Holiday scam awareness: Stay cyber safe this holiday break

Version 4

Published 12/9/2025 by Giuseppe Aloisi Last updated 12/11/2025 7:56 PM by Ran Luo

As the holiday season approaches, online shopping and package deliveries surge—and so do scams. Cybercriminals take advantage of the rush with fake websites, fraudulent messages, and too-good-to-be-true offers. Use this quick guide to stay safe before the holiday break.

Stay alert, shop smart, and enjoy a safe holiday season!

1. Watch for “Too Good to Be True” Deals

Scammers push unrealistic discounts, limited-time offers, and fake “back-in-stock” alerts. If the price or urgency seems suspicious, assume it's a scam until verified.

2. Double-Check the URL

Fraudulent websites often mimic real ones, look for:

- Misspellings (e.g., **walmarrt**, **bestbu-y**)
- Odd domains (e.g., **amaz0n.deals**, **.shop**, **.info**)
- Links sent from unsolicited texts or emails

Tip: Type the official URL manually or use bookmarks.

3. Don’t Click on Package or Order Links

Fake delivery notices spike during the holidays:

- “Your package is delayed—click to verify”

- “Confirm payment information”
- “Your order needs attention”

Tip: Go directly to the official website/app instead of tapping the link.

4. Recognize Payment Scams.

These are **always** scams:

- Requests for **gift cards**, **crypto**, or **wire transfers**
- Urgent “pay now” threats
- Overpayment scams or “refund the difference” requests

Tip: No legitimate business or government agency uses these methods.

5. Shop Safely Online

- Use a **credit card**, not a debit card—credit offers better fraud protection
- Enable **2FA (two-factor authentication)** and PassKeys where possible. Never share accounts
- Avoid entering payment info on public Wi-Fi

6. Verify Using Official Channels

If something feels off:

- Visit the official website yourself
- Call the company using verified contact details
- Delete suspicious messages without interacting

Tip: Trust your instincts—pausing for 10 seconds can prevent major fraud.

7. Report suspicious emails or calls

- If you receive suspicious emails in your Seneca inbox, use the Report Phish button
- Personal email report them using their built-in spam or fraud tools
- Report suspicious calls or text messages in your messaging apps

Tip: Don’t reply or provide information if you don’t know who you are interacting with!

tags : student-news