UNITED STATES SECRET SERVICE

Tips for Avoiding Scams 2026 Holiday Season

The holiday season is one of the most profitable periods for cybercriminals. This United States Secret Service advisory contains information that can help Americans remain vigilant during the 2026 holiday season and beyond.

Holiday Shopping Scams

Scammers may create fake websites that look like popular shopping sites, but they are used to steal your personal and payment information. Scammers can even pay to make their fake websites appear at the top of search engine results. If you get an email promising a great deal or see an advertisement on social media, don't click the link. Instead, type a known website address into your browser or use the retailer's official app.

Accidental Payment Scams

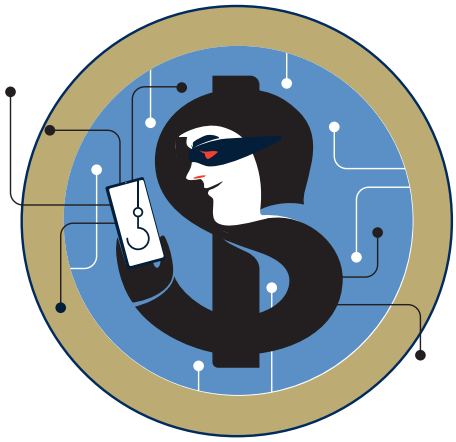
Scammers may send money to your payment app, claim it was sent by accident, and ask you to send the money back. This tactic may be used to initiate contact, pressure you into sending money, or disclose personal information. It may also be an attempt to commit fraud, theft, or money laundering. If you receive an accidental payment, don't send it back yourself. Contact the payment app's official customer support.

Investment Scams

Scammers may send unsolicited messages promising "quick returns" to help pay for holiday gifts, travel, or bills. After an initial investment, scammers may pressure victims to send more money. Be cautious of requests to pay with cryptocurrency or gift cards, send a wire transfer, or transfer money to a stranger's personal account. In 2025, the Internet Crime Complaint Center (IC3) received reports of more than $7 billion in losses from investment scams.

Charity Scams

Scammers may use the holiday season as an opportunity to steal money from people who want to donate to a good cause. Before donating in response to an unsolicited request, research the charity independently. Confirm that your donation will reach the intended charity and not a scammer.



Family Emergency Scams

Scammers may use technology to make calls that appear to come from and sound like a family member. If you receive a call from someone who sounds like a family member, claims to be in distress, and asks for money, it could be a scam. Hang up and call the family member using a phone number that you know belongs to them. If you cannot reach them, contact other family members or friends to verify the situation. In 2025, IC3 received complaints reporting more than $5 million in losses related to emergency or distress scams.

Online Invitation Scams

Scammers may send fake party invitations to steal your personal information, account credentials, or both. Be cautious of unexpected online invitations that request login credentials, financial information, or ask you to download a file. Even if you recognize the sender, contact them through a known, separate communication channel to confirm the invitation before opening links or attachments.

>

Tips for Avoiding Scams

Guard Your Personal Information

- Scammers may try to entice you to share personal or financial information. Do not provide this information unless you have independently confirmed that the request is legitimate.

Slow Down

- Scammers may promote deals that seem "too good to be true" or create a false sense of urgency to pressure you into acting without thinking. If you are pressured to act quickly, it may be a scam.

Use Caution When Shopping Online

- Scammers may use fraudulent websites to steal money and personal information from online shoppers. Confirm that an online retailer is legitimate before entering your payment-card information.

Use Gift Cards for Gifts, Not Payments

- Scammers may use gift cards in a variety of ways. Funds stolen from gift cards cannot be recovered. If someone demands payment by gift card, it is a scam.

Verify Charities

- Scammers may use names of fake organizations that are similar to reputable charities. Before donating, verify a charity through the BBB Wise Giving Alliance, Candid, Charity Navigator, or CharityWatch. Donate directly to a verified charity rather than through someone who claims to be an intermediary.



What to Do If You Are a Victim

Report fraud schemes to your local law enforcement agency, the Federal Trade Commission at https://reportfraud.ftc.gov, and the Internet Crime Complaint Center at https://www.ic3.gov/.

The United States Secret Service works closely with state, local, tribal, and territorial law enforcement agencies to investigate financial crimes.