FLORIDA CONSUMER
NEWSLETTER
December 2025
A publication of the Florida Department of Agriculture and Consumer Services

'TIS THE SEASON . . . FOR SCAMS

The holiday season is here! We're talking about holiday parties, spending time with family and friends, giving and getting gifts, and taking in all the holiday decorations. Although it is a time for celebration and joy, don't forget to stay vigilant when it comes to scams. With minimal effort, you can steer clear of falling victim to one of these holiday scams.

The Better Business Bureau (BBB) has gathered the following list of top holiday scams and how to avoid them.

1. **Deceptive advertisements on social media:**
   You frequently get product ads on your social media feed and some look very enticing. However, research the company/product prior to buying! BBB states that people have reported items that never show up despite prompt payment or getting fakes or items that in no way match the description of what was advertised. Others have been billed for that "free" trial to which they never agreed. The 2024 BBB Scam Tracker Risk Report indicates online purchases were the fourth chanciest scam reported by consumers.
   TIP: Before ordering, check out the business profile and online reviews on independent websites.

2. **Holiday apps:**
   Google Play and the Apple App Store have hundreds of holiday-themed apps where excited kids can live video chat with Santa, light the menorah, see Santa feed real reindeer, track the sleigh on Christmas Eve, or read him their wish lists.
   TIP: Watch out for free apps – most contain more advertising than other apps that charge a small fee AND can contain malware. Check the privacy policies closely to determine what information will be collected, and always read the reviews.

3. **Social media gift exchanges:**
   Have you heard of "Secret Sister" or "Secret Santa Dog" gift exchanges? If not, you have likely heard of this scheme where you provide your email address, promising to send a gift to another on the list, forward to their family and friends to do the same, and others will be doing the same for you. The problem with this is, anyone who participates has shared their personal information with the trickster and sent him a gift, and everyone involved has broken the law for participating in a pyramid scheme.
   TIP: Only buy gifts from trusted retailers for those who are near and dear.

4. **Free gift cards:**
   We all like "FREE." However, sometimes "free" comes with more than we want. Scammers take advantage of the excitement over the possibility of free by sending phishing emails, creating pop-up ads, or sending text messages, asking for personal information in exchange for free gift cards.
   TIP: If you have received such an email, mark it as spam or junk and delete it. Delete any similar unsolicited texts, too.

5. **Speaking of gift cards:**
   If you are contacted by a government agency, business, or other entity offering you anything in exchange for a gift card, it is a scam. No legitimate business will have you buy a gift card to pay them. The requests may come as a phone call, email, text, or social media message, and some will indicate it is urgent. The instructions may include a specific store for obtaining the gift card. All instructions, however, will direct you to provide the gift card number and PIN, either verbally or with a photo.
   TIP: If you have any doubts about whether or not it is a scam, ask yourself, "Is this someone I trust?" If not, it's a scam. When purchasing a gift card for a real gift, always keep a copy of the card and store receipt to report any scams to the gift card company and request your money be returned.

6. **Fake charities:**
   The holidays are a time for charitable donations but be wary of fraudulent charities and scammers. Avoid spontaneous donations to unfamiliar organizations. Trustworthy organizations will welcome your donations tomorrow as much as they do today.
   TIP: Verify charities are registered in Florida at Check-A-Charity. If possible, make donations through the charity's website using your credit card.

7. **Pet scams:**
   If you are thinking of adding a four-legged member to the family this holiday, watch out for scams. According to the Better Business Bureau, up to 80% of online pet ads are bogus.
   TIP: Before making the decision to purchase, be sure to see the animal in person.

TAKE CARE WHEN SHOPPING ONLINE

In what may be the busiest time of year for some, shopping online can certainly make our lives easier. Rather than going store to store, perusing the shelves or racks, you can choose the perfect gift with just a few clicks. Sometimes you know just what you are looking for and where to find it, but other times you see an advertisement on social media or get an email, and the product is just one link away. Before you click that link, consider if the website is legitimate.

