TRIBAL ISAC
INFORMATION SHARING & ANALYSIS CENTER

Holiday Shopping? Stay Safe Online This Season.

This holiday season from November to January, criminals will continue their attempts to scam users with fraudulent enticing deals, fake charities or causes, and fake travel offers or hotel reservations. Criminals want access to user accounts and devices. What do some of these scams look like?

Fake Online Stores & Deals: Scammers create look-alike websites or social media ads offering deep discounts on popular gifts like toys or electronics. Watch out for fake app stores as well.

Phishing Emails or Texts: These are messages that appear to come from shipping companies, retailers, or charities. They often claim a delivery issue or promotion and include malicious links.

Charity Scams: Fraudsters set up fake donation pages or impersonate real charities to steal money or data. Watch out for criminals using disasters or tragedies as a lure as well.

Gift Card & Sweepstakes Scams: Scammers ask users to pay with gift cards or to claim a prize that needs upfront fees or personal details.

Fake Order Confirmations: Phishing emails or texts that mimic legitimate companies and claim you made a purchase or need to verify an order. Beware of typos in the domain names or info that doesn't match the store.

Travel Scams: Beware of fake holiday rental listings, airfare that seems too low, or deals that ask for deposits or full payment upfront.

Social Media Shopping Traps: Watch out for posts or ads for trending products at unrealistic prices, often from new or unverified sellers.

Warning Signs. **Expect to see some common warning signs of holiday scams**.
- *The website lacks HTTPS (no padlock symbol)*
- *Requests for gift cards, crypto, or wire transfers*
- *Messages with pushy sales tactics*
- *Suspicious or mismatched sender addresses or domains*
- *Prices that seem too low*
- *Misspellings, poor grammar, or unusual phrases on the site or email*

Trust your gut! If a message appears to be from someone you know, pay attention to the *tone* and context of the message. If the wording doesn't sound like them, or the overall tone is off, it's likely a scam!

- If you intend to shop online, go to the vendor's website and confirm if the deals are there.
- Check your passwords, update them if needed, and consider using a password manager.
- Update patches for your web browsers to stay ahead of malware and criminals exploiting vulnerabilities.

Report Scams – even if you're not sure if it's a scam, or if you already opened or actioned it. Report scams to the tribal helpdesk, tech support, or your manager/supervisor. **Your reports help** more messages get blocked. Additionally, if you believe you've personally been a victim of a cyber scam, report the fraud to the FBI Internet Crime Complaint Center (IC3) at www.ic3.gov or the Federal Trade Commission at https://reportfraud.ftc.gov/