BioCatch

4 Formas en las que los estafadores financieros obtienen ventaja

BioCatch

El fraude a medida que avanza el año 2022

Los desarrollos globales recientes han creado amplias oportunidades para que los ciberdelincuentes se aprovechen de las personas vulnerables, e incluso de aquellas que tradicionalmente no eran vulnerables. La pandemia de COVID-19 amplió el uso de los canales digitales para la banca diaria, a la vez que los consumidores de todo el mundo adoptaron otros servicios, incluidos los pagos digitales, los pagos sin contacto y sin efectivo, y los servicios de comprar ahora y pagar después (Buy Now Pay Later, BNPL). El año pasado, el 93 % de los consumidores usó uno o más métodos de pago digitales[1], como Zelle, e hizo casi $100 000 millones en compras con el servicio BNPL[2]. Sin mencionar que los programas de estímulo del gobierno crearon flujos de efectivo inusuales que estaban listos para que los estafadores se aprovecharan de ellos.

El 93 % de los consumidores utilizaron uno o más métodos de pago digitales en 2021

Cada institución financiera se esfuerza por anticiparse a los estafadores para proteger a los clientes contra pérdidas financieras y preservar su reputación y marca. Sin embargo, la naturaleza dinámica del delito cibernético hace que la práctica de gestión del riesgo de fraude sea un desafío considerable. ¿Cómo será el panorama del fraude a medida que avanza el año 2022?

En este libro electrónico se analizarán cuatro formas en las que los estafadores financieros obtienen ventaja, incluidas las tácticas que están utilizando, los objetivos que son más vulnerables y las limitaciones de los controles de fraude actuales. Además, evaluaremos cómo las instituciones financieras pueden contraatacar.

CUATRO FORMAS EN LAS QUE LOS ESTAFADORES FINANCIEROS OBTIENEN VENTAJA

BioCatch

1 La ingeniería social y el estafador moderno

La ingeniería social no es un hecho nuevo, pero sigue siendo un método efectivo para que los estafadores logren el resultado deseado. La investigación de BioCatch muestra que las estafas de ingeniería social aumentaron un 57 % el año pasado y están presentes en uno de cada tres casos de fraude en la adquisición de cuentas. La mayoría de las estafas que involucran ingeniería social requieren cierta interacción para que un usuario divulgue información personal, descargue malware en su dispositivo móvil o proporcione una contraseña de acceso único que le permitirá al estafador eludir la autenticación de múltiples factores. Estas son algunas de las tácticas de ingeniería social que utilizan los estafadores para mantenerse un paso adelante.

Las estafas de ingeniería social aumentaron **un 57 %** en 2021

Smishing

El phishing por mensaje de texto, también conocido como smishing, es una forma de ataque de ingeniería social que se dirige a las víctimas a través de los teléfonos inteligentes. Un ataque de smishing utiliza mensajes de texto que parecen provenir de una organización legítima y, en la mayoría de los casos, contienen un enlace que lleva al usuario a un sitio de phishing. En los casos de smishing más recientes se envían mensajes directos a los consumidores en los cuales se los alerta sobre fraude o algún otro problema en su cuenta para obtener una respuesta. Una vez que un usuario responde, el estafador lo contactará a través del teléfono móvil y afirmará ser personal del banco.

El smishing ha aumentado en gran proporción en todo el mundo y las quejas sobre spam de mensajes de texto aumentaron más del 140 % el año pasado[3]. El smishing sigue siendo una gran preocupación, ya que los usuarios pasan mucho tiempo en sus dispositivos móviles: un promedio de cinco horas por día en 2021[4]. Además, la capacidad de concretar un ataque de smishing se ha vuelto más fácil con estafadores capaces de llegar a miles de víctimas potenciales en minutos y la posibilidad de usar bots de mensajes de texto para interceptar la contraseña de acceso único que la mayoría de los bancos utilizan para la autenticación adicional.

