الخليج

اقتصاد, أسواق الإمارات

14 أغسطس 2021 13:20 مساء

كيف تتفادى الاحتيال المالي ؟ .. 6 خطوات تضمن لك الحماية

ارتفعت في الآونة الأخيرة وتيرة عمليات الاحتيال المالي، وتعددت طرق المحتالين في خداع ضحاياهم، من انتهاك بيانات شخصية إلى سرقة الهوية وجرائم الاحتيال الإلكتروني عبر الشبكة العنكبوتية. وينصح الخبراء هنا بعدد من الخطوات يمكن للمرء اتباعها لتفادي الوقوع ضحية لجرائم الاحتيال المالي.

وفي ما يلي أبرز النصائح التي يمكن أن تساعدك على تجنب دروب المحتالين المتشعبة:

1 ـ لا تُحوّل أية أموال أبداً لأشخاص لا تعرفهم:

من منا لا يتلقى رسالة بريد إلكتروني مشبوه تحمل في طياتها وعوداً بثروة طائلة سواء أكانت الرسالة من أحد الأمراء في دول إفريقية أو من وريث لعائلة كبيرة لا يستطيع لسبب أو لآخر الحصول على ميراثه الموعود المحتجز في حسابات مصرفية في الخارج من دون مساعدتك لتحويل هذه الأموال الطائلة، مقابل وعد بمنحك جزءاً لا بأس به من هذه الثروة الضخمة.

وفي حال موافقتك لا بد طبعاً من أن يجد طريقة ما لإقناعك بتحويل مبلغ ما لحسابه، مبلغ بسيط طبعاً مقابل ما يعدك به من ثراء.

ويحذر الخبراء هنا من هذه الحيلة التي تعد اليوم الأقدم في كتاب النصب والاحتيال المالي العالمي، لكن ما زال يقع الكثير ضحية لها، ويؤكدون أنه ليس من الصحيح أبداً أن تحول أموال لغرباء تحت أي مسمى، أو في ظل أية ظروف، حتى على مستوى مطالبات المساعدة من أصدقاء قد يكون المحتال استولى على حساباتهم أو يقوم بإرسال البريد لك من حسابات شبيهة بأسمائهم، حسابات مزيفة طبعاً.

2 ـ لا تُفصح أو تشارك أبداً بياناتك المالية:

يجب أن تكون البيانات المالية والشخصية للمرء على درجة كبيرة من الخصوصية، وعلى الشخص ألا يشارك أبداً، بياناته المالية والمصرفية والشخصية مع جهات أو أشخاص لا يعرفهم حق المعرفة، وكذلك غض النظر عن طريقة تواصلهم معك سواء عبر البريد الإلكتروني أو الرسائل القصيرة أو وسائل التواصل المختلفة أو الاتصال الهاتفي.

والحيلة التي يقع فيها كثيرون تتعلق بالتحذير من توقف حساباتهم المصرفية أو بطاقات الصراف الآلي الخاصة بهم،

وغالباً ما يقعون ضحية في هذه الحالة ليشاركوا معلومات وبيانات يستغلها المحتال في القيام بعمليات شراء ببطاقاتهم الائتمانية أو ببطاقات الخصم. ويقول الخبراء إن على الشخص أن يدرك تماماً أن البنك الذي يتعامل معه لن يتصل به أبداً ليطلب منه بيانات مصرفية خاصة به على الهاتف.

3 ـ لا تضغط أبداً على الروابط التي تردك على البريد دون التحقق منها:

كثيراً ما ترد إلى الشخص رسائل بريد إلكتروني تعده بجائزة أو تخبره بوصول شحنة ما له على إحدى شركات الشحن أو غير ذلك من الحيل. وهنا لا بد من أن يتحقق من صحتها تماماً قبل الضغط على الرابط المرفق في الرسالة.

4 ـ اختر كلمة سر قوية يصعب التعرف إليها أو تحليلها:

يقوم كثيرون منا باعتماد كلمة سر وحيدة على جميع المواقع التي يشتركون فيها من بريد إلكتروني ومواقع تسوق وغيره، وهذا بالطبع يجعل مهمة المحتال على درجة كبيرة من السهولة، فأنت تسهل عليه مهمة الاحتيال عليك وتساعده على إنجازها بسرعة. وينصح الخبراء بتغيير كلمات السر بصورة دورية، وتنويع الكلمات المستخدمة بين المواقع المختلفة، بما يصعب عملية التعرف إليها وتحليلها، وهناك برامج تساعد على حفظ وتغيير كلمات السر المختلفة.

5 ـ حمّل برامج حماية من الفيروسات متطورة:

يؤكد الخبراء أهمية تحميل الشخص لبرامج متطورة للحماية من الفيروسات المختلفة وبرامج هجمات الفدية، وغيرها من وسائل اختراق الخصوصية، بما يكفل حماية البيانات والحسابات الخاصة من الهجمات العشوائية لقراصنة الإنترنت.

6 ـ لا تتسوق عبر مواقع مجهولة وتأكد من سلامة المواقع التي تزورها:

يحذر الخبراء من مخاطر التسوق الإلكتروني عبر مواقع مجهولة، ويؤكدون أنه على المرء فقط التسوق عبر المواقع .المعروفة، وعليه أيضاً أن يجري الأبحاث والدراسات الكافية لضمان سلامة المواقع التي يزورها

"حقوق النشر محفوظة "لصحيفة الخليج .2024 ©