشار تجارة السلاح غير الشرعي:

- الرغبة في التسلح.
- إعطاء الشعور بالأمان.
- عادات وتقاليد اجتماعية موروثة.
- اعتباره مظهراً من مظاهر الرجولة.
- المشكلات الاجتماعية التي تدفع الأفراد إلى حيازة السلاح، ومن أبرزها العنف.
- الكسب المادي وتحقيق الربح.

ما هي طرق الحماية منها؟

- تجنّب وحظر الصفحات والمواقع الإلكترونية التي تروّج لتجارة السلاح.
- مراقبة الأهل لأبنائهم على مواقع التواصل الاجتماعي من خلال معرفة أصدقائهم والصفحات التي يتابعونها.
- تجنب الأصدقاء الناشطين في هذا المجال.

الجرائم الإلكترونية

تجارة المخدرات

على أثر التطور التكنولوجي المتسارع في مجال الاتصالات، تغيّر أسلوب المروّجين، بحيث لم يَعد الترويج مقتصراً على الوسائل التقليدية، بل أصبحت المواقع الإلكترونية، وشبكات التواصل الاجتماعي من أهم قنوات ترويج هذه الآفة، باختيار وسائل ومغريات لجذب الشبان.

إضافة إلى ذلك، هناك المخدرات الرقمية التي انتشرت مؤخراً، وهي عبارة عن مقاطع نغمات موسيقية يُستمع إليها عبر سمّاعات للأذنين تقوم ببث ترددات معينة في الأذن اليمنى وترددات منخفضة عنها بفارق محسوب في الأذن اليسرى، ما يُظهر الموجة الثالثة التي تُسمع ويكون لديها التأثير ذاته لذاك الذي ينتج عن تعاطي المخدرات التقليدية.

أسباب انتشارها:

- استخدام ألغاز وشيفرات وصور خاصة عبر حسابات مشبوهة بغية الإيقاع بالضحايا.
- نشر لقطات فيديو لإظهار المدمنين بحالة قوة وفرح دائم بهدف جذب الآخرين.
- عرض لكيفية صنع المخدرات ومعرفة أنواعها وأشكالها.
- امكانية استفسار المستهدف عن كيفية الحصول على المخدرات فيجد مَن يقوم بالرد عليه، وتعريفه على أنواع المخدرات أو الأدوية وترغيبه بها.

ما هي طرق الحماية إلكترونياً؟

- رقابة الأهل لأبنائهم ومواكبتهم على مواقع التواصل الاجتماعي من خلال معرفة أصدقائهم والاطلاع على الصفحات التي يتابعونها.
- حظر الصفحات والمواقع التي تنشر هذه الأنواع من المخدرات.
- الإبلاغ عن صفحات المخدرات الرقمية.
- تجنّب الأصدقاء الناشطين في هذا المجال.
- إبلاغ الجهات الأمنية المختصة بأي محاولة إقناع اي نوع بشراء اي نوع من أنواع المخدرات.

الجرائم الإلكترونية

الابتزاز الإلكتروني

هي عملية تهديد وترهيب للضحية بنشر صور أو مواد تصويرية (مقاطع فيديو) أو تسريب معلومات سرية تخص الضحية، بهدف ابتزازها لدفع مبالغ مالية أو استغلالها للقيام بأعمال غير مشروعة لصالح المبتزّين. وعادة ما يتم اصطياد الضحايا عن طريق البريد الإلكتروني أو وسائل التواصل الاجتماعي.

أسبابه:

- الكسب المادي.
- تسريب معلومات سرية.
- القيام بأعمال منافية للأخلاق.

كيفية تجنّب الوقوع في فخ الابتزاز

- تجنّبْ طلب صداقات أو قبول طلب صداقات من قبل أشخاص غير معروفين .
- عدم التجاوب مع أي محادثة ترد من مصدر غير معروف.
- تجنّبْ مشاركة معلوماتك الشخصية حتى مع أصدقائك في الإنترنت.
- رفض طلبات محادثات الفيديو مع أي شخص، ما لم تكن تربطك به صلة وثيقة.
- تجنب التفاعل والانجذاب للصور المغرية المريبة للشك.

في حال تعرّضك لعملية ابتزاز

- عدم تحويل أي مبالغ مالية، وعدم الإفصاح عن رقم البطاقة المصرفية.
- تجنّب المحادثات مع المبتزّ، وإبلاغ الجهات المعنية عند وقوع الحادثة.
- عدم التواصل مع الشخص المبتزّ، حتى عند التعرض للضغوط الشديدة.

الجرائم الإلكترونية

الإتجار بالبشر

هو عملية استدراج ضحايا عن طريق الخداع أو الإكراه، بهدف الإتجار بهم بين البلدان والمناطق، فيُحرَمون استقلاليتهم وحريتهم في التنقل والاختيار، ويتعرّضون لمختلف أشكال الإساءة الجسدية والنفسية. لقد أسهمت شبكة الإنترنت وعلى نحو كبير جداً في كسر حواجز الزمان والمكان أمام عصابات الإجرام وفي تيسير شؤون عملية الإتجار بالبشر، بين الدول المستوردة والدول المصدّرة، وأيضاً في ترويج الإعلانات الخاصة بالعصابات.

أهداف الإتجار بالبشر

- الإتجار لأغراض السخرة (العمل من دون أي بدل مادي).
- الإتجار بهدف الاستغلال الجنسي.
- الإتجار بأعضاء البشر.

