2021 STATISTICS

$6.9 Billion
Victim losses in 2021

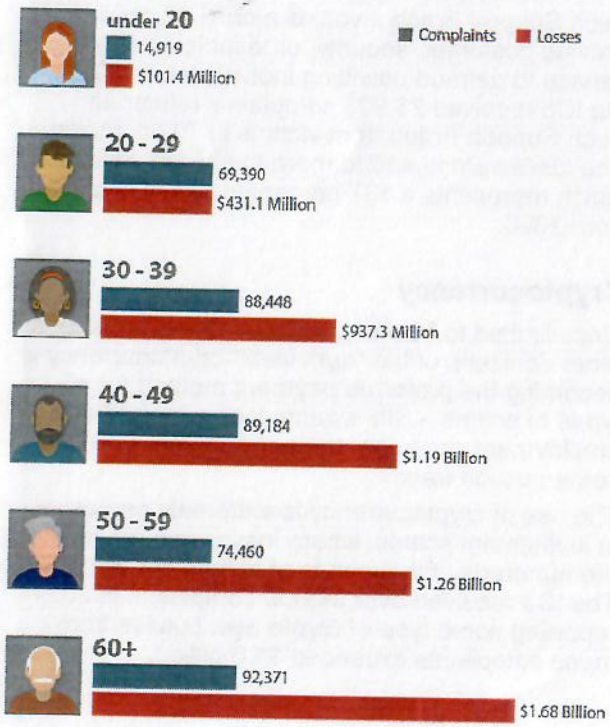
2,300+
Average complaints received daily

2021
2019
2018
2017
2016

552,000+
Average complaints received per year (last 5 years)

Over 6.5 Million
Complaints reported since inception

2021 Victims by Age Group



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.
- Print or save a copy of the complaint for your records.

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.

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. The IC3 refers actionable complaints as deemed appropriate to law enforcement and regulatory agencies for possible investigation. The IC3 will not contact you regarding your complaint.

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. In 2021, over 92,000 victims over the age of 60 reported losses of $1.7 billion to the IC3. This represents a 74 percent increase in losses over losses reported in 2020 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 2021, the IC3 received 19,954 Business Email Compromise (BEC) complaints with adjusted losses at nearly $2.4 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 2021, the IC3 received reports from 24,299 victims who experienced more than $956 million in losses to Confidence Fraud/Romance scams. Grandparent scams fall under this category. In 2021, over 450 Over 60 victims reported Grandparent scams, with approximate losses of $6.5 million.

Investment

Investment fraud involves the illegal sale or purported sale of financial instruments. Examples of investment fraud include advance fee fraud, Ponzi schemes, pyramid schemes, fraudulent crypto scams, and market manipulation fraud. More than 20,000 victims reported Investment scams in 2021, with losses over $1.5 billion.

Increasingly, victims of Romance scams report being pressured into crypto investments. In 2021, the IC3 received more than 4,325 complaints, with losses over $429 million, from this scam. Termed "pig butchering", the scam is so named because victims' investment accounts are fattened up before draining, much a like a pig before slaughter.

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 2021, the IC3 received 3,729 complaints identified as ransomware with adjusted losses of more than $49.2 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 2021, the IC3 received 23,903 complaints related to Tech Support Fraud from victims in 70 countries. The losses amounted to more than $347 million, which represents a 137 percent increase in losses from 2020.

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 34,000 complaints in 2021 reporting some type of crypto use. Losses from these complaints exceeded $1.6 billion.

personal information, like your Social Security, bank account, or credit card numbers.

If you get an email or text message from a company you do business with and you think it's real, it's still best not to click on any links. Instead, contact them using a website you know is trustworthy. Or look up their phone number. Don't call a number they gave you or the number from your caller ID.

Resist the pressure to act immediately.

Legitimate businesses will give you time to make a decision. Anyone who pressures you to pay or give them your personal information is a scammer.

Know how scammers tell you to pay.

Never pay someone who insists you pay with a gift card or by using a money transfer service. And never deposit a check and send money back to someone.

Stop and talk to someone you trust.

Before you do anything else, tell someone — a friend, a family member, a neighbor — what happened. Talking about it could help you realize it's a scam.

Report Scams to the FTC

If you were scammed or think you saw a scam, report it to the Federal Trade Commission.

ReportFraud.ftc.gov

FEDERAL TRADE COMMISSION

September 2020

How to Avoid a Scam

Four Signs That It's a Scam

1 Scammers PRETEND to be from an organization you know.

Scammers often pretend to be contacting you on behalf of the government. They might use a real name, like the Social Security Administration, the IRS, or Medicare, or make up a name that sounds official. Some pretend to be from a business you know, like a utility company, a tech company, or even a charity asking for donations.

They use technology to change the phone number that appears on your caller ID. So the name and number you see might not be real.

2 Scammers say there's a PROBLEM or a PRIZE.

They might say you're in trouble with the government. Or you owe money. Or someone in your family had an emergency. Or that there's a virus on your computer.