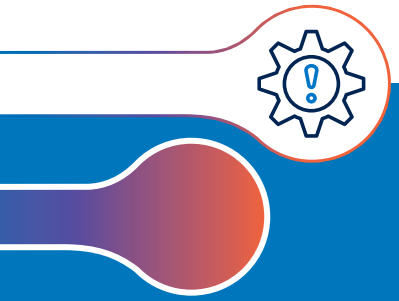
Estafas de voz

Las estafas de voz no son una estrategia completamente nueva, pero su éxito está dando como resultado una expansión a nivel mundial de esta táctica de estafa. Si bien las primeras estrategias de estafa financiera se centraron principalmente en clientes vulnerables, como los ancianos, cada vez son más los clientes más jóvenes, que valoran la comodidad por encima de la privacidad, los que se convierten víctimas. Este método de ingeniería social no es difícil de realizar para los estafadores, pero puede ser muy difícil de detectar, ya que el estafador no interactúa directamente con la plataforma bancaria y, en cambio, convence al usuario para que realice una acción. Por ejemplo, el fraude de pago automático autorizado es uno de los tipos más frecuentes de estafas de voz. En estos casos, se convence a un usuario de realizar un pago o una transferencia a una cuenta controlada por el delincuente.

El 35 % de las estafas de imitación de voz implica un pago superior a $1000

Estafas de acceso remoto

Los estafadores financieros han mejorado sus estrategias a estafas híbridas de múltiples capas que van mucho más allá de simplemente guiar a un objetivo para que realice una transacción. Esto suele ocurrir cuando se trata de herramientas de acceso remoto. Por ejemplo, un estafador puede comenzar con una estafa de voz de ingeniería social y luego cambiar de táctica para obligar a un objetivo a descargar una aplicación en su teléfono. Esta aplicación en realidad es un software que le permite a un delincuente obtener acceso remoto a su dispositivo. La metodología detrás de las técnicas de cambio o combinación está diseñada para eludir los controles de seguridad del banco e incluso obtener acceso a información personal o de cuenta adicional.



Conclusión clave

A medida que el consumidor moderno ha logrado superar los antiguos trucos de estafa, el estafador moderno se ha vuelto más sofisticado. Las estafas de ingeniería social han evolucionado para comprender las inclinaciones y tendencias humanas y se han vuelto a elaborar para dirigirse a los consumidores en los momentos exactos y con los métodos correctos. Las medidas de prevención del fraude heredadas, que dependen del dispositivo, la IP o los atributos de la red ya no son suficientes para los estafadores que han aprendido a eludirlas o falsificarlas, y se requieren nuevos enfoques que brinden una visibilidad más profunda del riesgo en una sesión digital.

BioCatch

2

El nuevo "cliente vulnerable"

Si bien cualquier persona con una cuenta bancaria, una tarjeta de crédito y acceso a Internet es una posible víctima de fraude financiero, algunos consumidores son más vulnerables a los estafadores. La Autoridad de Conducta Financiera (FCA) del Reino Unido define a un cliente vulnerable como "una persona que, debido a sus circunstancias personales, es especialmente susceptible de sufrir daños, en especial cuando una empresa no actúa con los niveles adecuados de atención". La vulnerabilidad del cliente está impulsada por cuatro factores: salud, acontecimientos de la vida, resiliencia y capacidad, y esa vulnerabilidad puede ser transitoria o continua, en virtud de los acontecimientos de la vida, la capacidad y la salud. Los principales eventos mundiales que han impactado a todos, combinados con el avance de las técnicas de estafa, han hecho evolucionar la idea del "cliente vulnerable" hasta volverse mucho más amplia.

Clientes mayores

Si bien hay una serie de nuevos "clientes vulnerables", los clientes mayores siguen siendo un objetivo principal para las estafas financieras. Los clientes mayores siempre han sido un grupo demográfico vulnerable principal, ya que se los conoce por tener un mejor crédito y más fondos, tienden a ser más confiados y no están familiarizados con las nuevas tecnologías digitales. Otra característica es que es menos probable que denuncien incidentes de fraude por vergüenza. Se estima que a las personas mayores las estafan con más de $3000 millones cada año[5], con una pérdida media de $600 por víctima mayor de 60 años y hasta $1600 por víctima mayor de 80 años.

