Visa Consulting & Analytics

CÓMO COMBATIR LAS NUEVAS AMENAZAS CIBERNÉTICAS

Qué pueden hacer las empresas para anticiparse a combatir las crecientes amenazas de los cibercriminales

El delito cibernético evolucionó: pasó de ser grupos poco organizados que atacaban a personas aisladas a ser una actividad criminal que involucra redes de actores bien entrenados y con todos los recursos, cuyo objetivo son los activos tecnológicos de las grandes corporaciones y su infraestructura interconectada para acceder a los datos con fines malintencionados.

Hoy, estos grupos organizados identifican las vulnerabilidades del ecosistema para sacar ventaja a escala industrial. Los cibercriminales son innovadores, ágiles y veloces para adoptar nuevas tecnologías y utilizarlas como objetivo. Cuando detectan una oportunidad, escalan los ataques para maximizar su éxito.

Los últimos meses fueron ideales para los cibercriminales. Debido al aumento de pagos digitales y al surgimiento de casos de uso de banca abierta con API, su territorio de ataque se extendió considerablemente.

En este artículo, Visa señala cuáles son las amenazas cibernéticas existentes y qué pueden hacer las empresas para combatirlas. Si las organizaciones tienen su objetivo en la mira, pueden anticiparse a las amenazas, combatirlas e implementar defensas.

Qué es el delito cibernético en el entorno de pagos

El delito cibernético es una actividad criminal en las que los computadores o la Internet son el origen, el objetivo o el lugar de desarrollo de un crimen.

En el contexto de los pagos, se refiere a toda actividad fraudulenta que tenga como objetivo los sistemas de pago digitales y las compañías que operan en el ecosistema de pagos.

El delito cibernético también incluye el robo de las credenciales de pago cuyo almacenamiento o procesamiento es a través de computadores y redes; el uso de credenciales de pago comprometidas para realizar pagos digitales, como los de *eCommerce*; y el uso de sistemas de pago digitales para monetizar otras formas de fraude, como los ataques con rescate o el robo de desembolsos de gobierno.

Es preciso reconocer que el escenario cambió

Los últimos 18 meses demostraron ser tierra fértil para los cibercriminales, debido al gran salto que realizó el comportamiento de los consumidores hacia el comercio digital y a los grandes desafíos que enfrentan las compañías para satisfacer las nuevas expectativas de estos.

Con ello, aumentaron los casos de fraude cibernético, entre los que se incluyen la filtración de datos, los ataques *ransomware* y las estafas de *phishing*. Si bien no son casos exclusivos de los pagos, muchos tienen una dimensión relacionada con los pagos (bien porque las empresas de pago pueden ser el objetivo de ataques similares, bien porque los cibercriminales pretenden utilizar los sistemas de pago para monetizar sus ganancias).

Mayor cantidad de consumidores y empresas como objetivos

El nuevo comportamiento de los consumidores aceleró los pagos digitales y, solo durante 2020, generó un incremento de US$26,7 billones en los volúmenes de compra en *eCommerce* a nivel global. Al haber mayor cantidad de consumidores que realizan transacciones *online*, son más susceptibles a los ataques de *phishing*.

