الـرافـديـن يحـذر زبـائنة من الاحتيال الالكتروني



حذر مصرف الرافدين، اليوم السبت، زبائنه من الاحتيال الإلكتروني وأصدر عدة إرشادات.

وفق بيان صادر عن مصرف الرافدين تلقته المطلع: إن "المصرف يحرص على توعية زبائنه والجمهور حول الممارسات السليمة في استخدام الخدمات الإلكترونية بشكل عام، وتوجيه الزبون إلى أخذ الحيطة والحذر، درءاً للمخاطر التي قد تنتج عن أي محاولات للوصول إلى المعلومات الشخصية والمالية للزبون، من خلال الاحتيال الإلكتروني، والاحتيال الهاتفي، والفيروسات وبرامج التجسس، وسرقة الهوية".

وأضاف أن "مصرف الرافدين يوصي زبائنه الالتزام بالإرشادات التالية:

1- تجنب السهولة في معرفة كلمة السر، والحفاظ على سريتها، وتجنب استخدام كلمات سر شائعة ومعروفة يسهل التنبؤ بها وقم بتغييرها دورياً. ينصح المصرف زبائنه -من أجل أمنهم وسلامتهم- بالامتناع عن استخدام المعلومات المعروفة كتاريخ الميلاد أو رقم الهاتف أو أي جزء يسهل التعرف عليه من اسم الزبون ككلمة السر.

2- تجنب إفشاء كلمة السر والبيانات الشخصية والمحافظة على سرية رقم بطاقة الراتب (ماستر او فيزا كارد) والإنترنت البنكي وتطبيق الهاتف البنكي، وعدم إفشائها حتى لموظفي المصرف .

3- تحديث معلومات وبيانات الزبون الموطن راتبه أو غير ذلك كلما طرأ عليها تغيير من خلال الفروع.

4- التحقق بشكل مستمر من حركات حسابك (عن طريق كشف حساب، حركات في تطبيق الهاتف)، وفي حال الشك في أي منها قم بمراجعة فرعك أو قسم التوعية المصرفية وحماية الجمهور في الإدارة العامة للمصرف".

وأوضح المصرف أن "هنالك أمثلة على رسائل الاحتيال منها:

1- رسائل التصيد

تصلك هذه الرسائل عبر تقمص شخصية موظف في البنك الذي تتعامل معه، حيث يرسل إليك رسائل يطالبك فيها بمعلومات حول حسابك البنكي أو بطاقة الائتمان بحجة التأكد من أرقامها.

2- الاحتيال عبر خدعة من تصفح حسابك

الكثير من المستخدمين تم الإيقاع بهم على الشبكات الاجتماعية من خلال حيلة "اعرف من تصفح حسابك على فيسبوك" أو أي شبكة اجتماعية أخرى.

3- رسائل الفوز بالجوائز

تزعم مثل هذه الرسائل بأنك فزت بجوائز قيمة أو رحلة إلى بلد ما، ويطلب منك صاحب الرسالة دفع مبلغ معين لاستلام جائزتك، لا تفعل ذلك أبداً.

4- الاحتيال عبر جمع التبرعات

جمع الأموال بصورة مخادعة، حيث ينشر هؤلاء المحتالون قصصاً وهمية حول حاجة مريض للعلاج أو أسرة فقيرة أو غيرها وطلب تبرعات من رواد الشبكات الاجتماعية.

5- عروض الوظائف عبر الإنترنت

في حال تقدمت بطلب عمل لوظيفة عبر الإنترنت، سيطلب منك حتماً ملئ استمارة الطلب، يمكنك فعل ذلك ولكن احذر من تدوين رقم حسابك البنكي وبطاقة الائتمان".

ولفت المصرف الى "نصائح للحماية من محاولات النصب والاحتيال كما يلي:

أ- لا تتفاعل مع الأشخاص الذين يطلبون منك دفع مبلغ مالي بسيط للحصول على جائزة أو هدية وغيرها من العروض.

ب- تأكد من هوية الأشخاص الذين يراسلونك بسبب حالة طارئة مع إدعائهم أنهم من أصدقائك أو اقربائك.

ت- الرسائل التي تتضمن أخطاء املائية ونحوية هي موضع شك دائماً ويجب عليك الحذر منها.

ث- إن كنت ترغب بتقديم مساعدة أو عون، فافعل ذلك من خلال الجهات الرسمية والموثوقة.

ج- لا تثق في الصفحات التي تمثل شركات كبيرة أو شخصيات عامة والتي لم تقم بالتحقق منها.

ح- لا تثق في أي صفحات اجتماعية تدعي أنها ستحقق لك الربح السريع من خلال الإنترنت أو العمل من المنزل.

خ- لا تقم بالضغط على الروابط التي تصلك عبر واتساب أو شبكات التواصل أو تلك التي يتم نشرها في التعليقات.

د- لا توافق على نقل محادثة مع شخص معين لخارج شبكات التواصل، كالتواصل عبر واتساب أو تقديم عنوان البريد الإلكتروني لهذا الشخص".

وأكد المصرف على، "أخذ إجراءات الحيطة والحذر لتفادي الوقوع ضحية الأساليب الجرمية التي تهدف للاحتيال على المواطنين وسرقة أموالهم من خلال قيام أشخاص بانتحال صفة موظفين عاملين في مؤسسات مالية أو مؤسسات دولية أو شركات خاصة، ومن ثم يقومون بما يلي:

1- التواصل مع الزبائن عبر وسائل التواصل الاجتماعي (فيسبوك، انستجرام، واتساب) بذريعة تقديم مساعدات وجوائز مالية أو رواتب شهرية لمدة محددة، وذلك مقابل الحصول على المعلومات الشخصية للمعتمد وبيانات وصورة البطاقة المصرفية الممنوحة له والرقم السري ورمز التحقق OTP.

2- استخدام البيانات والمعلومات اللازمة لإنشاء حسابات باسم الزبائن أو تعديل بيانات حساباتهم أو تحديث بياناتهم أو طلب الرقم الذي سوف يصلك برسالة SMS، ومن ثم تنفيذ عمليات تحويل إلكتروني لغايات تسديد فواتير ومشتريات وشحن أرصدة هاتف نقال أو إجراء تحويلات مالية إلكترونية لأشخاص آخرين.

3- التواصل مع الأشخاص المستفيدين من التحويلات المالية بذريعة تنفيذها لصالحهم عن طريق الخطأ، ومن ثم الطلب منهم القيام بعكس المبلغ عن طريق التحويل لحساب معين أو شحن رصيد هاتف محدد".