Los métodos para estafar a las personas mayores se han vuelto más frecuentes, con las estafas románticas, estafas de impostores y estafas de sorteos y loterías como las principales en la lista. El fraude en la apertura de cuentas también es un tipo importante de fraude para este grupo demográfico. Los datos relacionados con el fraude de BioCatch revelan que el 40 % de las víctimas de fraude de terceros son personas nacidas antes de 1960.

El 40 % de las víctimas de fraude de terceros tienen una edad declarada superior a los 60 años

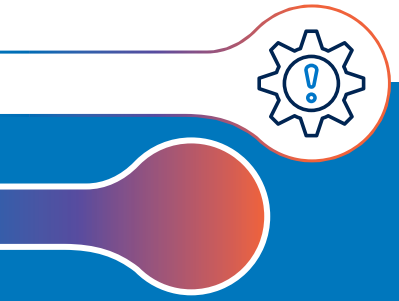
El 78 % de aumento de titulares de cuentas menores de 21 años que indican señales de actividad de mulas de dinero

Generación Z

Si bien los clientes de edad avanzada suelen ser el objetivo principal de los delitos financieros, la demografía se ha expandido de forma significativa hacia las generaciones más jóvenes. La pandemia global estimuló lo que se conoce como la Gran Renuncia, en la que millones de trabajadores en todo el mundo renunciaron a sus trabajos. La Generación Z ha liderado la carga con generosos pagos de estímulo del gobierno y beneficios por desempleo, que prolongan la búsqueda de empleo. Las redes sociales también han hecho que sea cada vez más fácil para los responsables de las mulas conectarse con los jóvenes. Muchos de los jóvenes reclutados en esquemas de lavado son menos cómplices, necesitan dinero rápido y fácil, pero no entienden por completo la legalidad de lo que se les pide que hagan.

Protección regulatoria

Las agencias gubernamentales son muy conscientes de los nuevos peligros de las estafas financieras dirigidas a grupos vulnerables. Como resultado, en este último tiempo aumentó la presión de los grupos de acción regulatorios y de consumidores para proteger a los clientes vulnerables y de edad avanzada. Por ejemplo, la FCA publicó nuevas recomendaciones en 2021 para clientes vulnerables y poblaciones que envejecen en áreas donde las sucursales bancarias físicas se están cerrando y cambian a los canales digitales. La FDIC también se ha interesado en proteger a los clientes vulnerables, en especial a los ancianos, mediante la creación del programa Money Smart para adultos mayores a fin de aumentar la conciencia entre las personas mayores y sus cuidadores para prevenir la explotación financiera de las personas mayores.



Conclusión clave

La industria financiera está dando pasos importantes para crear un entorno en el que las personas mayores y otras poblaciones vulnerables puedan realizar transacciones en un entorno libre de fraude. Con un mayor escrutinio regulatorio en todo el mundo, algunas instituciones financieras ya han comenzado a anticiparse al problema mediante la formación de grupos internos dedicados a atender a los clientes vulnerables. Además, se han formado grupos de la industria, como The Knoble, para identificar las mejores prácticas para los requisitos de detección e intercambio de datos dentro de las instituciones financieras, con el objetivo de combatir los delitos financieros, como las estafas a personas mayores. La tecnología que aprovecha el aprendizaje automático y la comprensión del comportamiento humano será un elemento fundamental para proteger a las poblaciones de clientes vulnerables.

BioCatch

3 Malware móvil en movimiento

Con el aumento del uso de dispositivos móviles, el acceso a Internet móvil y las aplicaciones móviles, no debería sorprender que el malware móvil esté regresando. A medida que los bancos, los minoristas y otros proveedores de servicios al consumidor buscan llegar a sus clientes en el lugar donde se encuentran, los estafadores también han adaptado sus estrategias. El uso de la autenticación de múltiples factores en dispositivos móviles ha creado brechas para que los atacantes con capacidades tecnológicas intervengan en momentos clave sin ser detectados y secuestren el sistema operativo o roben información personal y financiera con el objetivo de cometer fraude.

