استطلاع عالمي: 55% من مستخدمي الإنترنت داخل المملكة واجهوا عمليات احتيال

2 يوليو، 2026

كشفت نتائج استطلاع رأي عالمي جديد، عن أن أكثر من نصف مستخدمي الإنترنت داخل المملكة العربية السعودية 55%، قد تعرضوا لمحاولات احتيال خلال العام الماضي، في حين وقع حوالي 62% منهم، ضحية لهجمات استهدف حساباتهم وبياناتهم، مثل اختراق حسابات مواقع التواصل الاجتماعي، وتسريب البيانات، أو الإصابة بالبرمجيات الخبيثة.

ورصدت نتائج استطلاع الرأي، تغير مشهد الاحتيال الرقمي باستمرار، في ظل ظهور أساليب أكثر تطوراً واستهدافاً، مدعومةً بتقنيات الذكاء الاصطناعي، محذرة من تزايد هذه العمليات باستمرار، وتعرض المستخدمين الدائم لمخاطر محتملة في معظم أنشطتهم على الإنترنت، بداية من رسائل البريد الإلكتروني وتطبيقات المراسلة، مروراً منصات

التواصل الاجتماعي، ووصولاً إلى المتاجر الإلكترونية والتطبيقات.

واعتمد استطلاع الرأي، في رصده للبيانات وتحليلها، على تقنيات الذكاء الاصطناعي، وتعليم الآلة لتوفير حماية فعّالة للمستخدمين، وتفعيل هذه التقنيات ضمن قسم مخصص بتطبيقات كاسبرسكي، على نظامي ويندوز وmacOS، لتسهيل الوصول إليها وتعزيز تجربة الاستخدام، موضحة أنها قد نجحت بالفعل في التصدي لهجمات التصيد الاحتيالي، وحظر أكثر من 140 مليون محاولة تصيد خلال الربع الأول من عام 2026 فقط، وهو ما يؤكد الانتشار المتزايد للتهديدات عبر شبكة الإنترنت.

ويشهد الاحتيال الإلكتروني توسعاً ملحوظاً، في ظل التحولات العالمية، ففي مارس 2026، رصدت تقنيات مكافحة التصيّد زيادة في الأنشطة الاحتيالية المرتبطة بكأس العالم 2026، بما في ذلك مواقع مزيفة تنتحل صفة المنصات الرسمية للبطولة، لاستدراج المستخدمين للقيام بإجراءات غير آمنة، حيث أوضح خبراء كاسبرسكي أن هذه التقنيات تدمج بين تعلم الآلة، وتحليل الأنماط السلوكية، والتحليل اللحظي للتهديدات، ما يتيح للأنظمة اكتشاف نطاق واسعٍ من أساليب الاحتيال، بدءاً من حملات التصيّد التقليدية، مروراً بالمتاجر المزيفة، وصولاً إلى عمليات الاحتيال المرتبطة بالعملات الرقمية وغيرها من المخططات التي تهدف إلى إحداث خسائر مالية مباشرة.

وأوضح خبراء التقنية، أن حملات الاحتيال الإلكتروني، تستند بالوقت الحالي، على بيانات شخصية مسروقة من اختراقات سابقة، أو برمجيات سرقة المعلومات، أو حسابات مخترقة، أو غيرها من أشكال التعرض الرقمي، إذ يستغل المحتالون هذه البيانات في إنشاء رسائل موجهة، أو انتحال شخصيات موثوقة، أو زيادة مصداقية محاولاتهم الاحتيالية، وفي هذا السياق، يقدم حل كاسبرسكي بريميوم، حماية متقدمة ضد مختلف التهديدات السيبرانية عبر جميع الأجهزة، بما في ذلك الهواتف الذكية، وذلك من خلال تقنيات أمنية مصممة لكل منصة ومدعومة بالذكاء الاصطناعي وتعلم الآلة، كما ويتضمن أدوات للكشف عن تسرب البيانات وسرقة الهوية والتي تنبه المستخدمين إلى أي تعرض محتمل لمعلوماتهم الشخصية، بالإضافة إلى حل مدير كلمة السر من كاسبرسكي، لحماية بيانات الاعتماد وإنشاء كلمات مرور فريدة، وتقنيات الحماية السلوكية مثل System Watcher التي تعتمد على مراقبة سلوك التطبيقات وتحليل الأنماط لاكتشاف الأنشطة المشبوهة لحظياً.

ودمجت التطبيقات على على نظامي ويندوز وmacOS، هذه الإمكانيات في وحدة خاصة للحماية من الاحتيال تعتمد على الذكاء الاصطناعي، مما

يجعل استخدامها أكثر بساطة ووضوحاً، بينما تستمر هذه الوظائف في العمل تلقائياً في الخلفية على تطبيقات الأجهزة المحمولة.

من جانبها، قالت مارينا تيتوفا، نائبة رئيس قسم أعمال المستهلكين لدى كاسبرسكي، إن عمليات الاحتيال أصبحت معتمدة على الذكاء الاصطناعي، لتفرض واقعاً جديداً لا يمكنٍ تجاهله؛ لأنها تُنتَج بالذكاء الاصطناعي، وتزداد انتشاراً وحجماً باستمرار، وتظهر في كل مكان، بدءاً من مواقع بيع التذاكر المزيفة وصولاً إلى انتحال هوية الأصدقاء عبر تطبيقات المراسلة، مشيرة إلى أن الهجمات قادرة على خداع حتى أكثر المستخدمين خبرة، وبالتالي لم تعد قدرة الفرد على اكتشاف الاحتيال كافية، ولهذا السبب قدمت الشركة حلولاً جديدة، عبر دمج تقنيات الكشف بالذكاء الاصطناعي داخل منتجاتنا، لتتمكن تقنياتنا من اكتشاف ما قد تعجز العين البشرية عن رؤيته، وتوفير الحماية الفورية للمستخدمين.