المركزي العراقي يحذر من الاحتيال الإلكتروني ويطلق آليات جديدة لحماية الحسابات

كشف البنك المركزي العراقي، اليوم الأحد، عن آليات متعددة لاستقبال شكاوى المواطنين ومتابعتها مع المصارف وشركات الدفع والجهات المعنية، في ظل تزايد حالات الاحتيال الإلكتروني، مؤكداً تشديد الرقابة الإلكترونية والميدانية على القطاع المالي، إلى جانب حملات توعية مستمرة لتعزيز الثقافة المصرفية.

وأوضح حيدر غازي، مدير إعلام البنك المركزي العراقي في تصريح تابعته المطلع، أن:"البنك يستقبل الشكاوى عبر منصته الإلكترونية الرسمية ومنصة (أور) الحكومية، حيث يتم فرزها وتحويلها إلى المصارف أو شركات الدفع الإلكتروني لاتخاذ الإجراءات اللازمة وإبلاغ البنك بها تمهيداً لإعلام المشتكين".

وأضاف أن:"الرقابة تُنفذ على مستويات متعددة، تشمل الرقابة الإلكترونية عبر المقسم الوطني الذي يربط جميع المؤسسات المصرفية والمالية وشركات الدفع الإلكتروني، إلى جانب الزيارات الميدانية المفاجئة والتدقيق الدوري للملفات والمعاملات".

كما أكد غازي أن، عمل البنك يستند إلى قوانين وتعليمات رسمية منشورة على موقعه الإلكتروني.

ومن جهتها، شددت آمال الشويلي، مديرة إعلام مصرف الرشيد، على أن:"حماية حسابات الزبائن من الاحتيال الإلكتروني تمثل أولوية قصوى".

وأوضحت أن:"المصرف يعتمد أنظمة رقابية متطورة تمنع الوصول غير المشروع إلى بيانات العملاء"، مؤكدة أن:"المصرف لا يطلب أي معلومات شخصية أو سرية عبر المكالمات الهاتفية أو الرسائل النصية"، داعية المواطنين إلى عدم التفاعل مع الروابط المجهولة والإبلاغ فوراً عن أي حركة مشكوك فيها.

وأما محمد علي، معاون مدير قسم الشؤون المالية والتوعية المصرفية في شركة "كي كارد"، فأوضح أن:"غالبية حالات الاحتيال المالي الإلكتروني تعود لمشاركة المواطنين لبياناتهم السرية أو رموز التحقق مع جهات غير موثوقة".

ونوه بأن:"النظام الإلكتروني للشركة هو الجهة الوحيدة المخوّلة بإرسال رسائل الدخول أو رموز التحقق الخاصة بالتحويلات، وأن أي رسائل من خارج هذا النظام تُعد غير رسمية"، مشيراً إلى أن معظم عمليات الاحتيال تتم عبر روابط وهمية أو صفحات تنتحل صفة جهات مانحة للتبرعات أو الهدايا أو القروض.

وأكد علي استمرار التنسيق مع البنك المركزي لتنفيذ حملات توعية واسعة، تشمل التحذير من صفحات النصب الإلكتروني والتوعية الميدانية المباشرة، بهدف حماية الأموال والحسابات المصرفية، وتعزيز الشمول المالي والحد من مخاطر الاحتيال الإلكتروني.