VIEW ONLINE PRINT

The holiday season is in full swing, and it seems like everyone but the fraudsters are full of good will. Since the best defense against a scam is an informed consumer, this issue of the of the Florida Consumer e-Newsletter is full of information to help you keep your holidays merry and bright.

Protect Against Pet Scams

Considering buying a pet this holiday season? Make sure you do your homework before buying. Unfortunately, there are scammers out there who will lure their victims in with the promise of a new furry friend only to defraud them of hundreds or even thousands of dollars.

In a typical pet sale scam, a consumer will see an advertisement for an animal, most commonly a dog, accompanied by heartwarmingly cute pictures. The seller will usually claim to be far away but will offer to ship the animal to the new owner's location. Unfortunately for the buyer, the scammer doesn't truly have any pets for sale and is just sending pictures of animals found on the Internet.

Once the buyer sends the money, the scammer will come up with extra fees like crate rentals, pet insurance, vet bills, and unexpected shipping costs that must be paid before the pet can

be delivered to its new home. As long as the victim is willing to pay, the scammer will continue adding on new fees. The scammer typically uses untraceable wire transfers so once the buyer catches on, their money is long gone.

Look for the following red flags to avoid becoming a victim of a pet scam:

- **Wiring Money:** Never wire money to anyone you have met online. Also exercise caution when using peer to peer payment methods like Venmo, Google Pay, Apple Pay, Facebook Payments or Zelle.
- **Suspicious Photos:** Look out for pet images that look like stock photos. Consider doing an online image search of the photo to see if it's posted somewhere else.
- **Bogus Stories/Excuses:** Scammers will often come up with complicated reasons why they need immediate wire transfers or why they can't deliver a pet directly to you.

Additionally, the Florida Pet Law is a consumer guarantee that provides standardized health requirements for dogs and cats being sold or transported. Consumers should ask for a Health Certificate at the time of purchase of any dog or cat. A responsible breeder, shelter, or rescue organization will provide registration and veterinary health records.

According to the Pet Law, the animal should be examined by a licensed and accredited veterinarian no more than 30 days prior to the sale of the pet. The Pet Law has specific requirements, like certain vaccines, deworming, and a fecal check to look for intestinal parasites, that veterinarians must comply with prior to issuing the Health Certificate. Under certain conditions, it provides buyers with recourses if it is determined that the pet was unfit for sale at the time of purchase.

While the vast majority of pet breeders are legitimate, it can sometimes be difficult to spot a fraud. If you suspect that you have become a victim, report it immediately. You can file a complaint at FloridaConsumerHelp.com or by calling 1-800-HELP-FLA (435-7352) or 1-800 FL-AYUDA (352-9832) en Español.

Fraudulent Credit Card Alerts

Consumers need to be alert to a recent text scam that advises them a credit card account is restricted and requires that they call to remove the restriction. Upon calling the number provided, scammers make attempts to obtain the following information:

- **Date of Birth**
- **Social Security Number**
- **Mother's Maiden Name**
- **Card Account Number**
- **Expiration Date**
- **3 Digit Security Code**

Credit card companies would not ask for this information when you contact them in response to a text alert. If you receive a suspicious communication about your credit card, you should call the number on the back of your card to verify that it is legitimate.

If you think you may be a victim of a scam or that your personal information was compromised, you can place a fraud alert on your credit bureau by contacting one of the three major credit reporting agencies (Experian: 1-888-397-3742; TransUnion: 1-800-916-8800; Equifax: 1-800-685-1111).

You can also obtain tips on how to prevent scams, information on current scams, and also sign up for scam alerts at the following Federal Trade Commission (FTC) site: www.ftc.gov/scams.

Don't Get Scrooged by a Holiday Scam

Wouldn't it be nice if criminals took a break for the holidays, leaving the rest of us to enjoy our celebrations without the worry of scams and fraud? Unfortunately, they don't slow down at this time of year, and if anything, scammers actually ramp up their activity to take advantage of unsuspecting consumers.

Luckily, you can preserve your holiday cheer and reduce your chances of becoming a victim by learning a few signs of some common scams. Remember, these scams can take on holiday-themed forms at this time of year but can still be a threat all year long.

1. **Secret Sister/Gift Exchange Scam –** You may have already seen social media posts for a secret sister gift exchange, but know this: no matter who posted it or how much fun it claims to be, it's a scam. Even worse, depending on how it manifests and where you live, it may even be illegal to participate.