Las herramientas de acceso remoto se detectan en **1 de cada 24** casos de fraude móvil

Si bien el malware móvil no es tan frecuente como hace unos años, es mucho más específico y está mejor desarrollado. FluBot y TeaBot fueron dos de las familias más comunes de malware financiero dirigido a usuarios móviles el año pasado y aún se mantienen. El malware se propaga principalmente a los usuarios a través de bosquejos de aplicaciones falsas, como los servicios de entrega de paquetes, y continúa distribuyéndose en gran medida en Europa y Australia.

Las capacidades de acceso remoto son comunes en el malware financiero. Específicamente, TeaBot aprovecha las capacidades de los troyanos de acceso remoto (RAT) que permiten el registro de teclas, la interceptación de contraseñas de acceso único (OTP) y la recolección de otros datos contenidos en un dispositivo infectado. El malware se adapta a muchos idiomas y la lista de aplicaciones específicas aumenta a un ritmo acelerado.

Si bien la mayoría del malware móvil aún se dirige a los dispositivos Android, en gran parte debido a los sistemas abiertos de Google para el desarrollo y la distribución de aplicaciones, los estafadores han encontrado nuevas formas de eludir las medidas de seguridad de Apple para atacar los dispositivos iOS. Por ejemplo, dado que iOS no permite el control remoto de un dispositivo, los estafadores han sorteado este control con herramientas similares al acceso remoto, como Zoom, AnyDesk y TeamViewer. Los estafadores obligan a los usuarios a usar una de estas herramientas y compartir sus pantallas para que el estafador pueda guiarlos de manera más efectiva a través de una estafa. BioCatch se refiere a este método de ataque como una estafa de acceso remoto pasivo, y descubrió que más del 80 % de los casos de acceso remoto informados de iOS contienen esta característica de transmisión de pantalla positiva. Esto significa que el acceso remoto pasivo se estaba transmitiendo por varias pantallas para completar mejor el proceso de estafa.

Conclusión clave

El malware móvil es solo otro método que utilizan los estafadores para eludir los controles de fraude heredados y tomar el control de la cuenta. La detección de malware en dispositivos móviles se ha basado en gran medida en las tecnologías de escaneo antivirus (AV) tradicionales que buscan el nombre del paquete sospechoso y monitorean de forma periódica las aplicaciones y sus funciones de hash en busca de malware. Sin embargo, la tecnología en sí tiene limitaciones, ya que los archivos de malware cambian con frecuencia y las instituciones financieras no tienen control sobre el dispositivo del usuario final, por lo que incluso si pudieran ofrecer este servicio a los clientes, la adopción sería, en el mejor de los casos, esporádica. Las instituciones financieras deben mirar más allá del propio dispositivo y considerar controles de fraude basados en el comportamiento para detectar el malware móvil. Como el malware se comporta de manera muy diferente a la población de usuarios reales, y estos indicadores son comunes en la mayoría de las familias de malware, los comportamientos indicativos de malware se pueden descubrir en acciones como rutas de navegación, datos del acelerómetro y patrones de tocar y deslizar.

BioCatch

4 Los estafadores se volvieron más inteligentes. Los métodos de autenticación no tanto.

A medida que los estafadores se vuelven más inteligentes acerca de su enfoque para cometer fraude, las instituciones financieras aún luchan por mantener el ritmo. Los métodos heredados de prevención del fraude todavía se basan en gran medida en contraseñas, ID de dispositivos y contraseñas de acceso único a través de mensaje de texto, que aún son susceptibles a la intervención de los estafadores. El reemplazo de los métodos tradicionales de autenticación de usuarios es muy poco probable debido a su implementación global y aceptación por parte de los consumidores. Sin embargo, se deben reconocer sus limitaciones para detectar ingeniería social, malware y otras estafas avanzadas. Como resultado del aumento en el fraude basado en estafas, las instituciones financieras requieren soluciones que puedan ir más allá de los atributos basados en el dispositivo, la IP y la red y, en cambio, centrarse en el propio usuario.

