محافظ المحمول في مهب الاحتيال دولة تدفع الناس إلى الدفع الرقمي ثم تترك أموالهم مكشوفة لمكالمات مجهولة تمتص مدخراتهم

الأحد 15 مارس 2026 09:00 م

يكشف تصاعد شكاوى الاحتيال على محافظ الدفع عبر الهاتف المحمول خللًا فادحًا في منظومة الحماية والرقابة، لا مجرد سلوك إجرامي فردي. فالسوق التي تضم نحو 46,291,000 محفظة نشطة، وتستحوذ فيها فودافون كاش وحدها على 55% من المحافظ، تحولت إلى مساحة واسعة للاستدراج الهاتفي وسرقة الأموال، بينما يبقى المستخدم هو الحلقة الأضعف والأخسر دائمًا.

وتقوم الحيلة على مكالمة من رقم مجهول يدّعي الانتساب إلى شركة اتصالات، ثم تخويف العميل من وقف المحفظة أو تعطيلها أو طلب "تحديث عاجل"، قبل دفعه إلى مشاركة كود تحقق أو تنفيذ خطوة تمنح المحتال القدرة على السحب أو التحويل. ما يتكرر هنا ليس مجرد نصب تقليدي، بل فشل مزمن في بناء بيئة دفع رقمي تحمي الناس قبل أن تكتفي بنصحهم بعد وقوع الكارثة.

احتيال واسع وسوق بلا حماية

تزايدت الشكاوى لأن المحتالين صاروا يعتمدون على سيناريو ثابت وفعال: لهجة رسمية، اسم شركة كبيرة، رسالة خوف عاجلة، ثم كود على الهاتف. هذه الطريقة تستغل الثقة في المؤسسات أكثر مما تستغل الجهل التقني، ولذلك يقع فيها مستخدمون عاديون لا يملكون أدوات التحقق ولا يحصلون أصلًا على تحذير واضح ومكثف ومفهوم قبل استخدام الخدمة.

الخطر هنا أكبر من القصص الفردية. حين يكون هذا العدد الضخم من المحافظ متداولًا يوميًا بين ملايين المصريين، فإن ترك الحماية الفعلية عند مستوى "لا تشارك الكود" يعني أن الدولة وشركات الاتصالات دفعت المواطنين إلى الاعتماد على أداة مالية واسعة الانتشار من دون بناء طبقات ردع كافية توازي هذا الانتشار.

الجهاز القومي لتنظيم الاتصالات نفسه حذر من مشاركة رموز التحقق، وأكد أن الهجمات الحديثة تعتمد على أساليب خداع المستخدم عبر الرسائل أو المكالمات أو الروابط، كما شدد على أهمية الوعي بأي سلوك غير معتاد على الهاتف. لكن صدور التحذير بحد ذاته يثبت أن الخطر قائم وممتد، وأن المواطن ما زال يواجهه فرديًا في حين يفترض أن تكون الحماية مدمجة داخل الخدمة لا مرهونة بانتباه الضحية وحده.

المشكلة في النظام لا في الضحية

السلطة اعتادت تحميل المستخدم المسؤولية الكاملة: لا تضغط، لا ترد، لا تشارك، لا تثق. لكن هذه الصيغة تخفي المشكلة الأصلية، وهي أن النظام نفسه يسمح بأن تكون مكالمة واحدة مدخلًا لتحريك أموال أو الاستيلاء عليها أو استدراج صاحبها إلى إجراء خطر من دون حواجز ردع كافية.

الدكتور شريف هاشم، الذي شغل رئاسة المكتب التنفيذي للمجلس الأعلى للأمن السيبراني ونائب الرئيس التنفيذي للجهاز القومي لتنظيم الاتصالات سابقًا، قال إن الأمن الرقمي صار ضرورة للأفراد والمؤسسات والحكومات، وحذر من أن تكرار الهجمات أمر وارد ما لم تُبن قدرات حقيقية وخطوط دفاع فعالة. هذا الكلام يعني بوضوح أن النصيحة الفردية لا تكفي، وأن الحماية يجب أن تُبنى على مستوى المنظومة ذاتها.

ومن زاوية أكثر مباشرة، أوضح المهندس أحمد طارق، خبير أمن المعلومات، أن طرق الاحتيال لا تتوقف عند منصة بعينها، وأن الاختراق كثيرًا ما يمر عبر "الهندسة الاجتماعية" أو "فن اختراق البشر"، أي استغلال الخوف والثقة والارتباك لدفع المستخدم إلى تسليم ما يريده المحتال بنفسه. عندما تعرف الجهات الرسمية والخدمية هذه الحقيقة، ثم تترك العميل وحده أمامها، فهذه ليست فجوة وعي فقط، بل فجوة مسؤولية أيضًا.