This one works in a similar vein to a pyramid scheme. You buy six to ten gifts and mail them to other people on the list, and in turn, future participants send you gifts. Your initial handful of gifts is supposed to multiply as the list gets bigger, but too many victims of this scam report that all they got was a hit to their bank accounts when they sent off those first gifts.

2. **Charity Scams –** Thieves take full advantage of our goodwill and generosity, often with sad situations that make us feel grateful to have so much. With the widespread availability of crowdfunding and online posting through social media, it can be very difficult to know who to help and how.Be safe this season by designating your donations before the holidays and choosing reputable organizations whose values align with your own.
3. **Shipping, Fake Retail Scams –** As our holiday shopping gets fully underway, it can be hard to discern genuine retailers and their messages from the phonies. Copycat websites, fake internet storefronts and bogus emailed receipts that trick us into divulging sensitive information are just a few of the tools scammers can use to steal your identity, your money or both.
4. **E-Cards –** There are several reputable websites that offer adorable " e-cards," complete with photo personalization, animated video, and even musical sound effects. Unfortunately, the cards arrive as an email in your inbox telling you to click the link to view it; it takes no tech skill whatsoever to launch a spam email campaign that tricks recipients into downloading a virus instead of a delightful card. Make sure you verify it with the sender before you click any links.
5. **Seasonal Employment –** There's never a time when most of us couldn't use a little extra money, and scammers take advantage of that fact even more at the holidays. Bogus job offers that steal your identifying information, criminal scams that get you to " reship" stolen property and too-good-to-be-true jobs that require you to send in money or access to your bank account are just some of the ways scammers posing as employers can harm you.

This holiday season, arm yourself with information so you won't have to waste time worrying about scams and fraud. Also, do your friends and family a favor: give the gift of awareness by keeping others informed about these scams and more.

"Pass it On" at the Holidays

by Lisa Weintraub Schifferle, Attorney, Division of Consumer & Business Education, Federal Trade Commission

Holidays often mean time with family and friends. If you're looking for conversation starters that avoid tricky topics – like who should've won the World Series – why not chat about scams? *Pass it On*, an FTC education campaign, gives you new ways to talk about scams and how to prevent them.

Sharing **what** you know can protect someone **who** you know from a scam. That's why the FTC created Pass it On – articles, presentations, bookmarks, activities and videos – to get you talking about scams. Now, *Pass it On* has an updated website with four new topics. Here's a glimpse:

Maybe your retired aunt is looking for ways to make extra money and saw ads promising big money working at home – for a fee. Remind her to check out the company first and share this advice about work-at-home scams: don't pay money to earn money.

Commiserating about leaky roofs, old windows, or repairing a home after storm damage? Be sure to discuss home repairs scams. Before starting repairs, get three written estimates and proof of license and insurance.

If you want folks to kvetch about something other than why kids don't eat their vegetables, bring up unwanted calls. We all get them, and many are from scammers. Remind people to just hang up and don't trust caller ID. It can be faked. Ask your carrier about call blocking – or consider buying a call blocking device as a holiday gift.

Or maybe you prefer a little friendly competition? Quiz your friends and family about what a money mule is. Not sure yourself? Read more about money mule scams. The short answer is: when someone sends you money and asks you to send it on to someone else, you could be what law enforcement calls a money mule. Don't do it. You could lose money and get into legal trouble.

This year, when you pass the turkey, pass on your knowledge about scams. And if you know someone who's alone this holiday season, reach out to them too. You'll probably brighten their day and may even help prevent a scam.

FTC's Tips for Happy Holiday Shopping

by Gretchen Abraham, Division of Consumer & Business Education, Federal Trade Commission

Keep your holiday shopping merry and bright with an early gift from the Federal Trade Commission: tips to help you watch your wallet, shop wisely, and protect your personal information.

