THE U.S. DEPARTMENT OF THE TREASURY

Office of Cybersecurity and Critical Infrastructure Protection

Cyber-Safe Holidays: Recognizing and Avoiding Seasonal Scams

THE THREAT LANDSCAPE OF CYBER FRAUD

In 2025, cyber-enabled fraud continues to escalate as cybercriminals leverage emerging technologies to deploy increasingly convincing and sophisticated scams. In 2024, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) reported $16.6 billion in consumer losses, a 33% increase from 2023. During the holiday season, cybercriminals take advantage of increased online shopping, travel, shipping, charitable giving, and digital payments to steal sensitive information and perpetrate fraudulent activity. Staying aware of how scams evolve during this period helps consumers navigate the season safely and confidently.

SEASON OF SCAMS: MOST COMMON HOLIDAY SCAMS

BUSINESS IMPERSONATION

CHARITABLE GIVING

GIFT CARD DRAINING

The Federal Trade Commission (FTC) reported that imposter and impersonation scams were the top category reported to Consumer Sentinel in 2024. Leading up to and throughout the holidays, scammers frequently impersonate trusted brands and promote products at unusually low prices. Social media ads often direct to fake online stores that trick consumers into purchasing goods that are never delivered. According to a recent AARP survey, 39% of consumers filed fraud claims after purchasing something featured on a social media ad, up from 35% in 2024. IC3 receives tens of thousands of non-delivery and non-payment scam reports, costing consumers more than $785 million in 2024.

Americans contributed $592.5 billion to charitable organizations in 2024, according to Giving USA Foundation. Cybercriminals frequently exploit this generosity by creating fraudulent charities with convincing websites and aggressive email, mail, and telemarketing campaigns.

Gift card fraud also remains widespread. With 7 in 10 consumers planning to purchase gift cards in 2025, scammers continue tactics such as stealing card numbers from racks and draining the balance as soon as the card is activated.

EMERGING TECH SCAMS

Cybercriminals are increasingly harnessing artificial intelligence (AI) and cryptocurrency (crypto) to make scams more convincing, scalable, and difficult to trace. AI-based voice cloning, repeatedly flagged by federal agencies, allows criminals to mimic a family member's voice to request emergency funds, a particularly potent tactic during a busy travel season. AI-generated emails, ads, customer service chats, and even deepfake videos help scammers create highly realistic fake retailers, charities, and promotions.

FRAUD BY THE NUMBERS

$16.6B

Total losses reported to FBI's IC3 in 2024

$12B

Total losses reported to FTC's Sentinel in 2024

859,532

Total complaints received by IC3 in 2024

6.47M

Total reports received by Sentinel in 2024

83%

Of IC3 reports were specific to cyber-enabled fraud

40%

Of Sentinel reports were specific to fraud

$9.3B

Cryptocurrency losses reported to IC3 in 2024

$1.42B

Cryptocurrency losses reported to Sentinel in 2024

FIGHT BACK AGAINST FRAUD

Validate Sellers and Charities

Use independent reviews, official websites, and recognized charity registries – such as Charity Navigator and Charity Watch – to verify legitimacy.

Verify Before Engaging

Confirm unexpected messages about orders, deliveries, account issues, or urgent money requests by contacting the organization or person directly through trusted channels. Avoid using links or phone numbers provided in suspicious communications.

Use Safe Payment Methods

Choose payment methods that offer dispute protections, such as credit cards.

Strengthen Account Security

Enable multi-factor authentication, use complex and unique passwords, set transaction alerts, and closely monitor financial accounts, especially during the holidays.

Report Fraud Quickly

Report suspected fraud to your financial institution, the FTC, IC3. Provide screenshots, communications, and transaction details to support investigation or recovery efforts. Learn how to avoid a scam and what to do if you were scammed.

Remember

Holiday-themed cyber fraud is not merely a seasonal nuisance—it represents an annual surge layered on top of already unprecedented levels of fraud in the United States. As criminals adopt AI, expand crypto-enabled schemes, and exploit the spike in holiday transactions, heightened public awareness and basic protective steps remain our strongest defense.