# Denúncias apresentadas ao IC3 em 2025

## Destaques

**1.008.597 Denúncias**
**Perdas totais de 20,877 mil milhões de dólares**
**Aumento de 26% nas perdas a partir de 2024**
**Perda média de 20.699 dólares**

### Por faixa etária


### Top 10 tipos de crimes por valor de perdas em 2025

| Tipo de crime | Perdas em dólares |
|---|---|
| Investimento | 8,6 mil milhões |
| E-mail comercial comprometido | 3 mil milhões |
| Suporte técnico/assistência ao cliente | 2,1 mil milhões |
| Violação de dados pessoais | 1,3 mil milhões |
| Confiança/Romance | 929 milhões |
| Personificação do governo | 797,9 milhões |
| Não-pagamento/Não-entrega | 503 milhões |
| Violação de dados | 435 milhões |
| Emprego | 362,9 milhões |
| Fraude com cartão de crédito/cheque | 282 milhões |

**Leia mais no Relatório Anual do IC3 de 2025**
https://www.ic3.gov/AnnualReport/Reports

# DENUNCIE!

Se você, ou alguém que conhece, for uma potencial vítima de fraude cibernética, apresente uma denúncia ao IC3.

**www.ic3.gov**

Sugestões para apresentar a denúncia:

- Guarde os registos originais: e-mails, cartas, cheques, recibos, documentos de envio, etc.
- Informações sobre transações financeiras.
- Informações utilizadas pelos criminosos como contas bancárias, endereços, e-mails, sites e números de telefone.

Contacte as instituições financeiras para proteger as suas contas e agências de crédito para monitorizar a sua identidade quanto a atividade suspeita.

## Comunicados de utilidade pública e alertas do setor

O IC3 examina e analisa dados apresentados por meio de seu site e produz relatórios para identificar ameaças emergentes e novas tendências. Os comunicados de utilidade pública, alertas do setor e outras publicações que descrevem fraudes específicas estão disponíveis no site do IC3.

**www.ic3.gov**

CENTRO DE DENÚNCIAS DE CRIMES NA INTERNET

DENUNCIAR - ANALISAR - APRIMORAR - ENCAMINHAR - COLABORAR - PARTILHAR

**Departamento de Justiça dos EUA**
Agência Federal de Investigações
*Divisão Cibernética*


# CENTRO DE DENÚNCIAS DE CRIMES NA INTERNET

**www.ic3.gov**

# Nosso papel no combate ao crime cibernético

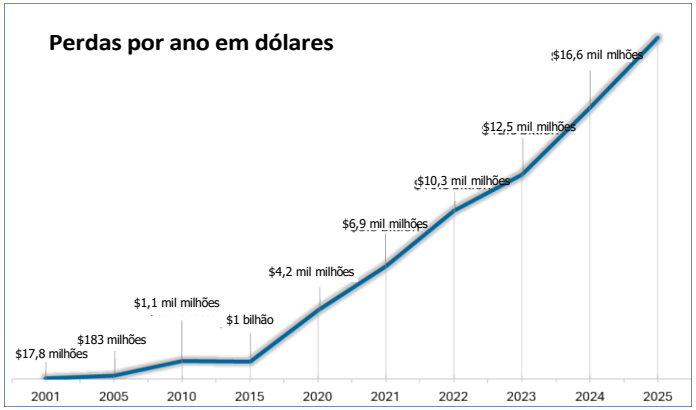
**Coleta:** O IC3 é o principal ponto de ligação entre o FBI e o público para a receção e coordenação de informações sobre crimes facilitados por meios digitais, incluindo intrusões, fraudes e golpes. As vítimas são incentivadas, e muitas vezes orientadas pelas autoridades, a apresentar uma denúncia no site www.ic3.gov. Os reclamantes devem documentar informações precisas e completas relacionadas à suspeita de crime cibernético, bem como quaisquer outras informações relevantes.

**Análise:** O IC3 examina e analisa os dados submetidos através do www.ic3.gov para identificar ameaças emergentes e novas tendências. O IC3 pode alertar rapidamente as instituições financeiras sobre transações fraudulentas, permitindo o congelamento dos fundos das vítimas se determinados critérios de denúncia forem atendidos.