Ola disruptiva

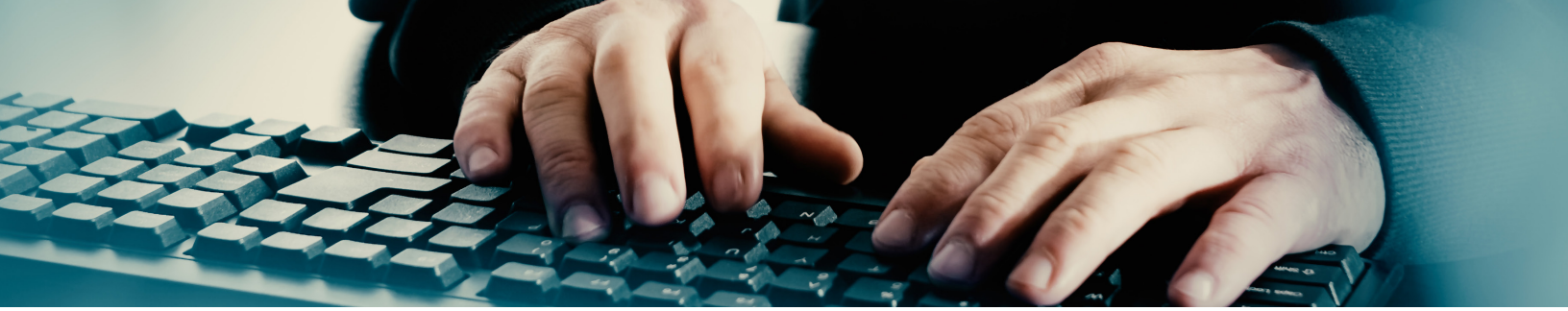
El mundo tuvo que adaptarse rápidamente al teletrabajo y a la implementación de nuevos modelos minoristas, como el de compra *online* y retiro en tienda (BOPIS). Cualquier alteración en la rutina tiende a favorecer a los cibercriminales, porque se pueden camuflar en los cambios de comportamiento, sacar ventaja de las modificaciones que están implementando los bancos y los procesadores, y atacar a comercios y consumidores.

Demora en alinear los sistemas y operaciones heredados

Durante muchos años, el sector de pagos atravesó una ola de fusiones y adquisiciones, que generalmente requiere la adopción de una nueva infraestructura de tecnología, la integración de diferentes operaciones de TI y la alineación de los equipos de gestión de riesgos. Si las organizaciones se demoran en adoptar una estrategia integrada de gestión de tecnología y ciberseguridad, los criminales podrían encontrar nuevas oportunidades que explotar.

Estos riesgos no son solo teorías. Por ejemplo, según el informe sobre delitos en internet del FBI, los reclamos por sospechas de fraude en internet aumentaron un 61% solo en 2020. Estos eventos de fraude, que van desde el robo de datos personales y corporativos hasta el fraude de tarjetas de pago, el *phishing* y el robo de identidad, representaron para las víctimas un costo superior a los US$4200 millones.[2]

1. *UN News, Global e-commerce jumps to $26.7 trillion, fuelled by COVID-19,* https://news.un.org/en/story/2021/05/1091182
2. *US Federal Bureau of Investigation, 2020 Internet Crime Report,* https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf



Cinco tendencias del delito cibernético

Los últimos meses, estas tendencias del fraude cibernético captaron la atención de las empresas de pago:

TENDENCIA #1

Ataques de enumeración (ataques que utilizan el método de prueba y error para robar información de inicio de sesión)

Los estafadores están aprovechando la crisis que sacude al *eCommerce* en todo el mundo para camuflar sus maniobras de prueba de cuenta.

Mediante los ataques de enumeración —que se refieren a la prueba automatizada, escalable y programática de los campos de pago comunes en las transacciones de *eCommerce*—, buscan lograr adivinar el número completo de la cuenta de pago, el código CVV2 o la fecha de vencimiento.

Para camuflar sus actividades, en ocasiones los cibercriminales crearon nombres de comercios relacionados con COVID y atacaron a los comercios vinculados con las donaciones. En otros casos más sofisticados, dirigieron ataques de enumeración automatizados a través de comercios de *eCommerce* de presencia global. Cuando efectivamente lograron obtener los datos de cuenta legítimos, la tendencia más común fue comprar criptomonedas.

