

كاسبرسكي: 257 ألف تهديد مالي تعرض لها مستخدمو «المدفوعات» الرقمية في الإمارات



أظهر استطلاع أجرته «كاسبرسكي» حول المدفوعات الرقمية، أن 18% من المشاركين في الشرق الأوسط تعرضوا لخسائر مالية مرتبطة بالتهديدات عند استخدام الخدمات المصرفية عبر الإنترنت، وخدمات المحافظ المحمولة. وخسرت أغلبية المستخدمين (92%) ما يصل إلى 1,000 دولار أمريكي بسبب هذه الحوادث، و(8%) تعرضوا لخسارة تجاوزت قيمتها 1,000 دولار.

ووفقاً لشبكة كاسبرسكي الأمنية، فقد تبين أنه تم حظر ما يزيد على 1.8 مليون تهديد مالي في الشرق الأوسط من قبل كاسبرسكي، ونحو 257 ألف تهديد مالي في دولة الإمارات. وفي العادة، يكون الهدف من هذه الهجمات سرقة المعلومات المالية، بما في ذلك أرقام بطاقات الائتمان، وبيانات تسجيل الدخول، وتعتمد في العادة على أساليب الهندسة الاجتماعية لجذب الضحايا.

ومع ذلك، لا يقتصر تأثير التهديد السيبراني الذي يستهدف المدفوعات الرقمية على الأعباء المالية التي يتكبدها المستهلكون فقط، ولكنه يطال أحوالهم النفسية أيضاً. وعلى سبيل المثال، قال 62% من المشاركين في الاستطلاع إنهم عانوا من صعوبات في النوم، وانتابتهم حالة من القلق الشديد بشأن احتمال استرداد أموالهم. وعبر العدد نفسه من المشاركين عن تدهور ثقتهم إزاء الجهات المزودة لخدمات الدفع الرقمي. وذكر 60% أنهم أصبحوا أكثر يقظة بعد تعرضهم لهذا النوع من الحوادث الإلكترونية، بينما لجأ 73% منهم إلى الاستعانة بالحلول الأمنية، مع تثبيتها على أجهزتهم، لمواجهة الفيروسات التي قد تصل إلى أجهزتهم.

• إطار عمل

وقال متحدث باسم فريق تكنولوجيا المعلومات لدى شركة اللولو للصرافة: «تعد المدفوعات الرقمية بمثابة العمود الفقري لعالم التجارة المعاصر، لكنها أصبحت هدفاً رئيسياً للتهديدات الإلكترونية. لذا يتعين على جميع الأطراف ذات الصلة، بما في ذلك الجهات المزودة للخدمات والعملاء، على حد سواء، أن يتحملوا المسؤولية، وتحديدًا عن طريق توخي الحذر، إلى جانب اتخاذ مختلف التدابير الاستباقية، بما يضمن لهم الحماية من مخاطر التهديدات الأمنية. ومن منطلق منظور تنظيمي بحت، نعتقد أن بناء إطار عمل قوي للحوكمة الإلكترونية، يعتبر من أفضل الطرق التي تضمن العمل بطرق آمنة ومسؤولة وأخلاقية، في الوقت الذي يمكننا فيه الحفاظ على ثقة العملاء، وغيرهم من الأطراف المعنية».

ومنذ ظهور جائحة «كورونا»، تعرّض 53% من المستخدمين في الشرق الأوسط وتركيا وإفريقيا لدى «كاسبرسكي»، إن جميع أصحاب استخدام نظم المدفوعات الرقمية. ولهذا السبب، تزداد أهمية معرفة سبل التفاعل بشكل آمن مع أي تقنيات ناشئة، بما في ذلك الخدمات المصرفية عبر الإنترنت وخدمات المحافظ المحمولة.

• نظام آمن

قال عماد حفار، رئيس الخبراء التقنيين لمنطقة الشرق الأوسط وتركيا وإفريقيا لدى «كاسبرسكي»، إن جميع أصحاب المصلحة، بما في ذلك المؤسسات الحكومية والجهات المزودة لخدمات الدفع الرقمي والمستخدمون، وحتى شركات الأمن السيبراني، تكون بحاجة إلى العمل معاً لإنشاء نظام دفع مستدام وآمن.

• حلول آمنة

:ولمساعدة المستخدمين في دولة الإمارات على تبني تقنيات الدفع الرقمي بأمان، يقترح خبراء «كاسبرسكي» ما يلي

1. تجنب مشاركة رقم التعريف الشخصي، أو كلمة المرور، أو أي معلومات مالية أخرى، مع أي شخص، سواء كان متصلاً، أو غير متصل بالإنترنت.
2. تجنب استخدام أي شبكة «واي فاي» عامة لإجراء أي معاملات عبر الإنترنت.
3. استخدم بطاقة ائتمان أو خصم منفصلة لإجراء معاملاتك عبر الإنترنت. وضع حداً للإنفاق على البطاقة.
4. للمساعدة في تتبع المعاملات المالية.
5. احرص دائماً على التسوق من المواقع الرسمية والموثوقة.
6. على جميع أجهزتك التي Kaspersky premium استخدم أحد حلول الأمان التي يمكن الوثوق بها، مثل.
7. تستخدمها في معاملاتك المالية. ومن شأن ذلك أن يساعد على اكتشاف الأنشطة الاحتيالية، أو المشتبه فيها،

والتحقق من مستوى الأمان على المواقع التي تزورها

• توصيات

أما بالنسبة إلى المطورين والبنوك والشركات التي تعمل في مجال تقديم خدمات الدفع الرقمية، فإن «كاسبرسكي» توصي بضرورة اتباع الإجراءات التالية

أولاً: الاستثمار في حلول الأمن السيبراني الشاملة التي يمكن أن تساعد في الكشف عن الاحتيال عبر مستويات متعددة من عمليات الدفع عبر الإنترنت ونقاط الاتصال مع المستهلكين

على المؤسسات المالية، (APT) ففي ظل تزايد الهجمات المعقدة التي تشنها مجموعات التهديدات المستمرة المتقدمة تبرز الحاجة إلى الرؤية المتعمقة والذكاء للتعامل مع التهديدات كعاملين ضروريين لحماية العملاء وضمان استمرارية مفيداً لدعم فرق تقنية المعلومات في تحليل Kaspersky Threat Intelligence الأعمال. ويكون استخدام خدمة التهديدات والحد من مخاطرها

ثانياً: تنظيم التدريبات المستمرة لنشر التوعية الإلكترونية للموظفين بشكل مستمر، من أجل مساعدتهم على معرفة علامات الخطر التي يجب البحث عنها حال تعرض المؤسسة لهجمات من هذا النوع، وفهم دورهم في حماية المؤسسة