Source:
Byte

Cada día millones de interacciones digitales suceden en todo el mundo y, con ellas, se multiplican también las oportunidades para el fraude. Lo que antes eran simples estafas con mensajes mal escritos, hoy se ha transformado en un negocio global impulsado por algoritmos, herramientas de Inteligencia Artificial y estructuras criminales que operan como auténticas empresas tecnológicas. Así lo advierte Facephi en su nuevo Fraud Intelligence Report 2025, donde analiza cómo el Fraud as a Service (FaaS) se ha consolidado como una industria clandestina de escala global.

“Cada interacción digital es una oportunidad para los delincuentes. El cibercrimen se ha sofisticado hasta el punto de replicar el comportamiento humano y burlar los controles tradicionales. Por eso, es necesario adoptar una visión que ponga la protección de la identidad en el centro. No basta con validar un rostro, hay que proteger todo el ciclo de vida de la identidad”, advierte Javier Mira, CEO de Facephi.

El fraude como servicio, una nueva industria global

El concepto Fraud as a Service define un modelo de negocio en el que los ciberdelincuentes ofrecen, de forma estructurada y profesional, paquetes completos con herramientas, tutoriales y soporte técnico para ejecutar ataques. Este modelo ha democratizado el acceso al fraude digital, permitiendo que cualquier persona con conocimientos básicos pueda participar en operaciones de robo de identidad, phishing o creación de cuentas falsas.

El Fraud Intelligence Report 2025 de Facephi subraya que esta tendencia ha convertido al fraude de identidad en uno de los delitos más rentables. Según datos del World Economic Forum, el impacto económico del cibercrimen alcanzará los 10,5 billones de dólares anuales este año, con la suplantación de identidad como principal impulsor. La facilidad con la que se pueden adquirir kits de fraude y servicios de deepfakes en la dark web ha llevado la amenaza a un nivel sin precedentes.

La identidad, el nuevo perímetro de la ciberseguridad

Durante años, las empresas han invertido en proteger sus redes y sistemas, pero Facephi considera que este enfoque ha quedado obsoleto. La compañía propone un nuevo paradigma, el Identity First Security, en el que la identidad digital del usuario se sitúa como el eje principal de toda estrategia de seguridad.

Este modelo parte de una premisa clara, la identidad ya no es un conjunto de datos o un documento, sino una llave personal que abre la puerta a todos los servicios digitales. De ahí que sea esencial garantizar que cada interacción esté verificada en tiempo real, utilizando tecnologías de autenticación continua basadas en biometría e inteligencia predictiva.

Facephi defiende que la seguridad debe construirse alrededor de la identidad, no de los sistemas. Para ello, propone una arquitectura integral que combine prevención, detección y respuesta frente a tres grandes frentes del fraude digital, la suplantación de identidad, la apropiación de cuentas (Account Takeover o ATO) y el fraude autorizado, como las denominadas cuentas mula.

Una radiografía del fraude digital y sus sectores más expuestos

El ámbito bancario encabeza la lista, con un incremento de los ataques de apropiación de cuentas mediante el uso de deepfakes o documentos falsos. Las fintech y los neobancos también sufren el impacto de la automatización del fraude, especialmente en los procesos de alta de usuarios, donde proliferan las identidades sintéticas

.

El sector del gaming es otro de los más golpeados, debido a la creación masiva de cuentas falsas desde granjas de dispositivos que buscan aprovechar promociones, bonos o alterar sistemas de recompensa. Esta tendencia se ha visto reforzada por la disponibilidad de bots generativos capaces de simular comportamientos humanos en juegos y plataformas online.

Facephi alerta además de que el cibercrimen como servicio está poniendo a prueba la capacidad de respuesta de los marcos regulatorios. La falta de una legislación armonizada, los vacíos legales en torno a los delitos digitales y la dificultad para rastrear operaciones transnacionales están creando un entorno de impunidad que favorece la expansión del fraude.

Identidad verificable, confianza digital y futuro seguro

El modelo Identity First no solo busca prevenir ataques, sino también generar confianza en los entornos digitales. En un contexto en el que la autenticidad de cada usuario se ha vuelto crítica, garantizar una identidad verificable se convierte en un requisito indispensable para operar con seguridad.

Facephi propone una seguridad sin fricciones, donde la autenticación sea continua, invisible para el usuario y respaldada por un “ADN digital” único que se actualiza con cada interacción. Este enfoque, basado en

inteligencia artificial y aprendizaje automático, permite anticiparse a los intentos de fraude antes de que ocurran, reforzando la protección de las empresas y de los ciudadanos.

Disponible en:

https://revistabyte.es/actualidad-it/fraude-ia-seguridad/ [1]

Links
[1] https://revistabyte.es/actualidad-it/fraude-ia-seguridad/