Don’t let scammers steal your holidays.

There are some common scams that thieves run through the holidays. Check out these tips to avoid holiday heartache and stay secure.

Phishing & lookalike sites

Phishing attacks target online shoppers with sites that imitate retailers. They post great limited-time deals for hard-to-get items in order to steal your credit card number and home address.

Check the URL in your browser.

Hover over suspicious links to see where they go.

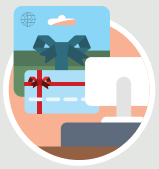
Watch for overly general greetings, misspellings, & suspicious sender email IDs.

Use credit cards rather than debit cards online. Unauthorized purchases are easier to dispute.

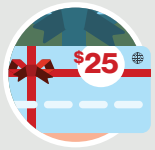
Keep an eye on your bank account.

Gift card fraud

Scammers sometimes copy codes off the back of gift cards on store racks, then wait and spend the money the second the cards are activated by a legitimate purchaser.



Buy gift cards from behind the counter.



Check the balance on pre-loaded cards.

Make sure the protective scratch-off tape on the back is intact.

Fake charities

We're more charitable during the holidays. Scammers know this so they cash in by soliciting donations under the guise of a good cause. Charity Navigator helps verify legitimate charities.

Avoid making donations by phone or mail.

Research charities before you donate.

Charity Navigator can help.

Letters from Santa

A recent scam offers to send personalized letters from Santa to your child with official “nice list” certification, for a small fee. But they can also grab credit card numbers or personal information.

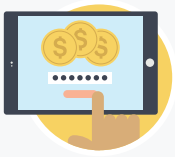
Watch for overly general greetings, misspellings, & suspicious sender email IDs.

Research the service before buying in.

Calls for immediate action are red flags.

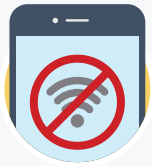
Public WiFi

Public WiFi is risky. You never know who else is connected, and hackers can gain access to your computer. They also set up fake hotspots to capture sensitive information like credit cards.



Avoid checking financial information or making purchases.

Logging onto social media accounts can expose sensitive information.

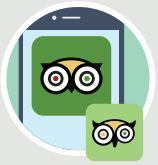


Try to verify connection is legitimate. Use VPN for Verizon internal network.

Fake iOS & Android apps

They may look like apps from your favorite companies, but they can steal your personal information when you download them, log in, search for products or place orders.

Only download from the official Google Play or Apple App stores.



Scammers imitate legitimate names.

Watch for typos or poorly formatted interfaces.

Only allow third-party app downloads from trusted sites.