THE U.S. DEPARTMENT OF THE TREASURY

Office of Cybersecurity and Critical Infrastructure Protection

Staying Cyber-Safe This Holiday Season

The holidays are a time for family and friends to gather and celebrate. It is also a time when fraudsters and scammers are at their busiest. Cybercriminals exploit holiday-related stress and distractions, making consumers more vulnerable to shopping, charity, and gift card scams. Understanding the common ways cybercriminals target consumers will help ensure a safe and secure holiday season for all.

In 2025, the FBI's Internet Crime Complaint Center (IC3) received over 1 million complaints totaling $20.877 billion in losses, increasing 26% from 2024. Cyber-enabled fraud comprised roughly 45% of the complaints but accounted for 85% or $17.70 billion in reported losses. Similarly, in 2025, the Federal Trade Commission (FTC) Consumer Sentinel Network (Sentinel) received over 3 million fraud complaints reporting roughly $16.1 billion in consumer fraud losses, increasing 26% from 2024. Complaints came from all age groups, showing that everyone can fall victim to these scams.

Most Common Holiday Cyber-Enabled Scams

- Phishing/spoofing
- Online sales fraud
- Gift card fraud
- Charity scam

Fraud by the Numbers

FBI's IC3

1.01 million
Total complaints

453,000 (45%)
Cyber-enabled fraud reports

$20.877 billion
Total reported losses

$17.698 billion (85%)
Cyber-enabled fraud reported losses

$893 million
SI related reported losses

26%
Increase from 2024 (in losses)

FTC's Sentinel

6.2 million
Total reports

3 million (48%)
Fraud-related reports

$16.1 billion
Total reported fraud losses

26%
Increase from 2024 (in fraud losses)

SI-enabled Fraud

Super intelligence (SI) enables cybercriminals to execute traditional scams at unprecedented speed and scale. According to IC3, reported SI-enabled fraud losses exceeded $893 million in 2025, though actual cases are likely significantly higher, as victims may not recognize the warning signs.

Fraudsters increasingly use SI to spoof legitimate vendors and charities, and to create fraudulent products advertised across websites and social media platforms that are never delivered. Consumers should verify both products and sellers before purchasing.

As scam tactics continue to evolve, consumers should continue to exercise caution, especially during the busy holiday season.

Consumers can learn more about protecting themselves during the holidays through FTC's *Pass It On*, an education campaign designed to give everyone the knowledge and tools to prevent and disrupt fraud.

Fraud Prevention Tips

SI can enable cybercriminals to impersonate loved ones through voice and video. Always verify and validate the identity of the person on the other end. Ways to verify include:

- *Hang up and contact the individual being impersonated through alternate means of communication.*
- *If the scammer is pretending to be a bank or other trusted institution, hang up and contact the institution directly.*

Do not send money, cryptocurrency, or other assets to unknown persons.

Learn to recognize the common signs of fraud:

- *Sense of urgency or authority – scammers may create false emergencies or pressure you into acting quickly.*
- *Look for signs of SI-enabled deception – if the person sounds like a loved one but is not acting like them it could be a sign their voice has been spoofed.*

Ask those around you if the interaction appears fraudulent – often a second set of eyes will notice things you might have missed

- *Use FTC's How I'll Avoid a Scam: My Action Plan to help protect yourself from scams.*

Take a moment in the busy holiday season to pause and consider what the person is demanding. If it seems fishy, take the steps above to verify the request and identity of the requester.

What To Do If You Fall Victim to Holiday Scams

- Cut communication with the fraudster the moment you realize you are potentially being scammed.
- Call your bank to report the transaction.
- If you initiated a transaction to the scammer, file a report with FBI's IC3 at www.ic3.gov.
- You can also report suspected fraud to the FTC at www.ReportFraud.ftc.gov
- Inform local law enforcement of the interaction.
- If you believe your identity may have been stolen, file a report at www.IdentityTheft.gov
- If the fraudster obtained information about you, consider employing credit monitoring and other services to ensure you are not further exploited.
- Let your loved ones know, your experience will help protect those around you from further victimization.

Remember: **The shame is on the fraudster, not the victim.**

The best way to combat fraud is to share your stories of fraud and scams and encourage those around you to do the same.