- **Assess the address bar.** Scammers will often use a URL that is close to a legitimate retailer's URL, but not quite the same. Does the address begin with "https?" The "s" indicates secure, and if you see it, it indicates the website's protocol is safe. Look for a padlock icon in the address bar. When you click on that icon you should see site information, such as a valid SSL, the cookies in use, and if your information is safe when sent to the site.

- **Weigh the website.** Does the website use proper grammar and spelling? Is there a contact page with a valid phone number and physical address? What about the website's privacy policy? If you answered "no" to any of these, it may not be legit.

- **Ponder the purchase.** Before making a purchase on a website with which you are unfamiliar, look into the company. Check out reviews on other sites for reviews of the company and reports of scams or trust ratings.

- **Decline the deal.** If you find a cheaper-than-dirt deal that cannot possibly be true, it's probably not. Check shipping and handling costs, delivery fees, etc. If you see any red flags, it is likely a scam.

- **Resist the impulse buy.** Again, research is key. Advertisers, legitimate and scam, have the ability to track your purchasing behaviors from social media ads and will tailor the ads you see. Do not act on a whim – always research the company and product before you buy to avert the scammers.

- **Consider the card.** Credit card companies allow disputes of fraudulent charges, which you may not be able to do if you purchase an item with a debit or gift card. If asked to pay by a prepaid gift card or a digital wallet app, such as Zelle, Venmo, or PayPal, it might be a scam.

FCC CONSUMER ALERT

The FCC recently released the following consumer alert regarding scammers offering discount cable and streaming services.

FCC Alert: Scammers Offering Discounted Cable and Streaming Services

Consumers are reporting robocalls and voicemails claiming a "50% discount on your monthly bill is set to expire" and urging them to call back immediately.

The Federal Communications Commission is alerting consumers about scam calls and texts claiming to offer 50% off of Comcast, Spectrum, or Prime bills. Consumers are reporting robocalls and voicemails claiming. For example, a caller stated:
"Hello. This is Comcast Xfinity. We're reviewing your account, and it appears your 50
percent discount on your monthly bill is set to expire today. To confirm and secure your
savings, call the number displayed on your caller ID immediately. This offer cannot be
extended. Thank you."

Complaints filed with the FCC report that consumers who do call the number back are often encouraged to act quickly to ensure they keep the "discount." The scammer will also claim the only way to secure the discount is to prepay for multiple months of service using a gift card. Pressure to act quickly and only accepting gift cards as payment are sure signs of scam.