بمعنى آخر، الدولة لم تفشل فقط في القبض على النصابين سريعًا، بل فشلت قبل ذلك في فرض تصميمات أكثر أمانًا، ورسائل تحذير إجبارية داخل التطبيقات، وآليات إيقاف فوري، ومراجعات دقيقة للمعاملات المشبوهة، ونظام تعويض واضح للضحايا. ولذلك يبدو الخطاب الرسمي أقرب إلى التنصل من المسؤولية منه إلى تحملها.

الهندسة الاجتماعية تسرق لأن الردع أضعف

الخبير وليد حجاج شرح كيف تُدار بعض عمليات الاحتيال والاختراق عبر تخويف الضحية أو دفعه إلى إدخال رمز أو PIN، بما يفتح الطريق أمام تحويل الأموال أو السيطرة على التطبيق أو الجهاز. جوهر الفكرة هنا أن المهاجم لا يحتاج دائمًا إلى كسر تقني معقد، بل إلى ثغرة بشرية يعرف كيف يصنعها بخوف مصطنع ورسالة عاجلة ولهجة واثقة.

هذا يفسر لماذا تتكرر المكالمات نفسها وتنجح بالأسلوب نفسه. النصاب يعرف أن المستخدم يسمع اسم شركة الاتصالات فيرتبك، ويعرف أن ثقافة الحماية ما زالت محدودة، ويعرف أيضًا أن آليات الردع اللاحقة بطيئة وغامضة ولا تعيد المال سريعًا، فيكسب من هشاشة البيئة كلها لا من ذكائه وحده.

الأخطر أن هذا النمط لا يمس فئة محددة فقط. هو يضرب كبار السن، والعمال، والطلاب، وربات البيوت، وكل من صار الهاتف بالنسبة له بنكًا صغيرًا وحافظة نقود يومية. ومع اتساع الاعتماد على المحافظ الإلكترونية في تحويل الأموال ودفع الفواتير والشراء، يصبح ترك هذه الفجوة مفتوحة شكلًا مباشرًا من أشكال تعريض مدخرات الفقراء والمستخدمين العاديين للخطر اليومي.

مسؤولية قانونية غائبة ومستخدم يدفع الثمن

الدكتور محمد حجازي، استشاري تشريعات التحول الرقمي، قال إن قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 هو الإطار الأساسي لمواجهة الجرائم الإلكترونية في مصر، وأشار إلى أن القانون يضع بعض المسؤوليات على مقدمي الخدمات للوصول إلى المتهم ومنع تسهيل الجريمة. هذه النقطة مهمة لأنها تؤكد أن المسألة ليست فراغًا قانونيًا، بل فجوة في التفعيل والردع والتنفيذ العملي.

إذا كان القانون موجودًا، والتحذيرات الرسمية موجودة، والخبراء يكررون منذ سنوات أن الهندسة الاجتماعية من أخطر أدوات الاحتيال، فلماذا ما زال المستخدم هو من يكتشف الجريمة بعد وقوعها؟ ولماذا لا توجد منظومة معلنة وسريعة لاسترجاع الأموال، أو تجميد المعاملة المشبوهة لحظيًا، أو مساءلة صارمة للجهات التي تدير الخدمة إذا ثبت قصور أدوات الحماية أو الإنذار المبكر؟

الحقيقة القاسية أن الدولة تريد مجتمعًا رقميًا يدفع ويتحول ويستهلك عبر الهاتف، لكنها لا تريد أن تتحمل الكلفة السياسية والرقابية لبناء حماية تليق بهذا التحول. لذلك يجد المواطن نفسه أمام معادلة مختلة: خدمة تتوسع كل يوم، ومخاطر تتوسع معها، ونصائح عامة بعد كل واقعة، بينما المال المسروق لا يعود بسهولة والثقة نفسها تنزف مع كل مكالمة جديدة.

لهذا لا تبدو أزمة محافظ المحمول في مصر مجرد ملف احتيال عابر. إنها دليل إضافي على طريقة إدارة تعتبر المستخدم ساحة تجريب، وتعتبر الحماية عبئًا مؤجلًا، وتترك أموال الناس رهينة لصوت مجهول على الهاتف.