STATISTICAS DEL 2022

10.3 Mil Millones
Pérdidas de victimas en el 2022

2,175+
Promedio de quejas recibidas a diario

651,800+
Promedio de quejas recibidas por año

Mas de 70. Millones
Quejas reportadas desde el principio del programa

Quejas de IC3 Agrupadas Por Edad

De 20 para abajo — Quejas: 15,782 — Pérdidas: $210.5 Millones

De 20 a 29 — 7,978 — $383 Millones

De 30 a 39 — 94,506 — $1.3 Mil Millones

De 40 a 49 — 87,526 — $1.5 Mil Millones

De 50 a 59 — 64,551 — $1.8 Mill Millones

De 60 para arriba — 88,262 — $3.1 Mill Millones

REPÓRTELO!

Si usted, o alguien que usted conoce, es una possible víctima del fraude por internet someta una queja al Centro de Quejas Contra Crimenes por Internet [IC3, por sus siglas en Inglés.]

www.ic3.gov

Consejos para someter las quejas:

- Mantenga todos los archivos originales: emails, cartas, cheques, recibos, documentos de envoi, etc.
- Documente la informacion que utilizó el estafador: números de cuenta, direcciones físicas y electronicas, paginas web, etc.
- Información de Transaccioes Financieras.
- Información utilizada por los criminales, como cuentas de banco, direcciones físicas y electronicas, páginas web y números telefónicos.

Póngase en contacto con sus instituciones financieras para resguardar sus cuentas, y con las compañias del credito para monitorear la seguridad de su identidad contra la actividad sospechosa.

Anuncios de Servicios Públicos

IC3 revisa y analiza la información sometida a travez de su página web, la cual genera productos de inteligencia resaltatando las amenazas emergentes y otras publicaciones que recalcan las estafas especificas y son publicadas en la página web de IC3.

www.ic3.gov

Departamento de Justicia de EE.UU.
Buro de Investigaciones Federales
División Cibernética

CENTRO DE QUEJAS CONTRA LOS CRIMINES POR INTERNET

www.ic3.gov

MIRANDO DENTRO DEL IC3

La Misión del IC3

La misión del Centro de Quejas Contra los Crímenes de Internet (IC3) es el proveer al público un medio seguro y conveniente para reportar información al Buró de Investigaciones Federales de toda actividad sospechosa relacionada con los crímenes facilitados por el internet. También el desarrollar alianzas efectivas con socios en la misma industria. La información es procesada y utilizada con propósitos de investigación e inteligencia para los agentes del orden público y para el conocimiento del público.

Las Quejas del IC3

Las quejas sometidas al IC3 cubren muchas clases de crímenes por internet, los cuales incluyen el robo de derechos de propiedad intelectual, la intrusión informática, el espionaje económico, la extorsión vía internet y el lavado internacional de dinero. También incluyen numerosos esquemas de fraude como robo de identidad, phishing, spam, reprocesamiento, fraude de subasta, fraude de pago, productos falsificados, estafas románticas y falta de entrega de los productos comprados, todos estos se informan al IC3.

Fraude Contra Ancianos

La Ley de enjuiciamiento y prevención contra el abuso de ancianos entró en efecto en octubre del 2017 para prevenir el abuso y la explotación de los ancianos y mejorar la reacción del sistema de justicia para las víctimas en casos de abuso y explotación de ancianos. Como respuesta a la creciente prevalencia del fraude contra los ancianos, el Departamento de Justicia (DOJ, por sus siglas en inglés) y el FBI se asociaron para crear la Iniciativa de Justicia para los Ancianos. El fraude contra anciano es definido como un esquema de fraude financiero que se dirige o afecta desproporcionadamente a personas mayores de 60 años.

El IC3 es la oficina del FBI responsable de recibir quejas de fraude contra ancianos. En el 2022, más de 82,000 víctimas mayores de 60 años reportaron al IC3 pérdidas de casi $3,1 mil millones. Esto representa un aumento del 84 por ciento cuando se compara con las pérdidas del 2021. Debido a que no es obligatorio reportar la edad, estas estadísticas sólo reflejan las quejas donde la víctima proporcionó su edad voluntariamente como “más de 60 años”.

