November Blog

Holiday Scams to Watch Out for This Season: Protect Your Money and Personal Information

The holiday season is a time for giving, shopping, traveling, and spending time with loved ones. Unfortunately, it's also one of the busiest times of year for scammers. As people shop for gifts, donate to charities, and prepare for holiday celebrations, fraudsters look for opportunities to steal money and personal information.

At Emerald Credit Union, we're committed to helping our members make informed financial decisions and protect their financial well-being. Understanding common holiday scams and knowing what warning signs to look for can help you enjoy the season with greater peace of mind.

5 Common Holiday Scams to Watch Out For:

1. Fake Package Delivery Notifications

Ordering gifts online is convenient, but scammers often take advantage of the increase in holiday deliveries. You may receive a text message or email claiming that a package couldn't be delivered, your address needs to be confirmed, or a small redelivery fee is required.

These messages may contain links to fake websites designed to steal your personal information, payment details, or account credentials.

How to protect yourself:

- Be cautious of unexpected delivery notifications, especially those requesting payment or personal information.
- Avoid clicking links in unsolicited texts or emails.
- Track packages directly through the retailer's website or the shipping company's official website or app.
- Never provide your banking information to resolve an unexpected delivery issue.

Remember: If a delivery message creates urgency or asks you to pay an unexpected fee through a suspicious link, stop and verify it before taking action.

2. Online Shopping Scams

Holiday sales can be tempting, especially when you're trying to find the perfect gift at a great price. Unfortunately, scammers may create fake online stores, copy legitimate retailers' websites, or advertise products at prices that seem too good to be true.

You might pay for an item that never arrives or unknowingly provide your payment information to a fraudulent seller.

November Blog Pt. 2

Holiday Scams to Watch Out for This Season: Protect Your Money and Personal Information

How to protect yourself:

- Shop with reputable retailers and verify website addresses before making a purchase.
- Be cautious of unfamiliar websites offering unusually low prices.
- Research sellers and look for independent customer reviews.
- Use secure payment methods and review your account transactions regularly.
- Avoid making purchases through suspicious social media advertisements or unsolicited messages without verifying the seller.

If a deal seems too good to be true, take a moment to investigate before entering your payment information.

3. Fraudulent Charities and Donation Requests

The holidays inspire many people to give back to their communities. Unfortunately, scammers sometimes take advantage of that generosity by pretending to represent charitable organizations or families in need.

Fraudulent donation requests may arrive by email, phone, text message, or social media. Scammers may use emotional stories or pressure you to donate immediately without giving you time to verify the organization.

How to protect yourself:

- Research a charity before donating.
- Visit the organization's official website instead of clicking links in unsolicited messages.
- Be cautious of high-pressure requests that demand immediate payment.
- Avoid donating through gift cards, cryptocurrency, or wire transfers when someone you don't know requests them.
- Ask how your donation will be used and verify that the organization is legitimate.

Giving back is a wonderful part of the holiday season. Taking a few extra minutes to verify a charitable organization can help ensure your generosity reaches the people and causes you want to support.

4. Gift Card Scams

Gift cards are popular holiday gifts, but scammers also use them to steal money. A fraudster may impersonate a government agency, a business, a family member, or even a supervisor and insist that you purchase gift cards to resolve an emergency or pay a bill.

Holiday Scams to Watch Out for This Season: Protect Your Money and Personal Information

They may ask you to send the gift card numbers and PINs. Once those details are shared, the money can be difficult or impossible to recover.

How to protect yourself:

- Never use gift cards to pay unexpected bills, fees, fines, or debts.
- Be suspicious of anyone demanding gift card payments to resolve an urgent situation.
- Verify unusual requests by contacting the person or organization through a trusted phone number.
- Keep gift card receipts and inspect physical cards for signs of tampering before purchasing them.

A good rule to remember: Legitimate businesses and government agencies do not require gift cards as payment for bills, taxes, or fines.

5. Phishing Emails and Text Messages

Phishing is a common form of fraud in which scammers impersonate trusted organizations to trick people into revealing sensitive information. During the holidays, these messages may appear to come from financial institutions, retailers, delivery companies, or popular online services.

A message might claim that your account has been locked, a payment has been declined, or suspicious activity has been detected. It may urge you to click a link and enter your username, password, debit card number, or other personal information.

How to protect yourself:

- Don't click links or open attachments in unexpected messages.
- Never share your passwords, PINs, or one-time verification codes with someone who contacts you unexpectedly.
- Contact the organization directly using a verified phone number or its official website.
- Pay attention to unusual wording, suspicious sender addresses, and unexpected requests.
- Enable multifactor authentication when available.

Remember that scammers can make messages look convincing. Even a message that uses a familiar logo or appears to come from a trusted organization may be fraudulent.

November Blog Pt. 4

Holiday Scams to Watch Out for This Season: Protect Your Money and Personal Information

Warning Signs That a Message Could Be a Scam

Although holiday scams take many forms, they often share similar warning signs. Be cautious if you encounter a message or request that:

- **Creates a sense of urgency.** You're told to act immediately or risk losing money, access to an account, or a special offer.
- **Requests sensitive information.** Someone asks for your password, PIN, account details, or verification code.
- **Offers something that seems too good to be true.** You win a prize you never entered to receive or find an unbelievable deal from an unfamiliar seller.
- **Demands unusual payment methods.** You're asked to pay with gift cards, cryptocurrency, or an unexpected wire transfer.
- **Contains suspicious links.** A message directs you to an unfamiliar website to confirm information or make a payment.
- **Pretends to be someone you trust.** A scammer impersonates a financial institution, business, charity, or loved one.

When something doesn't feel right, trust your instincts. Pause, verify the request independently, and never let pressure force you into a financial decision.

What Should You Do If You Suspect Fraud?

If you believe you've encountered a scam or accidentally shared personal or financial information, taking action quickly can help limit potential damage.

1. **Stop communicating with the suspected scammer**. Don't send additional money or information.
2. **Contact your financial institution.** If you shared banking information or believe your account may be compromised, contact your credit union using a verified phone number.
3. **Review your account activity.** Look for unfamiliar transactions and report anything suspicious promptly.
4. **Secure your accounts.** Change compromised passwords, use unique passwords for important accounts, and enable multifactor authentication where available.
5. **Report the incident.** You can report suspected scams to the Federal Trade Commission at ReportFraud.ftc.gov. If you shared your Social Security number, visit IdentityTheft.gov for guidance on protecting your identity.

November Blog Pt. 5

Holiday Scams to Watch Out for This Season: Protect Your Money and Personal Information

If you sent money through a payment service, contacted a fraudulent seller, or purchased gift cards for a scammer, contact the relevant bank, card issuer, or payment provider as soon as possible. Recovery isn't guaranteed, but acting quickly may help.

Enjoy a Safer Holiday Season with Emerald Credit Union!

The holidays should be a time to celebrate, connect, and create lasting memories—not worry about financial fraud. By staying alert, protecting your personal information, and taking time to verify unexpected requests, you can reduce your risk of becoming a victim of a scam.

At Emerald Credit Union, we're proud to guide and grow with our members throughout life's financial journey. Financial education and awareness are important parts of building lasting financial well-being, and we're here to help our members make informed decisions about their money.

If you receive a suspicious message claiming to be from Emerald Credit Union or have concerns about unusual activity on your account, contact us directly using our official contact information. Never rely on the contact details provided in a suspicious message.

From all of us at Emerald Credit Union, we wish you a happy, healthy, and financially safe holiday season!

EMERALD CREDIT UNION