Esto es lo mejor que pueden hacer los emisores:

- Sumar actividades de monitoreo de cuenta (que incluyan hacer un seguimiento de la funcionalidad y el comportamiento de API para detectar ataques de bot o *scripting*)
- Estar atentos a cualquier incremento inusual durante la contabilización de transacciones
- Prestar atención a los rechazos por números de cuenta no válidos
- Identificar el aumento repentino de solicitudes de autorización regulares desde la misma fuente (por ej., cada pocos segundos)
- Implementar protecciones de seguridad, como *IP Allowlist,* que indica las direcciones IP que pueden acceder a tu cuenta; reCAPTCHA, que permite que los anfitriones web distingan si el acceso a los sitios web es automatizado o por un humano, o la tecnología de huellas del dispositivo, que posibilita identificar un dispositivo con base en su configuración única

Si se sospecha un ataque, es importante actuar rápidamente e investigar. También es útil identificar las solicitudes de autorización con números de cuenta secuenciales y aplicar protección adicional para las cuentas con números similares, quizás mediante bloqueos específicos dirigidos a nivel de las transacciones.

TENDENCIA #2

Surgimiento repentino de *Click-and-collect* o BOPIS

Entre las tendencias más importantes del año pasado, se encuentra el surgimiento repentino de *Click-and-collect* o BOPIS.

Este nuevo modelo atendió las necesidades de los comercios y de los consumidores por igual, pero, lamentablemente, los cibercriminales no demoraron en hallar las vulnerabilidades de seguridad y cometer fraude en grandes volúmenes.

Por lo general, los cibercriminales utilizan credenciales de cuenta comprometidas para realizar compras *online* fraudulentas o para interceptar los detalles de las compras legítimas. Luego van a la tienda y se hacen pasar por los clientes para recoger los productos.

En esta instancia, la mejor solución es realizar mejoras en el procedimiento de parte del comercio; por ejemplo, se puede incentivar al cliente para que proteja sus cuentas *online* y se pueden aplicar verificaciones adicionales al momento del retiro, como la verificación del número de orden o de identidad.

TENDENCIA #3

Ataques de *ransomware* relacionados con los pagos

Los ataques de *ransomware* fueron noticia durante varios meses. Por lo general, el cibercriminal utiliza *malware* para encriptar datos en la tecnología fundamental del negocio de una compañía y luego solicita un pago de rescate para restituir el servicio.

Si bien los riesgos de *ransomware* alcanzan a todos los tipos de negocio, los cibercriminales direccionan cada vez más sus ataques al ecosistema de pagos y desarrollan sus estrategias en función de ello. Por ejemplo, además de (o en lugar de) inhabilitar los sistemas centrales, el delincuente también intenta robar los datos de las cuentas de pago. A menos que se cumpla con el rescate, los cibercriminales pueden amenazar con publicar estos datos online o venderlos al mejor postor.

Para prevenir estos ataques, las compañías deberían enfocar sus esfuerzos en enseñar y entrenar a sus empleados con las mejores prácticas en seguridad, como el reporte de e-mails o enlaces sospechosos. Por otra parte, las compañías deberían aplicar rigurosas estrategias de ciberseguridad para reducir la superficie de ataque, aplicar protecciones de seguridad de datos sólidas y cumplir con los estándares de la industria.

Además, las compañías deberían implementar una estrategia de defensa en profundidad que incluya controles de detección y prevención para evitar que las amenazas accedan a la red y lancen ataques de *ransomware*. Si los controles preventivos no logran detener que los atacantes encripten los datos, se recomienda que la compañía cuente con buenas capacidades de respaldo y recuperación.

TENDENCIA #4

Ataques a desembolsos de gobierno

A lo largo del año pasado, muchos gobiernos implementaron esquemas de asistencia financiera para sus empleados y para sus ciudadanos, e impulsaron la recuperación mediante pagos de estímulo.

El rápido crecimiento de estos programas representa un riesgo de fraude alto y, por lo general, están involucrados los sistemas de pago digitales. Por ejemplo, en EUA, los cibercriminales utilizaron credenciales de identidad robadas para solicitar seguros de desempleo y luego cargaron los fondos en cuentas de pago prepagas o virtuales. Luego monetizan estos fondos a través de la compra de tarjetas de regalo, criptomonedas o electrónica, o a través de transferencias de fondos entre personas (P2P).

