

South Dakota Office of the Attorney General

FOR IMMEDIATE RELEASE: Tuesday, Nov. 26, 2024

Contact: Tony Mangan, Communications Director, 605-773-6878

Attorney General Jackley Reminds Shoppers About Holiday Scams

PIERRE, S.D. – With the Christmas shopping season starting in earnest this week, South Dakota Attorney General Marty Jackley warns shoppers that scammers look to dampen the holiday spirit.

"Scammers enjoy the holidays for all the wrong reasons," said Attorney General Jackley. "They are always looking for ways to steal a person's personal and financial information whether people are shopping in a store or online."

One common scam during the holidays is receiving an email or text from the U.S. Postal Service, Federal Express or another delivery service telling the customer they have a package waiting and to click onto to the attached link for delivery instructions. Never click onto such a link but contact the delivery organization directly to confirm the information.

A scam that has increased during the holiday season involves gift cards. People who purchase gift cards should carefully check the card to make sure there has been no visible tampering with the package or the area to scratch off the code.

"Before you sign for an unexpected delivery, click onto a strange website or email, or agree to buy something over the telephone or Internet, always take a few minutes check out things first," said Attorney General Jackley.

If you believe you have been a victim of a shopping scam or theft, you are encouraged to call the Consumer Protection Division at consumerhelp@state.sd.us or call 1-800-300-1986 or 605-773-4400.

Consumers can also sign up for Consumer Alerts via email from the Consumer Protection Division at www.consumer.sd.gov. Email addresses will not be shared or sold to a third party.

The Consumer Protection Division offers these tips on how to stay shopping safe:

IN-STORE PURCHASES

- 1. Check the refund and return policies for restrictions and exceptions.
- 2. Are there re-stocking fees for returned items?
- 3. When buying gift cards, check for fees and expiration dates that apply.
- 4. Compare Prices.
- 5. Review warranties before purchasing.

Along with those traditional shopping methods consumers also need to proceed with caution when dealing with online retailers.

ONLINE SHOPPING TIPS:

- 1. Always place orders from a secure **connection** If your computer isn't protected from potential malicious software, your financial information and passwords are at risk from being stolen and anything else you store on your computer or do online.
- 2. Avoid offers that seem "to good to be true" Any e-store that promises too much at too low a price should cause you to pause before going forward. Look-a-like sites are out there waiting to take your information and money.
- 3. Don't use an e-store that requires more information than necessary to make the sale. Expect to provide method of payment, shipping address, telephone number, and email address IF the merchant requests other information walk away from the sale. Never give your bank account or social security information.
- 4. Need to create a password for a site? make it unique. Most site will allow you to make the purchase as a guest but if you want to create account use a unique and strong password.
- 5. Is the site secure? Look for the "https" NOT "http" the 's' tells you website is secure and encrypted to protect your information.
- 6. Use a Credit Card to make your purchases Credit cards have standard protections in place should your card information be stolen.
- 7. ALWAYS check the company's shipping and return policies. Know the time frames for eligible returns and do you need a RMA, Return of Merchandise Authorization number before returning merchandise.
- 8. ow the time frames you may be up against if you need to return the product.
- 9. If the Terms and Conditions are buried within the site or if they are vague stop and think before completing the purchase.

SMARTPHONE SHOPPING TIPS:

- 1. Be sure your computer and mobile devices are current with all software updates.
- 2. Be cautious of social media scams. Stick to the sites that you are familiar with and do not click on unfamiliar links.
- 3. Research price comparison apps. There are many malicious mobile apps just ready to be downloaded.
- 4. Do not download apps from unknown sources.

SCAM MESSAGE TIPS:

- 1. Never click or access the link that is provided.
- 2. Always go directly to source and contact them.
- 3. Scammers may tell you there is a fraud investigation, and you must "verify" your account or claim there is an unauthorized or fraudulent activity on your Amazon account
- 4. Common ways to detect a fake message:
 - 1. Misspelling and poor grammar;
 - 2. Abnormally long numbers;
 - 3. Suspicious link nothing relevant to the company they say they are from;
 - 4. Message is urgent; and,
 - 5. Message offers a refund.