La mitad de las compañías tiene dificultades para gestionar el fraude digital durante la pandemia

Más de la mitad (51%) de las empresas en Europa, Oriente Medio y África (EMEA) afirman que no son capaces de hacer frente a las nuevas amenazas de fraude, según revela un nuevo estudio. El Informe de Fraude EMEA de Experian, compañía tecnológica especializada en datos, software de decisión y analítica avanzada, constata que más de un tercio de las compañías (38%) no cree que pueda afrontar con éxito el fraude en todos sus canales, y el 42% cree que sus recursos para la prevención del fraude son insuficientes actualmente.

Sin embargo, casi nueve de cada diez (89%) considera que la gestión del fraude es una prioridad dentro de su empresa, lo que pone de manifiesto una preocupación real dentro de las empresas por abordar de forma rápida y efectiva las problemáticas relacionadas con el fraude.

Los datos apuntan a un aumento específico en tres tipos de fraude: el sim-swapping, un fraude mediante el cual los ciberdelincuentes roban la identidad de los usuarios a través del secuestro del número de teléfono al obtener un duplicado de la tarjeta SIM; el phishing, un tipo de fraude en el que los ciberatacantes engañan a los usuarios para que compartan información confidencial como datos, contraseñas o números de tarjetas de crédito, y el robo de cuentas.

UNA DE CADA TRES EMPRESAS DECLARÓ QUE EL VOLUMEN DE FRAUDE AL QUE SE ENFRENTAN HA AUMENTADO MÁS RÁPIDO QUE EL NÚMERO DE EMPLEADOS

Algo menos de la mitad (un 49%) de los responsables en la gestión del fraude y el riesgo en las empresas considera imprescindible garantizar un enfoque equilibrado en su estrategia de prevención, y solo uno de cada cinco considera crucial la inversión en inteligencia de dispositivos, verificación de correo electrónico, IA, aprendizaje automático o en una mayor automatización, de cara a gestionar y detener de forma efectiva los ataques fraudulentos.

Como dato positivo, del informe se extrae que los departamentos responsables de esta área tienen como aspiraciones clave para combatir el fraude, por un lado, la mejora de la prevención (en el 62% de los casos) y, por otro, la integración del aprendizaje automático en la optimización de modelos (en el 48% de los casos).

También hay una clara determinación de aumentar los conocimientos y el perfil de la actividad en prevención del fraude en casi la mitad (47,8%) de las empresas encuestadas. La preocupación en torno al trabajo aislado de los diferentes departamentos también es evidente. En este sentido, más de uno de cada cuatro equipos (28%) desea aumentar las interacciones con otros departamentos, incluidos los de TI, compliance y marketing.

LOS CASOS DE ESTAFAS TELEFÓNICAS CRECEN EXPONENCIALMENTE

Diversas marcas han visto cómo su imagen era utilizada para engañar a los usuarios. Microsoft, por ejemplo, ha habilitado una página para víctimas de una estafa en la que el usuario recibe una llamada de un supuesto técnico, que le avisa de una incidencia en su ordenador.

Colectivos vulnerables, como las personas que se enfrentan a desalojos, son víctimas de falsas ONG´s o entidades de caridad y personas que tratan de conseguir ayuda financiera, reciben ofertas para conseguir financiación, por supuesto, falsa.

Otro caso habitual es el de los estafadores que se hacen pasar por representantes de la compañía de electricidad, gas o agua, ofreciendo revisiones o falsas incidencias y solicitan los datos personales y bancarios para solucionar los supuestos problemas.

Por otro lado, la pandemia y las cuestiones de salud relacionadas con la COVID-19 se han convertido en la excusa perfecta para los delincuentes. Rastreadores falsos se ponen en contacto con sus víctimas, comunicándoles que han estado en contacto con un positivo. Les recomiendan un test casero gratuito, pero solicitan el número de tarjeta de crédito para cubrir los gastos de envío. Las vacunas a domicilio para ancianos también son un cebo recurrente.

ESPAÑA A LA CABEZA EN FRAUDES ONLINE

España se sitúa a la cabeza mundial en engaños, estafas y fraudes online: el país es el tercer objetivo más atractivo para los ciberdelincuentes, por detrás de EEUU y Alemania, según un estudio del centro de formación Ironhack, realizado en más de 30 países. El fraude online durante la desescalada fue un 95% superior a la media mundial y un 45% mayor que la media europea.

Fuente: Zona Movilidad