



FS-ISAC

Security Tips Newsletter

7 November 2025 | Issue No. 26

Be cyber smart to stay cyber safe.

Be on the Lookout for Fraud Scams During the Holiday Season

Summary

Each year, people worldwide are visited during the holidays - and not just by jolly St. Nick. Rather, it's fraudsters who take advantage of the seasonal spirit, and they can take the cheer out of your holiday.

Types of Schemes

Fraudsters use the latest technology in a variety of fraud scams that are headed to a community near you. Be wary of solicitations on social media, search engines, text, and email, and keep an eye out for these schemes:

Charity Scams. Scammers invent fake charities or spoof real ones to take advantage of those who want to help the needy during the holidays.

Fake Holiday E-Cards and Party Invitations. Using a twist on the phishing playbook, fraudsters insert links in holiday e-cards and digital invitations that take you to bogus sites, then steal your credentials and/or distribute malware.

Fake Online Retail Stores. Criminals send unsolicited emails containing links to fantastic deals at the website of a retailer you've never heard of.

Black Friday and Cyber Monday Scams. The internet blows up with shopping ads for Black Friday and Cyber Monday.

2024 Fraud Losses

"The Federal Trade Commission (FTC) reported that consumers lost over \$12.5 billion to fraud in 2024, a 25% increase from the previous year."

- [PR Newswire](#)

"Reported scam losses in the U.S. totaled a record \$16.6 billion, according to the FBI's Internet Crime Complaint Center (IC3), a 33% increase from 2023. This figure includes over 859,000 reported internet crimes."

- [CBS News](#)

"One of three Americans have fallen victim to an online scam during the

Malvertising schemes – i.e., fake ads for real stores – can more easily go undetected when people are expecting promotions.

Fraudulent Gift Cards. Everyone loves the gift cards grandpa gives – *in person*. Be on the lookout for fraudsters who claim you will receive a gift card by filling out a simple form, which gradually lures you into providing sensitive information.

holiday season – and of the 58% of those who've lost money to such scams, nearly 1 in 10 lost over \$1,000."

- [Yahoo Finance](#)

Malware QR Codes. Scammers can create QR codes leading you to a malware-laced website to infect your mobile device and computer. Sometimes they print QR codes on stickers that can be placed anywhere, even over legitimate advertisements.

Travel Scams. Fraudsters are using artificial intelligence to clone messages and make deepfake videos to promote fake travel deals, vacation rentals, holiday cruises, and more. These videos and voice messages look real, but won't send you anywhere you want to go.

Red Flags

Look for these red flags before you click:

- Unsolicited emails and phone calls asking for your confidential information or for information they would already have if they were legitimate.
- A tone of urgency or veiled threats ("you have five minutes to respond," "the sender's feelings will be hurt if you ignore the link," etc.)
- Unfamiliar retailers or websites that have unclear return policies and no contact information other than an email address.

Prevention Tips

Stop. Think. Ask yourself, "Is this too good to be true?" Then, educate yourself about fraud tactics and how to prevent yourself from becoming a victim.

- Check website legitimacy using online tools (e.g., Better Business Bureau, getsafeonline.com, etc.).
- Verify charities independently – search for their website or call their office – before making a donation.
- Check online retailers' URLs carefully for typographical errors and unusual spellings – mistakes signal a spoofed site.
- Never click on a link from an unknown and unverified source.
- Never share your personal information and banking credentials.
- Update security patches as soon as they become available – or have them installed automatically.
- Use multi-factor authentication whenever possible.
- Regularly monitor your financial accounts.
- Forward text messages to SPAM (7726)—then report, block, and delete through your service provider.

Resources

- [Learn more about AI scams](#)
- [Get Safe Online website checker](#)

If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to [IC3.gov](https://www.ic3.gov), law enforcement, and file a report with the [Federal Trade Commission](https://www.ftc.gov)

Getting Help

If you have been the victim of a data breach or loss of your personally identifiable information, or identify suspicious activity involving your financial institution, contact them immediately.

TLP WHITE 



12120 Sunset Hills Rd, Reston
VA 20190



© FS-ISAC 2025

To manage emails you may receive, please log in to the Member Services platform of the Intelligence Exchange to [update subscription preferences](#).