2022 STATISTICS

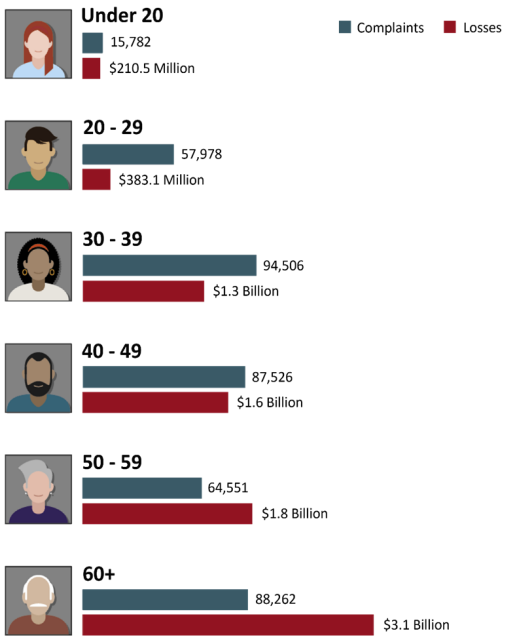
$10.3 Billion
Victim losses in 2022

2,175+
Average complaints received daily

651,800+
Average complaints received per year (last 5 years)

Over 7.3 Million
Complaints reported since inception

IC3 Complaints By Age Groups



REPORT IT!

If you, or someone you know, is a potential victim of internet fraud, file a complaint with the IC3.

www.ic3.gov

Filing tips:

- Retain original records: emails, letters, checks, receipts, shipping documents, etc.
- Document the information used by the scammer: account numbers, addresses, emails, websites, etc.
- Financial transaction information.
- Information used by the criminals such as bank accounts, addresses, e-mails, websites, and phone numbers.

Contact financial institutions to safeguard accounts, and credit bureaus to monitor your identity for suspicious activity.

Public Service Announcements And Industry Alerts

The IC3 reviews and analyzes data submitted through its website, and produces intelligence products to highlight emerging threats and new trends. PSAs, Industry Alerts, and other publications outlining specific scams are posted to the IC3 website.

www.ic3.gov

U.S. Department of Justice
Federal Bureau of Investigation
Cyber Division

INTERNET CRIME COMPLAINT CENTER

www.ic3.gov

A LOOK INTO THE IC3

Mission of the IC3

The mission of the Internet Crime Complaint Center (IC3) is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet facilitated criminal activity and to develop effective alliances with industry partners. Information is processed for investigative and intelligence purposes for law enforcement and public awareness.

IC3 Complaints

The complaints submitted to the IC3 cover an array of Internet crime including theft of intellectual property rights, computer intrusion, economic espionage, online extortion, and international money laundering. Numerous fraud schemes such as identity theft, phishing, spam, reshipping, auction fraud, payment fraud, counterfeit goods, romance scams, and non-delivery of goods are reported to the IC3.

Elder Fraud

The Elder Abuse Prevention and Prosecution Act was signed into law in October 2017 to prevent elder abuse and exploitation and improve the justice system's response to victims in elder abuse and exploitation cases. As a response to the increasing prevalence of fraud against the elderly, the Department of Justice (DOJ) and the FBI partnered to create the Elder Justice Initiative. Elder Fraud is defined as a financial fraud scheme which targets or disproportionately affects people over the age of 60.

The IC3 is the FBI office responsible for receiving Elder Fraud complaints. In 2022, over 82,000 victims over the age of 60 reported losses of almost $3.1 billion to the IC3. This represents a 84 percent increase in losses over losses reported in 2021. Because age is not a required reporting field, these statistics only reflect complaints in which the victim voluntarily provided their age range as "Over 60".

Internet Crime and the IC3

As technology evolves, so do the many methods used to exploit technology for criminal purposes. Nearly all crime that once was committed in person, by mail, or over the telephone can be committed over the Internet. The criminal element is empowered by the perceived anonymity of the Internet and the ease of access to potential victims. Criminals use social engineering to prey on their victims' sympathy, generosity, or vulnerability. The IC3 was designed to help address all types of Internet crime through its complaint system.

TRENDS

Business Email Compromise

In 2022, the IC3 received 21,832 Business Email Compromise (BEC) complaints with adjusted losses at nearly $2.7 billion. BEC targets both businesses and individuals performing transfers of funds, and is most frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers.

Confidence Fraud / Romance Scams

Confidence Fraud/Romance scams encompass those designed to pull on a victim's "heartstrings." In 2022, the IC3 received reports from 19,021 victims who experienced more than $735 million in losses to Confidence Fraud/Romance scams. Grandparent scams fall under this category. In 2022, almost 400 victims over 60 victims reported Grandparent scams, with approximate losses of $3.8 million.

Investment

Investment fraud involves the illegal sale or purported sale of financial instruments. Examples of investment fraud include advance fee fraud, Ponzi and pyramid schemes, fraudulent crypto scams, and market manipulation fraud. More than 30,000 victims reported Investment scams in 2022, with losses over $3.3 billion. Of that loss, over $2.57 billion involved cryptocurrency investments. Crypto-investment scams saw unprecedented increases in the number of victims and the dollar losses to these investors. Many victims have assumed massive debt to cover losses from these fraudulent investments and the most targeted age group reporting this type of scam

Ransomware

Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. A cyber criminal holds the data hostage, or threatens to destroy the data or release it to the public, until the ransom is paid. If the ransom is not paid, the victim's data remains encrypted. In 2022, the IC3 received 2,385 complaints identified as ransomware with adjusted losses of almost $34.4 million.

Tech Support Fraud

Tech Support Fraud involves a criminal claiming to provide customer, security, or technical support or service to defraud unwitting individuals. In 2022, the IC3 received 32,538 complaints related to Tech Support Fraud from victims in 80 countries. The losses amounted to more than $806 million, which represents a 132 percent increase in losses from 2021.

Cryptocurrency

Once limited to hackers, ransomware groups, and other denizens of the "dark web," cryptocurrency is becoming the preferred payment method for all types of scams – SIM swaps, tech support fraud, employment schemes, romance scams, even some auction fraud.

The use of cryptocurrency is extremely pervasive in investment scams, where losses can reach into the hundreds of thousands of dollars per victim. The IC3 received over 52,000 complaints in 2022 reporting some type of crypto use. Losses from these complaints exceeded $3.8 billion.