Valley First
CREDIT UNION

Holiday Scams: How to Protect Yourself During the Busy Season

The holiday season brings plenty of opportunities to shop, travel, and give back to the community. Unfortunately, it also creates opportunities for fraudsters looking to take advantage of increased spending and the fast-paced nature of the season.

Understanding how holiday scams work can help you protect your personal information, your accounts, and your finances.

What Are Holiday Scams?

Holiday scams are fraudulent schemes that capitalize on seasonal activities such as online shopping, charitable giving, package deliveries, and holiday travel. Scammers know that people are often busier than usual during this time of year and may be more likely to act quickly without verifying a request.

Criminals frequently impersonate trusted retailers, shipping companies, charities, financial institutions, or popular online services. They may send urgent messages claiming there is a problem with a package, an account issue, or a limited time offer that requires immediate action.

Their goal is simple: to steal money, personal information, login credentials, or payment details.

Common Holiday Scams

Online Purchase Scams - Fraudsters create fake websites or online listings that advertise popular products at deeply discounted prices. After payment is made, the merchandise never arrives.

Non-Payment Scams - Individuals selling products online may encounter buyers who appear legitimate but never complete payment after receiving the goods or services.

Auction and Marketplace Fraud - Some scammers misrepresent products sold through online marketplaces or auction sites. The item received may be significantly different from what was advertised, defective, or counterfeit.

Gift Card Scams - A common red flag is anyone requesting payment using gift cards. Scammers often claim gift cards are needed to pay fees, taxes, utility bills, or secure a special offer. Remember: Legitimate businesses, government agencies, and financial institutions will not demand payment through gift cards.

Shipping and Delivery Scams - With increased package deliveries during the holiday season, fake shipping notifications become more common. These messages often contain links designed to steal personal information or install malicious software on your device.

How to Protect Yourself

Taking a few simple precautions can significantly reduce your risk of becoming a victim of holiday fraud:

1. Use Strong Passwords and Multi-Factor Authentication

Create unique passwords for your online accounts and enable multi-factor authentication whenever available. This adds an extra layer of security if your password becomes compromised.

2. Verify Websites Before Making a Purchase

Before entering payment information, make sure the website address is legitimate and begins with "https://". Take a moment to confirm that you are shopping with a reputable retailer.

3. Be Skeptical of Deep Discounts

If a deal seems unusually attractive or significantly lower than competitors' prices, proceed with caution. Scammers often use unrealistic discounts to lure shoppers into making quick purchases.

4. Avoid Clicking Suspicious Links

Never click links or download attachments from unexpected emails, text messages, or social media messages. Instead, navigate directly to the company's official website or contact the organization through verified channels.

5. Monitor Your Accounts Regularly

Review your account activity throughout the holiday season. Identifying suspicious transactions quickly can help minimize potential losses.

Stay Alert This Holiday Season

Fraudsters rely on urgency, excitement, and distraction to successfully carry out their schemes. Taking a few extra moments to verify offers, delivery notifications, and requests for information can help keep your finances secure.

If something seems suspicious, trust your instincts and investigate before taking action. A little caution can go a long way toward helping you enjoy a safer, more secure holiday season.

Valley First Tip: If you receive a phone call or message claiming to be from Valley First and are unsure whether it is legitimate, contact us directly using a trusted phone number or visit your local branch. Never use contact information provided in a suspicious email, text, or social media message.