STAR
Bank | Insurance | Private Advisory

The Grinch who Scammed Christmas

Just as the Grinch is looking to steal your holiday cheer, scammers also want to rob you of your hard-earned cash and/or personal identifying information (PII). As you embark on holiday shopping, make yourself aware of common holiday scams and fraud. The two most prevalent frauds are **non-payment** and **non-delivery transactions**.

In non-payment fraud, a seller ships a product and is never paid. In non-delivery fraud, the buyer pays for an item but the seller never ships the product.

Other holiday scams to be on the lookout for in 2022:

- **Fake retailer websites -** Social media or phishing email links directing buyers to a bogus website.
- **Gift Card Scams -** Untraceable funds are a favorite for scammers.
- **Fake Charities -** The holiday season is a great time to donate to a cause dear to your heart. Scammers take no shame in preying on the charitable nature of good people.
- **Holiday/seasonal employment scams -** While legitimate employers utilize seasonal workers, make sure you are not providing any PII to bad actors.

Tips to avoid being scammed:

- **Safeguard your personal belongings (wallet, purse) when shopping.**
- **Beware of phishing - Verify any and all requests for your PII.**
    - Email - Prize winnings, account closure, credit card charges, account cancellation notices, etc.
    - Text - Unsolicited messages requesting information, or links to click.
    - Phone calls - from "spoofed" numbers appearing to be from companies, banks or government officials.
- **Regularly monitor your bank accounts and balances.**
- **Know whom you are buying from, or selling to, and avoid certain payment methods.**
    - Never wire funds to individuals.
    - Peer 2 Peer (P2P) payment methods (Venmo, Zelle, CashApp, etc.) are for friends and family – **not for online marketplace purchases.**
    - Never purchase gift cards from individuals.
    - Shop online with well-known retailers.
    - Shop on secure websites; look for the letters "http(s)" to begin the web address, indicating a secure website.
- **Practice online safety and awareness**
    - Do not open emails or click links on unsolicited text/email messages.
    - Do not use the same password for all your logins.
    - Consider an encrypted password manager.
    - Ensure your computer's antivirus software is up to date.
- **If something seems "too good to be true" it probably is.**

May you experience joy this holiday season and the financial peace of mind that comes from following these tips and staying aware of emerging fraud trends. Happy Holiday Shopping from your STAR Fraud Investigations Team.