En esta instancia, la mejor defensa es una alianza entre el gobierno, la industria de pagos y los organismos de seguridad. Además, existen verificaciones y controles adicionales que pueden incorporar los emisores para minimizar los riesgos; por ej., una verificación de identidad mejorada en las instancias de apertura y carga de cuenta, o el seguimiento de las técnicas de monetización sospechosas luego del desembolso de fondos.

TENDENCIA #5

Malware en puntos de venta e *e-skimming*

El ecosistema en el que operan los pagos se continúa basando en el uso de detalles de cuenta (el número de cuenta completo, el código CVV2 y la fecha de vencimiento).

Estos datos están bajo el escrutinio constante de los cibercriminales, quienes están al acecho de más formas de obtener detalles nuevos: la nueva tendencia es el aumento del fraude *e-skimming* o *skimming* digital.

En los ataques se inyecta un código malicioso en los sistemas de *eCommerce* del comercio con el fin de recolectar detalles de las tarjetas de pago que se ingresan en las páginas. Si el ataque es exitoso, usualmente los cibercriminales pueden tener acceso constante a los servidores comprometidos y moverse por toda la red del comercio.

Protegerse de estos ataques es, generalmente, responsabilidad de los comercios y sus proveedores, que deben garantizar que se estén implementando los controles cibernéticos más avanzados. Por ejemplo, en una buena gestión, se realizan actualizaciones y parches de software periódicamente, se cuenta con buen *firewall* en funcionamiento, se tiene un control efectivo del acceso a los portales administrativos y se realizan análisis periódicos de los sistemas para detectar vulnerabilidades o *malware*. También es cada vez más habitual que se utilicen técnicas como la tokenización para que los datos de cuenta sean menos sensibles.

Estos cinco tipos de fraude cibernético son una gran preocupación en el entorno actual. Sin embargo, no solo evolucionan los pagos, sino también las técnicas de los cibercriminales, por lo que es probable que surjan nuevos tipos de fraude relacionados con las criptomonedas, la actividad P2P y la cadena de suministro.

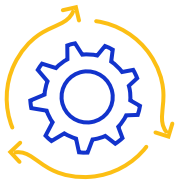
Tres categorías de amenaza

Al evaluar el riesgo de fraude cibernético, puede resultar útil plantearlo desde tres perspectivas distintas, que pueden ayudar a revelar las vulnerabilidades relacionadas y las soluciones más efectivas.

En relación con las personas

Esta es la MÁS importante. Prácticamente todo ataque exitoso se generó porque no se siguieron los protocolos (se hizo clic en el enlace de un e-mail sospechoso, no se respetaron los consejos para la contraseña o, en algunos casos, se trató de una colusión con los cibercriminales, lo que se conoce como amenaza de infiltrado). Esto no se aplica solo a los empleados, sino también a los proveedores y a las terceras partes, ya que suelen tener acceso a los sistemas de la organización.

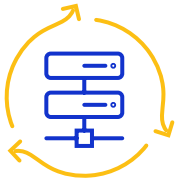
La dimensión humana es considerada como el eslabón más débil y requiere atención constante: seguimiento efectivo de las nuevas contrataciones, capacitación y comunicación para todos los empleados, y enseñanza y comunicación para los clientes. Algunas organizaciones también utilizan ejercicios de "amenaza simulada" para identificar las brechas en capacitación, procedimientos o tecnología que reforzarían las defensas.



En relación con los procedimientos

El aumento del fraude en las compras con retiro sin contacto es una muestra clara de que se necesitan análisis de riesgo y procedimientos sólidos (en este caso, la verificación de identidad mejorada), y pone en evidencia cuáles son las consecuencias si se pasan por alto. No obstante, los procedimientos uniformes e invariables a nivel global también puede ser una vulnerabilidad (con los cibercriminales no solo buscando procedimientos consistentes, sino anomalías consistentes en los procedimientos). Además, a veces las organizaciones tienen procedimientos, pero no cuentan con una política consistente al respecto, como la gestión de parches o cuestiones sobre la seguridad de la red.