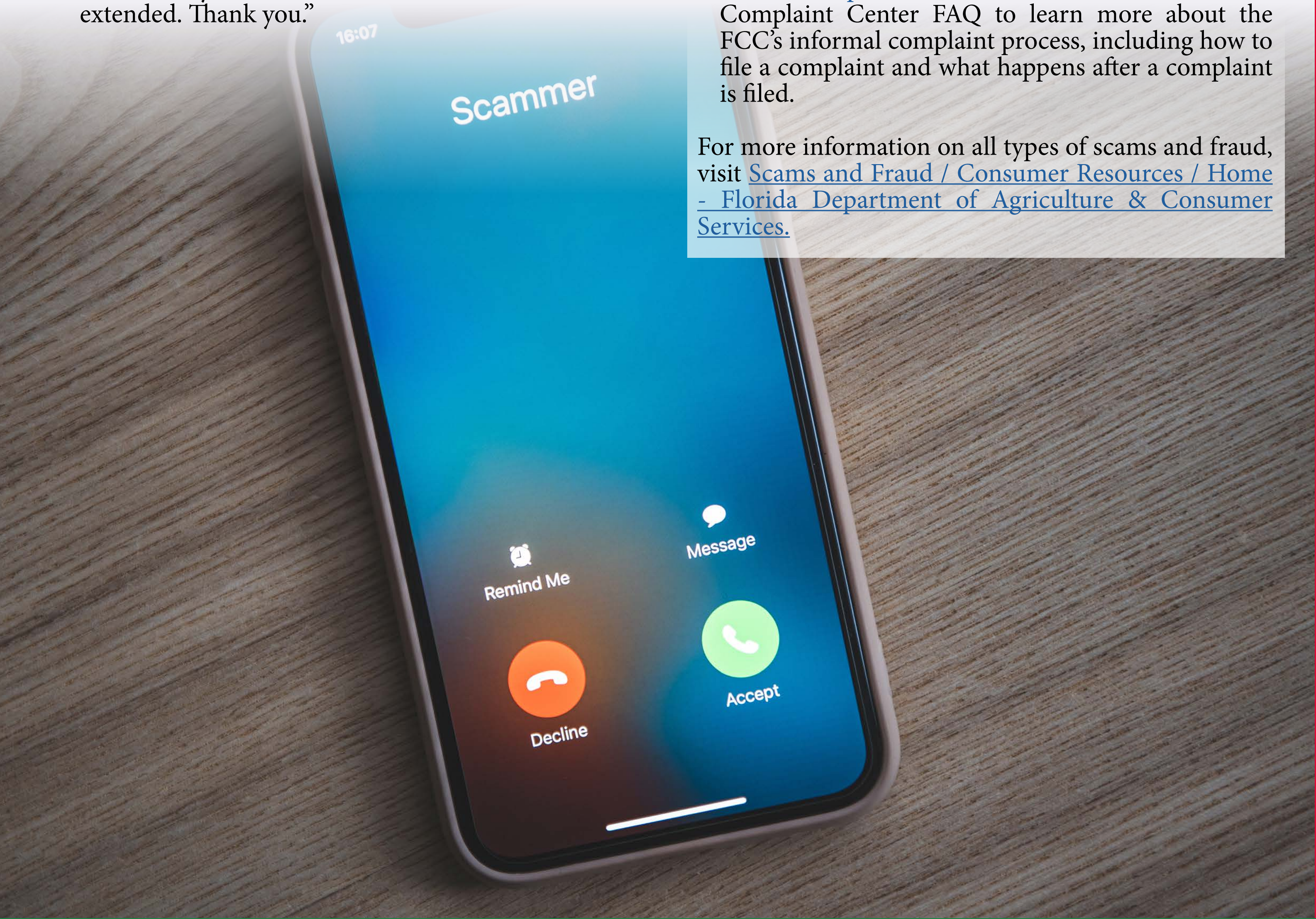
If you have questions about your cable bill or streaming subscriptions and discounts, call or email your service provider at the official customer service number or email address listed on your bill. Many services also offer the chance to chat with customer service on their official website or in your account portal.

What to Do if You've Been Scammed

If you think you're the victim of a scam, you should:

- Report it to local law enforcement as soon as possible.
- Contact the gift card company. They may be able to help you recover your money.
- File a complaint with the FCC. Read the FCC Complaint Center FAQ to learn more about the FCC's informal complaint process, including how to file a complaint and what happens after a complaint is filed.

For more information on all types of scams and fraud, visit Scams and Fraud / Consumer Resources / Home - Florida Department of Agriculture & Consumer Services.



FLORIDA'S PET LEMON LAW

If your family is considering adding a new furry member, knowing your rights before making the purchase may provide some relief in case something goes wrong.

The Florida Pet Law, Section 828.29, Florida Statutes, provides standardized health requirements for dogs and cats sold within Florida. Pet dealers are prohibited from deliberately misrepresenting the health of any dog or cat within the state. Florida law defines a pet dealer as anyone who sells more than two litters or 20 dogs or cats to the public per year. The Florida Pet Law is not applicable to hobby breeders, county or municipal animal control facilities, or registered nonprofit humane organizations.

Pet dealers are required by the law to provide the consumer with a written notice which details the purchaser's rights, along with an official certificate of veterinary inspection, attesting to the breed, sex, age, color, and health record of the pet, including a list of vaccines. If the dealer is unfamiliar with this requirement or refuses to provide either document, be cautious.

Upon purchase of the pet, the law provides new owners with specific time periods within which certain actions must be completed. Any contagious or infectious diseases must be documented by a veterinarian within 14 days; congenital or hereditary defects, or misrepresentations as to the breed, sex, age or color, must be documented within one year. Upon knowledge of any of the above, the consumer has two days to notify the dealer of the findings, and three days to provide the written documentation.