**Encaminhamento e aprimoramento:** O IC3 agrupa denúncias relacionadas para efeitos de encaminhamento, que são fornecidos às autoridades locais, estaduais, federais e internacionais para eventual investigação. A agregação e o aprimoramento aumentam o apoio e os níveis de atuação da acusação em investigações, novas e em curso, e ajudam na detecção de métodos emergentes, tendências e identificadores de indivíduos.

**Coordenação:** O IC3 facilita a coordenação 24 horas por dia/7 dias por semana/365 dias por ano, dos esforços de resposta a ameaças, com parceiros internos e externos, em apoio a uma abordagem governamental integrada de gestão de incidentes cibernéticos. O IC3 desempenha um papel fundamental na cooperação do FBI com parceiros internacionais no combate ao crime cibernético, trabalhando com a sede do FBI, os escritórios locais e os adidos policiais para apoiar investigações em todo o mundo.

**Sensibilização pública:** Comunicados de utilidade pública, alertas do setor e outras publicações sobre fraudes específicas são disponibilizados no site www.ic3.gov. À medida que mais pessoas tomam conhecimento dos crimes cibernéticos e dos métodos utilizados para a sua prática, todos ficamos mais bem preparados para reconhecer os perigos associados à atividade cibernética e em melhor posição para evitar cair em esquemas fraudulentos na internet.





## Um quarto de século de denúncia de crimes cibernéticos

Nos últimos 25 anos, o IC3 tem sido o principal ponto de ligação entre o FBI e o público no que respeita a informações relacionadas a atividades criminosas viabilizadas pela Internet. Desde a nossa criação, houve um aumento notável no número de denúncias ao IC3. Onde no início recebíamos alguns milhares de denúncias por mês, o IC3 passou a receber, em média, milhares de denúncias por dia. Com base nas informações que recebemos, o IC3 elabora relatórios anuais, desenvolve campanhas de sensibilização pública e emite alertas setoriais dirigidos ao setor privado. O IC3 mantém-se como um recurso essencial para os nossos colegas das forças de segurança no combate ao crime cibernético.

### Denúncias ao IC3

As denúncias apresentadas ao IC3 abrangem uma variedade de crimes na Internet, incluindo roubo de direitos de propriedade intelectual, invasão de computadores, espionagem económica, extorsão online e branqueamento de capitais a nível internacional. Inúmeros esquemas fraudulentos, como o roubo de identidade, phishing, spam, reenvio, fraude de leilão, fraude de pagamento, contrafação de bens, burlas românticas e não entrega de mercadorias são comunicados ao IC3.

### Ameaças cibernéticas

Redes comprometidas, roubos de criptomoedas e espionagem corporativa são alguns exemplos do aumento vertiginoso das ameaças cibernéticas. A cada ano, os nossos adversários tornam-se mais sofisticados e cada vez mais implacáveis - atacando redes elétricas, interrompendo o funcionamento de hospitais e alimentando tensões geopolíticas. Actores cibernéticos patrocinados pelo Estado utilizam todos os elementos do seu poder nacional para atacar os EUA e suas infraestruturas críticas. Criminosos cibernéticos qualificados exploram vulnerabilidades, novas e já existentes, para roubar o nosso dinheiro e reter os nossos dados para obter resgate. O combate a estas ameaças constitui a missão principal do programa de segurança cibernética do FBI. O IC3 coordena e partilha informações com todos os escritórios de campo do FBI e com os nossos parceiros de inteligência com vista ao combate às ameaças cibernéticas.

### Fraude envolvendo idosos

A cada ano, milhões de idosos americanos são vítimas de algum tipo de fraude financeira ou esquema de confiança, incluindo burlas românticas, esquemas de lotaria, fraudes de suporte técnico e golpes de sorteio - entre outros. Denunciar fraudes contra idosos ao IC3 ajuda o FBI a identificar e agir contra golpistas que se aproveitam dos nossos entes queridos mais velhos.