الأسباب التي تقف وراء زيادة الإتجار بالبشر وبيع الأعضاء البشرية:

- انتشار الفقر والبطالة وتدهور الوضع الاقتصادي.
- استغلال هذا المجال لتحقيق أرباح هائلة.
- الحروب والنزاعات المسلحة والصراع السياسي.
- ازدياد معدلات اللجوء والهجرة الداخلية والخارجية .
- التقدّم الطبي العلمي والتقني وما حققه من إنجازات في نقل الأعضاء البشرية وزراعتها.
- تعدّد الأمراض وتنوعها وانتشارها، وزيادة أعداد المرضى المحتاجين إلى الأعضاء في أنحاء العالم.
- كثرة عدد الأطفال غير الشرعيين وأطفال الشوارع ما يجعلهم عرضة لسرقة أعضائهم.
- عدم وجود بدائل صناعية لبعض أعضاء جسم الإنسان.
- ضعف الرادع الاجتماعي والديني والأخلاقي لدى بعض فئات المجتمع.

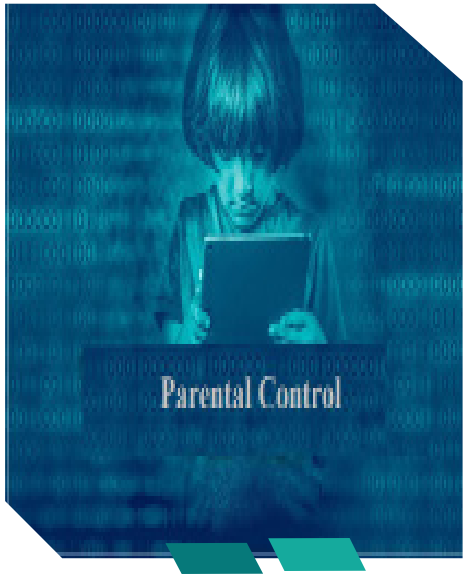
ما هي طرق الحماية منها؟

- تجنّب وحظر الصفحات والمواقع الإلكترونية التي تروّج للإتجار بالبشر، وإبلاغ الجهات المختصة عنها.
- مراقبة الأهل لأبنائهم على مواقع التواصل الاجتماعي من خلال معرفة أصدقائهم والصفحات التي يتابعونها.
- الوعي وعدم الانجرار وراء المحرّضين.
- لفت النظر والتنبيه إلى تجنب الوقوع ضحية لعمليات الإقناع وغسل الدماغ.

الجرائم الإلكترونية

إنترنت آمن للأطفال

- تعتبر توعية الأطفال وحمايتهم من مخاطر الإنترنت مسألة في غاية الأهمية. فالأطفال بمختلف أعمارهم يدخلون عالم الانترنت مستخدمين حواسيب ولوحات وهواتف ذكية بهدف اللعب والتسلية. إلا أنهم يجهلون مخاطر هذا العالم الواسع والغير محدود، بالتالي فإنهم عرضة للعديد من المنشورات والمحتويات السيئة التي تنعكس وتؤثر سلباً على حياتهم بمختلف جوانبها(العاطفية، النفسية، الإجتماعية ...). هنا يكمن دور الأهل الأساسي في أهمية مراقبة إستخدام أطفالهم للإنترنت و توعيتهم حول مخاطرها العديدة، أبرزها:



- التحرش والتعنيف المعنوي
- المواقع الإباحية
- التحرش الجنسي
- العنف والترهيب
- المحتوى الغير ملائم لبعض الألعاب الإلكترونية
- الإنعزال الاجتماعي
- العاب الميسر الغير شرعية و ما تخلفه من إدمان

إرشادات عامة للأهل؟

- التحقق من طريقة استخدام الأطفال للانترنت وفق أعمارهم
- استخدام برمجيات الحماية بهدف حصر المواقع المسموح بزيارتها وحظر المواقع الخطرة
- تشجيع الأطفال على الحوار ومناقشة ذويهم حول أية مشكلة يواجهونها اثناء إستخدام الإنترنت.
- توعية الأطفال وتحذيرهم حول خطر التواصل، محادثة، مشاركة صور لهم ، إفشاء معلومات شخصية (عنوان السكن، رقم الهاتف...) و لقاء أي شخص غريب او مجهول الهوية.
- العمل على بناء الثقة مع الأطفال للمحافظة على تواصل دائم فيما بينهم.
- مراقبة الأطفال من حين لآخر لمحاولة اكتشاف أيّة أمور مريبة يخفونها او يتعاملون معها بسريّة تامة.

1717

www.general-security.gov.lb

Lebanese General Security - المديرية العامة للأمن العام اللبناني

@DGSG_Security

everteam

EverteamGS
ever-team
@EverteamGS

KEEPING INFORMATION SAFE AND SECURE

THE LEADING SOLUTION PROVIDER
NEXT TO YOU

OUR **WORLDWIDE** CUSTOMER

- America
- Europe
- Middle East and Africa
- Asia and Pacific

SOME **FACTS ABOUT US**

- **25+** Years Experience
- **3000+** Customers
- **1000+** Employees Worldwide
- Validated by Major Analysts (Such as **Gartner**)

WHAT TYPE OF SOLUTION **ARE YOU LOOKING FOR?**

Data Management
- Data Integration
- Big Data Storage
- Content and File Analytics

Content Services
- Web App Studio
- Document Management
- Digital Assets Management

Process Services
- Dynamic Case Management
- Intelligent Business Process Management
- Correspondence Automation and Tracking

Information Governance
- Physical Archive
- Records Management
- GDPR Compliance

info@everteam-gs.com
www.everteam.com