Upon notification, the consumer is afforded three options:

- The consumer may return the pet to the dealer for a full refund and reimbursement of veterinary costs.
- The consumer may exchange the pet for another of equal value and be reimbursed for veterinary costs.
- The consumer may choose to keep the pet, and the dealer will be responsible for reasonable veterinary costs to treat or cure the animal.

Issues concerning the health certificate should be directed to the Florida Department of Agriculture and Consumer Services at (850) 410-0950.

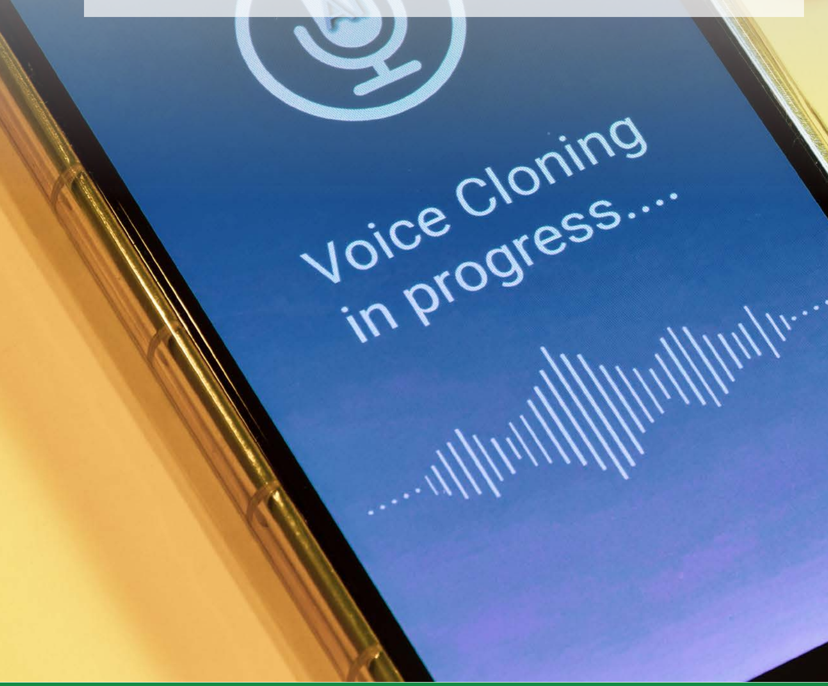
AI VOICE CLONING

Last month, we discussed the rising use of artificial intelligence, or AI. There are numerous ways AI is utilized in daily life, like voice assistants (think Alexa or Siri), music or movie recommendations on your streaming service, or customer service chatbots; the list in both our personal lives and industry is expanding daily. However, as with any new technology, it has been adapted for use in scams. This month, we are going to look in detail at AI voice cloning scams.

AI-enabled voice cloning tools are being used maliciously to mimic voices, then defraud victims. Some of the various tactics utilized are as follows:

- **CEO fraud** – The CEO of your company contacts you with an urgent request: he (or she) needs to pay for a company order immediately. Unfortunately, the CEO does not have their purchasing card available. They want you to use your personal account and wire money to complete the transaction and you will be reimbursed by the company. What would you do?
- **Grandparent scam** – Your grandchild calls you and asks for help. He is in trouble and needs money wired immediately or the situation could get much worse. How do you say no?
- **Government and law enforcement impersonation** – The IRS has just contacted you to say that your most recent tax return was erroneous, but you can avoid an audit, penalties and jail time by paying the difference by wire transfer over the phone. Should you agree?

Each of these scams likely have multiple red flags in common. Here are things that you should look for if faced with a similar situation.



- Unusual contact information. You probably do not recognize the number from which the call is placed.
- There is an urgency to the call, and the caller is not deterred by your questions, insisting you must send the funds NOW without consulting others or verifying their request.
- Emotional manipulation. The caller uses your emotions to elicit a response from you. The CEO may tell you that your actions will result in a big promotion, your grandchild may cry and plead, and the government employee may threaten you with legal action.
- Unusual payment methods. The caller requests gift cards, wire transfers or cryptocurrency.
- Lack or normal human sounds. The caller's voice is flat and has no variation in tone, or the cadence is off. There are no filler noises like a sigh or clearing of the throat.
- Lack of, or odd, background noises. There may be no background noise you would normally hear, like others talking or traffic, or the noise may be strange, like an electronic echo.
- Repetition. No matter what you say, the caller repeats the same or similar phrases.

