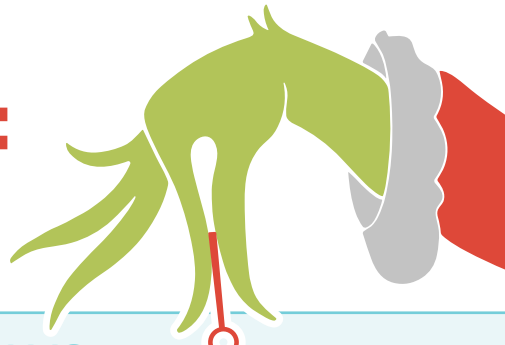
LOCK OUT FRAUD

HOLIDAY SCAMS:
DON'T LET SCAMMERS STEAL YOUR CHEER



WHY HOLIDAY SCAMS ARE **DANGEROUS**

Holiday scams are particularly dangerous because of how well they blend in with legitimate seasonal activities. During the holidays, everyone is busy traveling, shopping, and giving. Deals come and go, multiple shipping notices are updated regularly, and charities ask for donations. Criminals will try to sneak fake messages through with the real ones. They will try to trick consumers using false urgency, by claiming that a sale ends tonight, a package can't be delivered and needs additional information from you now, a family member is in need, or a charity needs your donation urgently.

IF YOU'VE BEEN A VICTIM OF A HOLIDAY SCAM

Don't be embarrassed. Stop sending money and contact the bank immediately. The sooner the bank is notified, the better they can help.

Wisconsin consumers should also report holiday shopping scams at consumerprotection.wi.gov or 800-422-7128. If personal information has been compromised, visit identitytheft.gov for guidance. Report the incident to the Federal Trade Commission and the FBI Internet Crime Complaint Center at ic3.gov to help authorities track and combat scam trends.

BEWARE OF HOLIDAY SCAMS

The holiday season is a busy time, and criminals know it. They will try to use the rush of the season to trick people into sending money or sharing personal information. Be cautious of fake online stores, fake listings for popular gifts, fake delivery notices, and fake charities. Criminals will use these to send scam texts, emails, phone calls, social media, and online ads. They may even disguise themselves as a retailer, shipping company, or charity you already know and trust.



HOW TO **PROTECT YOURSELF**

Scammers count on consumers being too busy to recognize something's off. Take a moment and pause before clicking, buying, or giving. Verify directly through a retailer, shipping company, or charity's official website. Always verify independently before following through on any request. Also, remember that scammers often ask targets to pay with gift cards, wire transfers, cryptocurrency, or payment apps because that money is difficult to trace and get back.

- **Be skeptical of deals that seem too good to be true.** Especially on websites or from unrecognized sellers.
- Before using an unfamiliar store, look for legitimate reviews, a customer service number, or a physical location. **Remember: criminals may even pose as legitimate retailers, shippers, or charities, so always verify.**
- **Don't click on links or respond to texts or emails** about a missed delivery, a shipping fee, or a problem with a package.
- **Track packages** by going directly to the retailer or shipping company's official website or app.
- **Verify a charity before donating.** Watch out for look-alike names and websites. Scammers may copy the name, logo, or phone number of a real charity.
- **Never let someone pressure you into giving immediately.** A legitimate charity will welcome a donation tomorrow just as readily as today.
- **Give directly** through the charity's official website rather than through a link in a text, email, or social media post.

To see more Lock Out Fraud Resources, check out: wisbank.com/lock-out-fraud/

Wisconsin Bankers ASSOCIATION