- **Make a list and a budget.** Those impulse purchases (looking at you, cozy sweater) are less tempting when you have a game plan. Consider how much you're willing to put on your credit card, and how long it might take to pay it off. If money's tight, paying for a gift over time through layaway might help.
- **Do your research.** Read reviews and recommendations about the product, seller, and warranties from sources you trust. If you're shopping online, check for reports that items were never delivered or not as advertised. Spreading holiday cheer by donating to charityor a crowdfunding cause? Look into it first to make sure it's legitimate.
- **Look for the best deals.** Check out websites that compare prices for items online and at your local stores. Remember there may be shipping costs for online orders. Look for coupon codes by searching the store's name with terms like "coupons," "discounts," or "free shipping." To save extra money, keep an eye out for rebates.
- **Keep track of your purchases.** Make sure the scanned price is right, and save all your receipts. If you shop online, keep copies of your order number, the refund and return policies, and shipping costs. Then have your packages delivered to a secure location or pick them up at a local store. Treat gift cards like cash and keep them in safe place.
- **Give gifts, not personal information.** Protect yourself online by shopping only on secure websites with an "https" address. Stick to shopping apps that tell you what they do with your data and how they keep it secure. Avoid holiday offers that ask you to give financial information – no matter how tempting. They might be trying to steal your identity.

For even more timely tips, sign up for free consumer alerts from the FTC at ftc.gov/subscribe.

E-Skimming for the Holidays

E-skimming happens when a hacker inserts malicious credential-stealing software into a retailer's website. While you are checking out with your credit card or debit card, the hacker is stealing your payment information from the shopping cart in real-time. They may even be using your card or selling the information on the dark web before you are done with the transaction.

Here are some things you can do to protect yourself from e-skimming:

- **Enable alerts on your cards -** "Card Not Present" transaction alerts are a good idea anyway, and they are one of your best defenses against e-skimming. This alert, usually sent

by text or email, comes from your card issuer and lets you know anytime your card is used to make a number-only purchase. As soon as the transaction is processed, the alert is issued. You can contact your bank immediately and stop the payment from going through, as well as close that card and order a new one.

- **Monitor your account -** It is important that all consumers take a routine peek at their bank and card accounts in order to make sure there is nothing suspicious going on. Your card may be used or sold by a hacker, and there can be a limited window of time for you to dispute any charges in order to avoid accepting responsibility for them.
- **Use trusted websites and look for HTPPS -** Hackers have a fun game of seeing who can earn the most credibility by taking down bigger and bigger targets. However, the more trusted and secure the retailer, the more likely they are to have strong security protocols in place. Avoid sites you are not familiar with, no matter how great the advertised deals are.
- **Consider a low-limit card for online purchases -** Especially with holiday shoppingcoming up, you might consider a low-limit credit card for use on the internet. It can help reduce the amount of damage a hacker can do if your card information is stolen online.
- **Pre-plan your holiday shopping -** If you are doing a lot of online shopping in the next few weeks, it is a good idea to plan what you will be buying and from which retailers. First, it will help you stick to your holiday budget, but more importantly, you will not be lured into opening dozens of online accounts and spreading your spending around. Limiting where you shop can help reduce your risk of encountering an e-skimmer.

If you think you have been a victim of identity theft, contact the Identity Theft Resource Centerfor toll-free, no-cost assistance at 888.400.5530. For on-the-go assistance, check out the free ID Theft Help App from ITRC.

Click to View Food Recalls

The Division of Food Safety monitors food from the point of manufacturing and distribution through wholesale and retail sales to ensure the public of safe, wholesome and properly represented food products.

Click to View Consumer Product Recalls

The Consumer Product Safety Commission provides consumer product recall information as part of the agency's mission to protect consumers and families from hazardous products.

The Florida Department of Agriculture and Consumer Services is the state's clearinghouse for consumer complaints, protection, and information. Consumers who believe fraud has taken place can contact the department's consumer protection and information hotline by calling 1-800-HELP-FLA (435-7352) or, for Spanish speakers, 1-800-FL-AYUDA (352-9832) or visit us online at FloridaConsumerHelp.com.

Follow us on Twitter -- @FDACS and @NikkiFriedFL

Florida Department of Agriculture and Consumer Services
Nicole "Nikki" Fried, Commissioner

You are subscribed to the Florida Consumer E-Newsletter. To change your email preferences, please point your browser to: http://www.freshfromflorida.com/Divisions-Offices/Consumer-Services/Consumer-E-Newsletter

Please do not reply to this message. It was generated from an account that isn't monitored, so replies to this email will not be read. You're welcome to get in touch with us through the Contact Us page of our website at www.FloridaConsumerHelp.com.

FDACS-P-00030 Rev. 12/19