La situación amerita establecer diversas protecciones, como el análisis y la validación de código fuente, servicios rigurosos de respuesta a incidentes, el análisis de comportamiento, el análisis de errores en el inicio de sesión, el control de salud de la cuenta del sistema y revisiones y actualizaciones periódicas de todos los procedimientos.



En relación con la tecnología

Siempre existirán riesgos cuando se realicen transferencias con valor monetario y cuando se recolecten, procesen, almacenen y transmitan credenciales de pago. Y ahora que más pagos son digitales, la tecnología está bajo escrutinio constante... esta es la realidad de operar en el sector de pagos.

En los días que corren, toda empresa de pagos debe ser una empresa de tecnología y todo equipo de gestión de riesgos debe tener amplios conocimientos tecnológicos. Las organizaciones deberían priorizar sus mecanismos de defensa, que incluyan información actualizada de amenazas, segmentación y análisis de redes, seguimiento de cerca y protección de *endpoints*, tokenización y autenticación biométrica.

Dos medidas para las organizaciones

1

Colaboración entre las áreas de seguridad cibernética y de fraude de pagos

Visa observó que todos los equipos de riesgo de alto rendimiento comparten una misma característica: emplean una visión integral del delito cibernético, el fraude financiero y el riesgo de pagos.

Reconocen que sus adversarios cuentan con conocimientos sofisticados sobre el ecosistema de pagos y sobre el rol del banco dentro de este. Su perspectiva es que los cibercriminales comprenden el tipo de procedimientos, controles y vulnerabilidades de la banca, que surgen de organizaciones y gestiones aisladas. Comprenden, además, que las amenazas más grandes suelen estar en los puntos en común, al igual que las soluciones efectivas.

Construyeron sus equipos y procedimientos de manera adecuada. Combinan experiencia en gestión de riesgos (tradicionalmente asociada con los equipos de prevención de fraudes) con experiencia en tecnología (tradicionalmente asociada con los equipos de ciberseguridad). Obtienen más que colaboración; obtienen colaboración activa y conjunta.

2

Crear un marco de estrategia de seguridad (diseño, definición, diagnóstico y defensa) para proteger la organización por medio de principios clave de seguridad

Los equipos de riesgo líderes establecieron principios de seguridad global en torno a la gestión de identidad y acceso, la criptografía y la seguridad en infraestructura y aplicativos, entre otras. También desarrollaron una estrategia de seguridad cibernética completa a partir de estos principios.

Este marco es una estrategia imprescindible. Por ello, colaboran con otras áreas de negocio, por ej., con equipos de tecnología y de datos. También incorporan una buena cuota de liderazgo ejecutivo desde el principio para obtener patrocinio y financiación.

Cómo Visa puede ayudarte

Visa cuenta con la experiencia en ciberseguridad que necesitas para que, con la ayuda de datos analíticos y capacidades de inteligencia artificial, puedas adaptarte al cambiante escenario comercial y protegerte de las crecientes amenazas a la ciberseguridad.

Mientras, VCA se encuentra en la posición ideal para trabajar con los clientes y formular una estrategia de ciberseguridad, gestión de riesgos y evaluación de cumplimiento normativo, además de entrenar, concientizar y educar en cuestiones de cibernética. De modo similar, los expertos en el tema pueden asesorar en áreas de resiliencia operativa, que incluye parches y gestión de vulnerabilidades, gestión de identidad y acceso, seguridad de las solicitudes y ataques de *hacking* ético, protección de datos y evaluación de la capacidad de respuesta a incidentes.

