بياناتك وصورك بأيدٍ خبيثة.. نصائح للتعامل مع الابتزاز الإلكتروني

الاثنين 4 فبراير 2019 09:02 م

في ديسمبر/كانون الأول 2018، عثرت عائلة الشابة الهندية ألينا (22 عاماً) على جثة ابنتهم معلقة في سقف غرفتها، وكشفت تحقيقات الشرطة عن أن الفتاة قررت الانتحار بعد أن هددها شاب يسكن في نفس منطقتها بنشر فيديوهات لها لأنها رفضت الزواج منه.

إن كنت تظنين أنك لا يمكن أن تقعي ضحية "الابتزاز الإلكتروني"، فربما أنت على خطأ، حتى لو لم تكوني ممن ينشرن صورهن وفيديوهاتهن على وسائل التواصل الاجتماعي، فقد تكونين صيدا سهلا لشخص قام باستعادة محتويات هاتفك الجوال بعد بيعه.

ويعرف "الابتزاز الإلكتروني" (Cyber-extortion) بأنه الحصول على مكاسب مادية أو معلومات من الأشخاص والشركات بالإكراه عن طريق التهديد بنشر أمور خاصة وبيانات سرية عبر مواقع التواصل الاجتماعي.

وتصل صورك وبياناتك الشخصية إلى الشخص المبتز إما عن طريق اختراق الحسابات الشخصية مثل فيسبوك وإنستغرام، أو استعادة محتويات الهاتف الجوال بعد بيعه، أو من خلال الضحايا أنفسهم، الذين قد يرسلون صورهم وفيديوهات لهم في أوضاع غير لائقة إلى آخرين (صديق أو حبيب)، والذي يستغل بدوره ما يمتلكه من محتوى للتهديد والحصول على ما يريد.

ويتم الأمر من خلال عصابات منظمة، تستخدم الفتيات في التواصل مع الضحايا عبر فيسبوك، وإغرائهم كي يرسلوا صوراً ومحادثات فاضحة.

ماذا تفعلين إذا تم ابتزازك؟

أولا: قبل كل شيء، لا تحاولي الرد على الشخص المبتز، أو إقناعه بعدم نشر صورك، فقد يجدك خائفة فيتمادى في مطالبه، وقد يجد لهجتك عنيفة معه فينفذ تهديده على الفور.

ثانيا: لا تستجيبي لطلبه أبدا، سواء بدفع المال، أو منحه معلومات بطاقتك البنكية، لأن استجابتك في المرة الأولى ستشجعه على طلب المزيد من المال، أو مزيد من الصور والفيديوهات.

ثالثا: لا تقومي بمسح المحتوى الذي يتم ابتزازك به، مهما كنت قلقة منه أو تشعرين بالخجل من ظهوره للعلن، ولا رسائل التهديد، لأنك بذلك تحذفين دليلاً ضد إدانة المبتز، وتجعلين الصور والفيديوهات بحوزته هو فقط.

رابعاً: وفي الوقت الذي لا يجب عليك التخلص من أدلة الإدانة، يجب عليك حظر (Block) الشخص المبتز من متابعة حساباتك على مواقع التواصل الاجتماعي، وتغيير كافة كلمات المرور الخاصة بحساباتك وبريدك الإلكتروني.

خامسا: لا تكوني بمفردك، ومن الأفضل أن تخبري شخصاً موثوقاً به بما حدث معك، ليقدم لك الدعم النفسي، حتى تتجاوزي هذه المحنة.

سادساً: لا تترددي في الاتصال بالجهات المعنية بالأمر، وهي هنا إدارة مكافحة الجرائم الإلكترونية، الموجودة بكافة الدول، فهي الجهة الأقدر والأسرع في التعامل مع مثل هذه الجرائم، ومن ثم توجيه اتهام رسمي للشخص المبتز.

ففي مصر، توجد إدارة لمكافحة جرائم الحاسبات وشبكات المعلومات، ويمكن الإبلاغ عن أي محاولات للابتزاز من خلال موقع وزارة الداخلية، أو من خلال الخط الساخن على الرقم 108.

وفي قطر من خلال الهاتف 2347444 أو على الخط الساخن 66811575. وفي الأردن يمكنك الإبلاغ عن الجرائم الإلكترونية من خلال الرقم المجاني 192. كما وفرت السعودية خطا ساخنا على الرقم 1909 للإبلاغ عن حالات الابتزاز.

وهي أيضاً متوفرة بدولة الإمارات من خلال موقع هيئة تنظيم الاتصالات وفي البحرين من خلال إدارة مكافحة الجرائم الإلكترونية وفي لبنان عن طريق خدمة "بلغ".

كيف تحمين نفسك من سرقة معلوماتك؟

1- اختاري كلمات سرية قوية لحساباتك على مواقع التواصل الاجتماعي، وهي الكلمات التي يصعب على المخترق تخمينها، بحيث تكون بعيدة عن اسمك وتاريخ ميلادك، وكذلك الأرقام 123 بشكل متتابع، وهي كلمات المرور التي يفضلها غالبا المستخدمون

2- لا تثقي في مواقع التواصل الاجتماعي، فمهما كان الشخص الذي ترسلين إليه صورك أو معلوماتك أمينا، وحتى لو نشرت صورا ترينها أنت فقط، فلن تضمني أن يتعرض حسابك للاختراق، وتصبح خصوصياتك كلها في متناول يديه

3- لا تجري محادثات فيديو في أمور خاصة مع شخص لا تعرفينه جيدا، خاصة إن كان حسابه أنشئ حديثا، فقد يجرك للحديث عن أسرار تخصك أو تخص غيرك، وتصبح في ما بعد وسيلة تهديد للحصول على المال أو لمعرفة المزيد من المعلومات

4- لا تكتفي بمسح الصور والأرقام والخروج من كافة حساباتك على جوالك قبل بيعه، فيجب عليك عمل "فورمات" (Format) للجهاز، ثم تشغيل كاميرا الفيديو وترك الهاتف في غرفة مظلمة مثلا حتى تمتلئ ذاكرة الهاتف الداخلية تماما وحينها سيغلق الهاتف الكاميرا تلقائياً، بعدها احذفي الفيديو، حتى تتأكدي من أن أي شخص سيحاول استعادة محتويات الكاميرا لن يجد سوى هذا الفيديو المظلم

وإذا رغبت في مزيد من التأكد، يمكنك من خلال موقع (Drfone) استعادة محتوى هاتفك لتعرف هل تم التخلص من كافة الصور والفيديوهات أم لا، وهو متوفر على نظامي (iOS) وأندرويد