BROKEN ARROW
CHAMBER of COMMERCE

CHAMBER MEMBER NEWS

Five Tips to Avoid Fraud This Holiday Season

By: Barbara Russo, Vice President of Digital Strategy, TTCU Federal Credit Union

Nothing would take the joy out of your holidays quite like being scammed. Here are five of the most common scams that TTCU's staff have seen lately – and how to avoid them.

1. Shop reputable companies online.

More holiday shopping is expected to take place online than ever before. But it is good to stick to companies you know. A recent Federal Trade Commission report said that the most common type of fraud started with ads on Instagram and Facebook offering bargain prices. These are often from companies you've never heard of. The scammers work hard to make the ads and their website look legitimate, with professional photos and graphics. Often, the item never arrives, or it may take several months to be delivered and not resemble the photo. Ordering from companies you know can help you avoid holiday shopping headaches this Christmas.

2. Avoid romance scams.

The holidays can be lonely for many people, and this year it's even worse because of the isolation of COVID. Online dating sites can provide access to potential companions, but keep in mind that some of these people may be fraudsters. The scammers build fake personas using false photos and biographical details, often messaging many people at once. They'll talk to their potential victims for up to a year, waiting until the person feels a deep connection before the scammers ask for money. On average, the victims lose $5,000, but might lose much more.

3. Be careful when opening emails.

Another tactic scammers use is to send fake emails – called phishing – to try and capture your personal information. Be wary of emails that contain typos, ask for personal information or try to get you to open an attachment or click a link. Always hover with your mouse over a link in an email before clicking to make sure you're being directed to the site you think you are.

One scam email that many TTCU members have received recently claims to be from your email provider notifying you of a problem with your account. Some other common phishing scams include fake flyers and deals, fake shipping notices, and fake receipts and invoices.

4. Avoid giving scammers access to your devices.

One frequent tactic scammers use is to call claiming to work for a legitimate company – such as Microsoft – and tell you that your computer has a virus. They will direct you to download a program or app that gives them access to your computer, allowing them to capture your private information, including online banking logins.

Another form of fraud involves payment methods such as Cash App. These only offer customer service through the app itself. But fraudsters have put phone numbers online. If you call one of these fraudulent numbers, you'll be directed to download another app, which allows the scammers to access your Cash App data, including banking information.

5. Check your accounts more frequently.
Fraud is more common over the holidays, so checking your accounts frequently can help you stop theft in its tracks. Watch for unauthorized transactions or purchases you don't recognize. If you think your account may be compromised, reach out to your financial institution as soon as possible.

Be alert to potential fraud, and have a safe and happy holiday season!

Source:
https://www.ftc.gov/news-events/blogs/data-spotlight/2020/10/scams-starting-social-media-proliferate-early-2020

Barbara Russo
Vice President of Digital Strategy
TTCU Federal Credit Union

Barbara Russo is the Vice President of Digital Strategy for TTCU Federal Credit Union. She has over 20 years of experience working in financial fraud prevention and mitigation.