

شدد بنك الكويت المركزي على البنوك المحلية بتطوير آليات المراقبة على العمليات المالية المنفذة عن طريق ترميز البطاقات التي تستخدم في المحافظ الإلكترونية مثل «آبل باي» و«سامسونج باي» وغيرها، وذلك من خلال اعتماده نهجاً يدمج بين تقنيات ترميز البطاقات وتحليل البيانات المتقدم لتحسين أمان العمليات المصرفية، مع التركيز على تتبع السلوك والموقع والتكرار للكشف عن الاحتيال والتصدي له بشكل استباقي. وطالب بنك الكويت المركزي البنوك في كتاب رسمي بشأن الضوابط الأمنية على ترميز البطاقات، والذي اطلعت عليه «الأنباء»، بوضع اشتراطات أمنية فعالة على أنظمة المراقبة لدى البنوك مثل سلوك العميل والموقع الجغرافي للعمليات المراد تمريرها والتكرار في تلك العمليات.

وتستخدم عملية ترميز البطاقات لتحسين أمان معاملات الدفع الإلكتروني، من خلال استبدال معلومات البطاقة الحساسة، مثل رقم البطاقة الكامل (PAN)، برمز «Token»، والذي يستخدم لإتمام المعاملات بدلا من استخدام بيانات البطاقة الأصلية، مما يقلل من خطر اختراق البيانات أو إساءة استخدامها.

وتظهر الاشتراطات التي طالب «المركزي» بوضعها، أنه يحث البنوك على استخدام تقنيات المراقبة والتحليل المتقدم لتحسين أمان العمليات المنفذة لمنع الاحتيال، والتأكد من أن العمليات المالية تنفذ بشكل آمن ومشروع بالتركيز على تحليل الأنماط وتقييم العمليات بناء على عدة معايير أمنية لضمان شرعيتها لتحديد الأنشطة المشبوهة وإيقاف العمليات غير المشروعة قبل تنفيذها.

وترتكز آليات التأمين التي طالب «المركزي» بتطبيقها على 3 عناصر للمراقبة والتحليل تبدأ بسلوك العميل من خلال تحليل أنماط إنفاقه المعتادة مثل المبلغ، نوع العمليات، وأوقات تنفيذها، وإذا كانت العملية تختلف بشكل كبير عن النمط المعتاد مثل شراء بمبلغ كبير أو من تاجر غير مألوف، يتم تنبيه النظام أو إيقاف العملية للتحقق.

ويتمثل العنصر الثاني في الموقع الجغرافي من خلال التحقق من موقع تنفيذ العملية مقارنة بالموقع المعروف للعميل، فإذا كانت العملية تجرى من بلد أو منطقة مشبوهة أو بعيدة عن مكان العميل المعتاد، يمكن رفضها أو طلب تأكيد إضافي.

ويتمثل العنصر الثالث في التكرار بالعمليات، وذلك من خلال مراقبة عدد العمليات المتتالية خلال فترة زمنية قصيرة، فإذا زادت العمليات بشكل غير طبيعي مثل محاولات دفع متكررة بفارق زمني ضئيل فقد يكون هذا مؤشرا على نشاط احتيالي.

ودعا «المركزي» البنوك إلى استحداث آلية تمكن العميل من الاختيار بتفعيل خدمة إضافة البطاقات المصرفية على المحافظ الإلكترونية مثل محفظة (Apple Pay, Samsung Pay)، على أن تكون الخدمة غير مفعلة بشكل تلقائي لجميع العملاء، وعدم إجراء أي من المعاملات المرتبطة بالبطاقات المرمزة في حال عدم قيام العميل بتفعيل هذه الخدمة بشكل مسبق، ومنها على سبيل المثال عدم إجراء إرسال رمز التحقق لمرة واحدة (OTP) الخاص بإضافة البطاقة المصرفية على المحافظ الإلكترونية.

ولفت «المركزي» في كتابه إلى أنه في حال قام العميل بإضافة بطاقته المصرفية إلى المحفظة الإلكترونية لترميز البطاقة مثل محفظة (Apple Pay, Samsung Pay) من خارج تطبيق البنك، فإنه يتعين تنفيذ الاجراءات التالية:

- وضع خطوة امنية إضافية لتفعيل البطاقة المصرفية من خلال المصادقة عبر تطبيق البنك، مع إيضاح سبب المصادقة.

- إيقاف طلبات الإضافة من خارج تطبيق البنك الناشئة من خارج الكويت، ما لم يتم العميل بالتواصل مع البنك لتأكيد إضافة البطاقة

من جانبه.

وشدد «المركزي» على البنوك بإضافة قائمة على تطبيق البنك تمكن العميل من الاطلاع على البطاقات الخاصة به والمعرفة في أي من المحافظ الإلكترونية مثل (Apple Pay, Samsung Pay) محمداً بها أنواع الأجهزة التي تمت عملية التفعيل من خلالها مثل ( iPhone, Android Phone, Smart Watch).

وأكد «المركزي» على البنوك بضرورة الالتزام بالمادة (32) من تعليمات تنظيم أعمال الدفع الإلكتروني للأموال الصادرة في مايو 2023، والتي تنص على «وضع السياسات والإجراءات والنظم والضوابط اللازمة للكشف عن الاحتيال وآلية التعامل معه، وإبلاغ الجهات المختصة عن الحالات والتقارير المتعلقة بالاحتيال، مع إخطار البنك المركزي بصفة مستمرة عنها وفق المدة والصيغة التي يحددها»، مطالباً بالالتزام بتطبيق ما ورد في كتابه وموافاته بالخطة الزمنية اللازمة للانتهاء من ذلك.