Some scammers say there's a problem with one of your accounts and that you need to verify some information.

Others will lie and say you won money in a lottery or sweepstakes but have to pay a fee to get it.

3 Scammers PRESSURE you to act immediately.

Scammers want you to act before you have time to think. If you're on the phone, they might tell you not to hang up so you can't check out their story.

They might threaten to arrest you, sue you, take away your driver's or business license, or deport you. They might say your computer is about to be corrupted.

4 Scammers tell you to PAY in a specific way.

They often insist that you pay by sending money through a money transfer company or by putting money on a gift card and then giving them the number on the back. Some will send you a check (that will later turn out to be fake), tell you to deposit it, and then send them money.

What You Can Do to Avoid a Scam

- **Block unwanted calls and text messages.**

  Take steps to block unwanted calls and to filter unwanted text messages.

- **Don't give your personal or financial information in response to a request that you didn't expect.**

  Legitimate organizations won't call, email, or text to ask for your

Buying a gift card to pay someone?

STOP

It's a scam!

Gift cards are for gifts, not for payments.

ftc.gov/giftcards

government imposter **IRS**
PRIZES online shopping
arrest business imposter
ransom **imposter** scam
tech support deportation
family/friend imposter **IRS**
romance scams **PRIZES**
SWEEPSTAKES **lotteries**

Avoiding Identity Theft

Identity theft can make it hard for you to get credit, a job, a place to live, or utilities. But you can reduce your risk of being hurt by identity theft.

How can I protect my identity?

Protect your personal information. That helps you protect your identity. Here are some things you can do:

- At home
  - keep your financial records, Social Security and Medicare cards in a safe place
  - shred papers that have your personal or medical information
  - take mail out of your mailbox as soon as you can
- As you do business
  - only give your Social Security number if you must. Ask if you can use another kind of identification
  - do not give your personal information to someone who calls you or emails you
- On the computer
  - use passwords that are not easy to guess. Use numbers and symbols when you can
  - do not respond to emails or other messages that ask for personal information
  - do not put personal information on a computer in a public place, like the library

How will I know if someone steals my identity?

Read your bills and account statements. Watch for:

- things you did not buy
- withdrawals you did not make
- a change of your address that you did not expect
- bills that stop coming

Avoiding Identity Theft

Look at medical statements. You might see charges you do not recognize. That might mean someone stole your identity.

Get your credit report. You get one free credit report every year from each credit reporting company. To order:

- Call Annual Credit Report at 1-877-322-8228.
- Answer questions from a recorded system. You have to give your address, Social Security number, and birth date.
- Choose to only show the last four numbers of your Social Security number. It is safer than showing the full number on your report.
- Choose which credit reporting company you want a report from. (You get one report free from each company every year.)

The company mails your report to you. It should arrive two to three weeks after you call.

Read your credit report carefully. Look for mistakes or accounts you do not recognize. This could mean someone stole your identity.

Money Wiring Scams

Wiring money is like sending cash. Do not wire money to people you do not know.

How do I spot a money wiring scam?

Most money wiring scams look like this:

- someone you do not know asks you to wire money

A scammer might use different ways to convince you to wire money. The scammer might say:

- you won a prize, or inherited money, but you have to pay fees first
- you won the lottery, but you have to pay some taxes first
- a friend or family member is in trouble and needs you to send money to help
- you need to pay for something you just bought online before they send it
- you got a check for too much money and need to send back the extra

These are all tricks. When you hear stories like these, you have spotted a money wiring scam.

How do I avoid a money wiring scam?

Scammers are good at being friendly. They also are good at fooling people. Here is how you can stop a scammer:

- Never wire money to someone you do not know.
- Never wire money because someone contacted you:
  - even if you feel like you know the person
  - even if the person says he is your friend or related to you

Money Wiring Scams

What if I already wired money to someone?

If you sent money to someone who contacted you, report it to the Federal Trade Commission (FTC).

- Call the FTC at 1-877-382-4357
- Go online: ReportFraud.ftc.gov

The FTC uses complaints to build cases against scammers. Any information you can give helps investigators.

have you HEARD about...

Grandkid Scams

Here's how they work:

You get a call: "Grandma, I need money for bail." Or money for a medical bill. Or some other kind of trouble. The caller says it's urgent — and tells you to keep it a secret.

But is the caller who you think it is? Scammers are good at pretending to be someone they're not. They can be convincing: sometimes using information from social networking sites, or hacking into your loved one's email account, to make it seem more real. And they'll pressure you to send money before you have time to think.

Here's what you can do:

1. **Stop. Check it out.** Look up your grandkid's phone number yourself, or call another family member.
2. **Pass this information on to a friend.** You may not have gotten one of these calls, but chances are you know someone who will get one — if they haven't already.

Your online
SWEETHEART
asks for money.

No
matter the
reason...

Stop.

Don't send money to an online love interest.

You won't get your money back.