Los entes reguladores en el Reino Unido reconocieron la vulnerabilidad de las contraseñas de acceso único y la autenticación basada en el conocimiento desde el principio para cumplir con la Directiva de Servicios de Pago II (PSD2). En 2021, la Oficina del Comisionado de Información del Reino Unido adoptó el uso de la tecnología biométrica del comportamiento como un factor de adherencia para una autenticación sólida de los clientes. En Singapur, una serie de ataques recientes de smishing que dieron como resultado pérdidas de millones de dólares llamó la atención de los reguladores financieros, que tomaron medidas inmediatas, como exigir a las instituciones financieras que eliminen los enlaces de todas las comunicaciones con los clientes.

Mayores expectativas del consumidor, mayor riesgo comercial

Los consumidores han desarrollado mayores expectativas de protección por parte de sus bancos e instituciones financieras, incluida la expectativa de recibir un reembolso por las pérdidas asociadas con actividades de fraude o estafa. Sin embargo, los riesgos asociados con el delito cibernético son mucho mayores que las pérdidas financieras. Los consumidores se ofenden exponencialmente cuando sienten que sus datos financieros no cuentan con la protección suficiente, y sus quejas pueden llevar con rapidez a daños en la reputación y pérdida de clientes.

Las instituciones financieras también han dado grandes pasos para mejorar la experiencia del cliente y las comunicaciones en los últimos años. El delito cibernético afecta directamente su capacidad para brindar la comodidad y la personalización que los clientes esperan en los canales digitales, y lo último que desean es comprometer estos esfuerzos al agregar más fricción o limitar la forma en que se comunican y comercializan nuevos productos y servicios.

"Continuar insistiendo en que los clientes evadan múltiples obstáculos para demostrar que son dignos de una relación comercial ignora la realidad de que los clientes hoy en día tienen múltiples opciones disponibles. Para muchos clientes, la conveniencia es un factor más importante que la seguridad de sus decisiones diarias".

Gartner, Don't Treat Your Customer Like a Criminal (No trate a su cliente como un delincuente), julio de 2021

Conclusión clave

Entre la amplia disponibilidad de información personal y financiera robada para la venta en el mercado negro y los métodos de ataque que aprovechan el malware, las herramientas de acceso remoto y la ingeniería social, las debilidades de los métodos tradicionales de autenticación de usuarios han quedado expuestas. Además, la experiencia del usuario y la comodidad están cada vez más en el centro de los nuevos proyectos de detección de fraude, por lo que la tecnología que puede abordar una variedad de casos de uso de fraude al tiempo que presenta un recorrido sin fricciones para la mayoría de los buenos usuarios impulsará futuras estrategias de autenticación.

BioCatch

Protección financiera más inteligente que los estafadores

Sin duda, la detección de fraudes financieros ha avanzado más en los últimos años, pero últimamente parece que los estafadores van un paso adelante. En lugar de continuar reaccionando a los ataques de delitos cibernéticos, es hora de dar un giro y que las instituciones financieras dicten de manera proactiva el futuro de la protección para sus clientes y para ellos mismos.

La única forma de hacerlo es estar al tanto de lo que sucede en la industria y adoptar por completo las estrategias, tecnologías y soluciones que tendrán el mayor impacto en la protección del cliente preparada para el futuro. En la actualidad, la biometría del comportamiento de BioCatch ofrece resultados extraordinarios para las organizaciones, incluidas 25 de las 100 principales instituciones financieras del mundo, y expone los ataques de fraude más avanzados.

La biometría del comportamiento funciona de forma pasiva en el contexto de una sesión web o móvil del usuario para monitorear miles de parámetros, como la forma en que una persona sostiene el teléfono, la presión que usa cuando escribe, cómo se desplaza o alterna entre campos y cómo navega a través de una aplicación o formulario. Debido a que las interacciones de cada persona con un dispositivo o aplicación son únicas, la biometría del comportamiento puede diferenciar entre las actividades de un usuario genuino y las actividades de un estafador.

