

FOR IMMEDIATE RELEASE:

Contact: James Hallinan

December 10, 2015

(505) 660-2216

Attorney General Issues Holiday Scam Alert

Albuquerque, NM – As the shopping season ramps up, Attorney General Hector Balderas issued a holiday scam alert today to help New Mexicans protect themselves. The three most prominent holiday scams New Mexico may experience involve fake online shopping websites, fraudulent gift cards and fake charities.

“I want all New Mexicans to be aware of the threat scammers pose this holiday season as they attempt to prey on New Mexicans’ generosity,” said Attorney General Hector Balderas. “Whether it’s fake shopping websites, depleted gift cards, or even fake charities, scammers are out in force during the holiday season. Do your research and don’t become a victim.”

ONLINE SHOPPING – FAKE WEBSITES

The scam: Scammers launch a copycat website of a well-known retailer – or, create a website offering popular, sometimes previously "sold out" merchandise at crazy discounts.

How it works: A classic phishing scam – often by email but increasingly through links on social media sites – the email appears to come from a legitimate company and the link sends you to a phony website where you're asked to enter personal information.

What to do: Search the retailer; type in "vendor name + scam" and see what comes up.

Type URLs directly into your browser; do not click on a link from an email or social media site unless you are absolutely sure the message is from the legitimate business.

On the payment page, look for "https" at the beginning of the address (the "s" stands for "secure").

Shopping on a new site? Look for a return policy and contact information including a real address, a toll-free customer service number, and other ways to reach the company if you have a problem.

Use a credit card, NOT a debit card, when shopping online for greater protections against possible fraud.

GIFT CARDS

The Scam: Depleted gift cards

How it works: Thieves hit a store gift card rack, secretly write down or electronically scan the numbers off the cards, then check online or call the toll-free number to see if someone has bought the cards and activated them. As soon as a card is active, the scammers drain the funds. By the time you, or the person you give it to, try to use the same card that was actually purchased, the money is long gone.

What to do: Only purchase gift cards from reputable sources. Better yet, get them directly from the store they're from – and preferably directly from the store cashier – and ask them to scan the card to ensure it has the correct balance.

Carefully examine both sides of the card and look for signs of tampering such as an exposed PIN. If you find anything questionable, ask for another card and examine that one, too.

Online gift card purchases should be made directly from the retailer's website. Never buy them on auction sites even if it looks like a great deal; these cards may be stolen or counterfeit.

Keep your receipt as proof of purchase until the card's value has been exhausted.

Don't provide your personal information: no reputable business will require you to provide your Social Security number, bank account information, or date of birth in order to purchase a gift card; you're not applying for credit.

FAKE CHARITIES

The scam: The end of the year is a prime time for charitable donations, and scammers try to take advantage. Fake charities are among the most popular holiday scams.

How it works: Scammers either misuse the name of a genuine organization, or make up their own and ask you for money.

What to do: Only donate to charities you know. If a new charity piques your interest, be sure to verify it on nmag.gov, charitynavigator.org, guidestar.org or through the Better Business Bureau.

If you get a request via phone, call the charity back and ask if they can send you material about them to your address.

Don't donate cash, use a wire transfer or a prepaid credit card. Verify the organization's correct name and donate by check.

Beware of charities that raise funds for local fire fighters or police. Check their authenticity before offering money.

Ask how much of your donation will go for the cause. Some charities often spend the majority of their money for internal operational costs.

FIVE TIPS TO FOLLOW IF YOU'VE BEEN VICTIMIZED:

File a police report. Go to your local police station and file a report about the fraud or scam so you can prove to your bank and credit reporting companies you've been scammed.

Tell your credit card company and bank. If you are the victim of identity theft or some other financial scam, contact the fraud department at your credit card company and bank. You may have to close the account or the institution may just remove the fraudulent transactions.

Report the fraud to the three credit reporting companies. Do this as soon as possible, especially if your personal information was used to take out a new credit line, make purchases, take out loans, or anything else that could affect your credit. Each credit reporting company has a fraud unit: Equifax: (800) 525-6285; Experian: (888) EXPERIAN or (888) 397-3742; TransUnion: (800) 680-7289.

Gather evidence. In addition to the police report, save what you can related to the suspected fraud. Having items such as letters/emails of solicitation, prospectuses, cancelled checks, cash receipts, receipts for cashier's checks or money orders, bank statements, investment statements, or medical statements could help you get your money back or protect yourself from further victimization.

Report the scam to the Office of the Attorney General's Consumer Protection Division by calling 505-222-9100.

###