Servicios de asesoramiento en ciberseguridad de VCA

Módulos de asesoramiento en ciberseguridad (creado con los EXPERTOS de Visa en conjunto con terceros)			**Descripción**
Gestión de riesgos (estrategia y gestión)	**1**	**Estrategia cibernética, arquitectura y controles**	Define las estrategias cibernéticas y los mapas de acción, los controles de seguridad y la arquitectura de referencia en sintonía con los hallazgos obtenidos de la evaluación de madurez
	2	**Gestión de riesgos y cumplimiento normativo**	Permite que la organización identifique y comprenda los riesgos comerciales clave y los niveles de exposición a las ciberamenazas, para implementar las mejoras necesarias
	3	**Entrenamiento, concientización y educación cibernética**	Desarrolla una cultura madura respecto de los riesgos cibernéticos, mediante la definición y la oferta de programas que mejoren las habilidades técnicas y promuevan la educación en seguridad
Resiliencia operativa (preparación operativa y defensiva)	**4**	**Parches y gestión de vulnerabilidades**	Ayuda al diseño y a la gestión de programas para identificar, priorizar y remediar las vulnerabilidades en seguridad y las debilidades en infraestructura
	5	**Gestión de identidad y acceso (IAM)**	Ayuda con herramientas, procesos y métodos IAM para mejorar la seguridad y minimizar la fricción en la experiencia del usuario
	6	**Prueba dinámica de seguridad de aplicaciones (DAST)**	Evalúa las aplicaciones y los controles de seguridad de la organización en diversos niveles de los sistemas de las grandes empresas mediante el uso de métodos DAST
	7	**Protección de datos**	Contribuye con la protección de información confidencial o privada y de activos críticos, más allá de los límites de la organización
	8	**Evaluación de la capacidad de respuesta a incidentes**	Revisa la capacidad y el alcance actuales de la detección de eventos de seguridad; analiza los mecanismos de respuesta para resolver incidentes relacionados con los pagos y las transacciones

Sobre *Visa Consulting & Analytics*

- Nuestros consultores cuentan con décadas de experiencia en la industria de pagos y son expertos en estrategia, producto, gestión de portafolio, riesgos y ciberseguridad, recursos digitales y más.
- Nuestros científicos de datos son expertos en estadísticas, analítica avanzada y *machine learning* con acceso exclusivo a datos obtenidos a través de VisaNet, una de las redes de pago más grandes del mundo.
- Entender las condiciones económicas que afectan al consumo permite a nuestros economistas brindar información única y oportuna sobre las tendencias de consumo global.

Somos un equipo global de cientos de consultores de pago, científicos de datos y economistas en los seis continentes.

La combinación de nuestra amplia experiencia en consultoría de pagos, nuestra inteligencia en estrategias económicas y la amplia variedad de datos con la que contamos, nos permite identificar conocimientos prácticos y recomendaciones que ayudan a tomar mejores decisiones comerciales.

Para más información, contacta a tu ejecutivo de cuenta Visa, envía un correo electrónico a **Visa Consulting & Analytics** a **VCA@Visa.com** o visita **Visa.com/VCA**

Sobre *Visa Risk*

Asegurar el ecosistema de pagos requiere inversión e innovación constantes en materia de nueva tecnología y colaboración con nuestros socios comerciales. Nuestro trabajo es proteger a Visa y a los socios en su ecosistema, y permitirles que sean el motor para el comercio más seguro, más resiliente y más confiado para todas las personas y en todos los lugares.

Proponemos iniciativas en seguridad para el mercado local y global, compartimos información y mejores prácticas, analizamos las tendencias de seguridad en desarrollo y promovemos la colaboración en materia de riesgo entre las regiones y a nivel global.

Visa Risk utiliza un conjunto de capacidades, analítica y experiencia a nivel de la red para proteger la seguridad y la estabilidad del ecosistema de pagos y minimizar las pérdidas por fraude de los clientes.

Visa Consulting & Analytics es un equipo global de especialistas en estrategia, marketing, operaciones, riesgo y consultoría en economía, con décadas de experiencia en la industria de pagos. Nuestro equipo de expertos en la materia utiliza análisis de la red de pagos con mayor cantidad de transacciones de compra del mundo, por lo que podemos brindarte estrategias probadas e información corroborada que contribuirán con tus objetivos comerciales.