El 64 % de los casos confirmados de fraude en la apertura de cuentas indicaron una falta de familiaridad con los datos personales

CUATRO FORMAS EN LAS QUE LOS ESTAFADORES FINANCIEROS OBTIENEN VENTAJA

Casos de uso para la banca y los pagos

BioCatch

El riesgo: Fraude en la apertura de cuentas

La solución: *Las brechas en las soluciones actuales están dejando puntos ciegos en el proceso de apertura de cuentas. Por ejemplo, en los casos en los que un cliente no tiene una relación previa con la organización, la mayoría de los controles de prevención de fraude heredados no cuentan con los datos históricos para identificar si un solicitante es bueno o malo. La biometría del comportamiento no requiere una relación existente y detecta aplicaciones de alto riesgo al buscar patrones como alta fluidez en la aplicación, poca familiaridad con los datos y análisis de la edad.*

El riesgo: Adquisición de cuentas

La solución: *La adquisición de cuentas se presenta de muchas formas capaces de eludir la mayoría de los controles de autenticación y prevención de fraude actuales. La biometría del comportamiento busca anomalías en las interacciones digitales que pueden indicar ataques tanto de humanos como no humanos, como malware, bots, herramientas de acceso remoto y métodos manuales de adquisición de cuentas.*

El riesgo: Detección de cuentas mulas

La solución: *Identificar cuentas mulas es un desafío porque, en algunos casos, involucra una cuenta genuina y las acciones del titular de una cuenta genuina. Los comportamientos asociados con una cuenta mula variarán según el nivel de complicidad y la etapa del recorrido de la banca digital. BioCatch ha desarrollado un enfoque único para descubrir la actividad de mulas mediante la identificación de cinco personajes de mulas. Cada uno de estos personajes exhibe diferentes patrones de comportamiento y está destinado a alinearse con los tipos de mulas que normalmente se observan operando dentro de las instituciones financieras. La biometría del comportamiento se puede utilizar para distinguir entre comportamientos que son mucho más comunes en mulas que en usuarios que abren cuentas legítimas o acceden a sus propias cuentas por razones legítimas.*

El riesgo: Estafas de ingeniería social

La solución: *Muchas estafas de ingeniería social pasan desapercibidas porque es el usuario real el que realiza el pago bajo la dirección de un estafador. La capacidad de detectar cambios sutiles en el comportamiento digital para sugerir que una víctima puede estar actuando bajo coerción o siendo guiada a través de una sesión es clave para detener las estafas de ingeniería social en tiempo real. La biometría del comportamiento analiza factores como la duración de la sesión, la segmentación de escritura, la vacilación y el desplazamiento del dispositivo para determinar si la intención de un usuario es legítima o sugiere que puede tratarse de una estafa de ingeniería social.*

ACERCA DE BIOCATCH

BioCatch es líder en la biometría del comportamiento, que analiza el comportamiento físico y cognitivo de un usuario en línea para proteger a los usuarios y sus activos. Nuestra misión es desbloquear el poder del comportamiento y brindar información procesable para crear un mundo digital donde la identidad, la confianza y la facilidad de uso coexistan sin problemas. Las principales instituciones financieras de todo el mundo utilizan BioCatch para combatir el fraude de forma más eficaz, impulsar la transformación digital y acelerar el crecimiento empresarial. Con más de una década de experiencia en el análisis de datos, más de 60 patentes y una experiencia antifraude sin igual, BioCatch continúa innovando para resolver los problemas del mañana. Para obtener más información, visite www.biocatch.com.

1 Chase Bank

2 Cornerstone Advisors

3 Comisión Federal de Comunicaciones de los EE. UU.

4 ZDNet, "We spent 5 hours a day on our mobile devices in 2021" (Pasamos cinco horas al día en nuestros dispositivos móviles en 2021), enero de 2022

5 Consumer Affairs

BioCatch