How can you protect yourself if the scammers are using a familiar voice and emotional tactics to take advantage? You can protect your financial security with just a few easy steps.

- Minimize the publicly available content online. If there is very little voice content online, it is harder for the scammer to procure samples to clone your voice, and those of your loved ones and colleagues.
- Always verify. Create a family safe word to use in such situations. If the caller is unable to furnish it, it's probably a scam. Companies should employ a rigorous verification process that would ferret out any such activities, with mandatory employee training. Consult a trusted individual for advice.
- Ask questions. If the call is from a strange number, yet the caller is known to you, ask the caller a question that only he or she would know the answer to.
- See it in writing. For the government or law enforcement impersonators, ask to see it all in writing. No government agency will force you to make a payment by phone, and definitely not with a gift card.

Although these scenarios sound unsettling, if you remain calm, look for the clues and take a few extra steps with security, you can avoid becoming a victim.

Next month, we will continue the series on AI scams and how to avoid them.

THE NEW SCAM – GHOST TAPPING

When your arms are full of holiday shopping purchases, isn't it convenient when you can just tap your credit card to pay? Although it is convenient, it is also the target of a new scam. Learn how to keep your credit card safe from ghost tapping.

The Better Business Bureau (BBB) recently issued an alert for a new scam – ghost tapping. The new scam involves tap-to-pay cards and mobile wallets. Tap-to-pay technology uses Near Field Communication (NFC), allowing devices to swap data at very close range. While NFC is largely safe, scammers can exploit it, especially in crowds or distracting situations (like holiday shopping).

Ghost tapping does not need the physical contact required with previous debit and credit card scams. The scammers only need a scanning device and to be in close range to you. Be aware of the following situations:

- Close contact in public places: Scammers may try to "accidentally" bump into you and secretly charge your tap-enabled credit card or mobile wallet.
- Fake merchants: At various fairs, markets or festivals, scammers may pose as vendors and specify tap payments, charging you much more than the trifling items they're selling.
- Charity fraud: Scammers might ask for a small donation but then charge your card for much more.
- Rushing a purchase: Especially during the holiday season, scammers are expecting you to be inattentive, tapping your card without checking the business name or transaction amount.
- Starting small. In some instances, small withdrawals are made to sidestep fraud detection systems, which means you may not immediately notice the theft.

What signs could indicate ghost tapping? Your bank may notify you of small "test" charges that seem odd, or you notice suspicious charges after being in crowded situations or attending a public event. Also be leery of vendors who request you tap without showing you a total or providing a receipt.

Follow these tips to protect yourself from falling prey to ghost tapping.

- Use an RFID-blocking wallet or sleeve to stop wireless skimming.
- Before tapping your card, confirm the name of the merchant and amount of the total on the payment screen.
- Contact your bank about enacting transaction alerts for your account.
- Check your accounts often for unusual activity or transactions you do not recognize.
- Consider swiping or inserting your card in high risk areas, rather than tapping.

ABOUT THE FDACS DIVISION OF CONSUMER SERVICES

FDACS is Florida's state consumer protection agency responsible for regulating charities and handling consumer complaints. FDACS handles more than 400,000 consumer complaints and inquiries, oversees more than 500,000 regulated devices, entities, and products like gas pumps and grocery scales, performs over 61,000 lab analyses on products like gasoline and brake fluid, performs nearly 9,000 fair ride inspections, and returned over $2.8 million to consumers through mediations with businesses.

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 THE ICON ABOVE TO SEE THE LATEST RECALLS, MARKET WITHDRAWALS, & SAFETY ALERTS.

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.

CLICK THE ICON ABOVE TO SEE THE LATEST RECALLS, MARKET WITHDRAWALS, & SAFETY ALERTS.

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