Internet Crime and the IC3

A medida que la tecnología evoluciona, también lo hacen los muchos métodos utilizados para explotar la tecnología con fines delictivos. Casi todos los delitos que alguna vez se cometieron en persona, por correo o por teléfono se pueden cometer a través de Internet. El elemento criminal está potenciado por el anonimato percibido de Internet y la facilidad de acceso a las víctimas potenciales. Los delincuentes utilizan la ingeniería social para aprovecharse de la simpatía, generosidad o vulnerabilidad de sus víctimas. El IC3 fue diseñado para ayudar a abordar todos los tipos de delitos en Internet a través de su sistema de denuncias.

TRENDS

Compromiso de Correo Electrónico Empresarial

En 2022, el IC3 recibió 21,832 quejas de Business Email Compromise (BEC) con pérdidas ajustadas de casi $ 2.7 mil millones. BEC se dirige tanto a empresas como a individuos que realizan transferencias de fondos, y se lleva a cabo con mayor frecuencia cuando un sujeto compromete cuentas de correo electrónico comerciales legítimas a través de ingeniería social o técnicas de intrusión informática para realizar transferencias no autorizadas.

Fraude de confianza / Estafas románticas

Las estafas de fraude de confianza / romance abarcan aquellas diseñadas para tirar de las "fibras del corazón" de una víctima. En 2022, el IC3 recibió informes de 19,021 víctimas que experimentaron más de $ 735 millones en pérdidas por fraude de confianza / estafas románticas. Las estafas de abuelos entran en esta categoría. En 2022, casi 400 víctimas de más de 60 víctimas reportaron estafas de abuelos, con pérdidas aproximadas de $ 3.8 millones.

Inversión El fraude de inversión implica la venta ilegal o la supuesta venta de instrumentos financieros. Los ejemplos de fraude de inversión incluyen fraude de tarifas anticipadas, esquemas Ponzi y piramidales, estafas criptográficas fraudulentas y fraude de manipulación del mercado. Más de 30,000 víctimas reportaron estafas de inversión en 2022, con pérdidas de más de $ 3.3 mil millones. De esa pérdida, más de $ 2.57 mil millones involucraron inversiones en criptomonedas. Las estafas de criptoinversión vieron aumentos sin precedentes en el número de víctimas y las pérdidas en dólares para estos inversores. Muchas víctimas han asumido deudas masivas para cubrir las pérdidas de estas inversiones fraudulentas y el grupo de edad más específico que informa este tipo de estafa son las víctimas de 30 a 49 años.

Ransomware

El ransomware es un tipo de software malicioso, o malware, que cifra los datos en una computadora, haciéndola inutilizable. Un ciberdelincuente mantiene los datos como rehenes, o amenaza con destruir los datos o divulgarlos al público, hasta que se pague el rescate. Si no se paga el rescate, los datos de la víctima permanecen encriptados. En 2022, el IC3 recibió 2.385 quejas identificadas como ransomware con pérdidas ajustadas de casi 34,4 millones de dólares.

Fraude de soporte técnico

El fraude de soporte técnico implica un reclamo criminal para proporcionar al cliente, seguridad o soporte técnico o servicio para defraudar a personas involuntarias. En 2022, el IC3 recibió 32,538 quejas relacionadas con el fraude de soporte técnico de víctimas en 80 países. Las pérdidas ascendieron a más de $ 806 millones, lo que representa un aumento del 132 por ciento en las pérdidas desde 2021.

Criptomoneda

Una vez limitada a hackers, grupos de ransomware y otros habitantes de la "web oscura", la criptomoneda se está convirtiendo en el método de pago preferido para todo tipo de estafas: intercambios de SIM, fraude de soporte técnico, esquemas de empleo, estafas románticas, incluso algunos fraudes de subastas. El uso de criptomonedas es extremadamente generalizado en las estafas de inversión, donde las pérdidas pueden alcanzar los cientos de miles de dólares por víctima. El IC3 recibió más de 52,000 quejas en 2022 que informaban algún tipo de uso de criptografía. Las pérdidas de estas quejas superaron los $ 3.8 mil millones.