FLORIDA CONSUMER
NEWSLETTER
July 2026
A publication of the Florida Department of Agriculture and Consumer Services

DISASTER PREPAREDNESS WITH PETS

The only way to reduce the devastation of a disaster is to be prepared. The more you prepare, the better your chances of reducing suffering and risk for yourself, your family, your animals, and your community. If you live in Florida, you must plan for disasters, such as hurricanes, and that planning should include your pets. Any disaster that threatens humans threatens animals as well.

Why Pet Owners Must Have a Plan

Frightened animals quickly slip out open doors, broken windows, or other damaged areas of your home opened by the storm. Released pets are likely to die from exposure, starvation, predators, contaminated food and water, or on the road where they can also endanger others. Even normally friendly animals of different species should not be allowed together unattended since the stress of the storm may cause distinct behavior changes. REMEMBER: If you must evacuate, then conditions are not only unsafe for you, but they are also unsafe for other living creatures.

Develop A Plan

If you are planning to evacuate to a temporary shelter, some shelters will allow pets to accompany their owners. Please contact the temporary shelter in your area to find out their rules and limitations.

If they are unable to house both you and your pets, arrange shelter for your pets at a veterinarian or kennel close to your evacuation location so that you will have as much contact with them as possible. You and your pets will fare better if you are together. If you plan to shelter your pets at a kennel or clinic, call before evacuating to determine if space is available. Allow sufficient time to travel from the kennel to your evacuation location after making certain that your animals are secure.

If you plan to go to a hotel, determine in advance whether pets are welcome and what, if any, special rules are applicable. Find pet-friendly hotels, restaurants, and more using these resources:

- Pets Welcome - A pet-friendly road trip planner.
- BringFido - Book pet-friendly hotels and vacation rentals.
- Trip With Pets - Pet-friendly hotels and accommodations.

If You Must Evacuate

LEAVE EARLY! An unnecessary trip is far better than waiting too long and not being able to leave safely. All animals should have secure carriers (or collapsible cages for large dogs) as well as collars, leashes, and rabies tags. Carriers should be large enough for the animals to stand comfortably and turn around. Train your pets to become familiar with their carriers ahead of time. The carrier will be a secure and comforting refuge if the animal is required to live in it for days - even weeks - after the storm.

Ensure all your pets have current immunizations and take these records with you if you must evacuate. Photograph each of your pets and include these pictures with your immunization and other medical records.

Your pet survival kit should include:

- Ample food (at least a one-week supply)
- Water/food bowls
- Medications
- Specific care instructions
- Newspapers and plastic trash bags for handling waste
- Brushes, combs, and other hygiene items
- Toys and others comfort items
- Muzzle, if necessary
- Manual can opener, if necessary

Ask your veterinarian for emergency care recommendations.

Throughout the evacuation and the storm, your pets will need reassurance from you. Remain calm, keep as close to their normal routine as possible, and speak to them in a calm, reassuring voice.

If You Can Stay at Home

It is just as important to adequately plan for your pets even if you don't have to evacuate. Carriers, collars with proper ID, and leashes should be maintained for your pets at all times. Your pets will be most comfortable and secured in a safe area of your home until the storm has passed. If they are not secured during the storm and your house is damaged, your pets may escape and become disoriented, since normal landmarks and scent trails could be obliterated. If your pets become lost, proper ID will ensure their return to you. Place your pet food and medication in watertight containers in a cool, dry, dark place. Store adequate water for your pets. Your normal water source may become contaminated. If you bring plants into the home before a storm, be careful not to allow pets access to them since many ornamental plants are poisonous.

After The Storm

Walk your pets on a leash until they become reoriented to their home. USE CAUTION: Downed power lines and other debris pose real dangers to you and your pets. Do not allow pets to consume food or water which may have become contaminated. Be extremely careful in using candles or oil lamps, particularly around pets. Never leave them unattended. When you know that you have done everything you can do to protect all members of the family, disaster preparedness will give you tremendous peace of mind.

Summary Of Key Considerations

MAKE SURE ALL PETS ARE WEARING PROPER IDENTIFICATION. If you become separated, it will be their ticket home.

Get your pets inside and under control as soon as a warning is announced. DO NOT LEAVE A DOG TIED OUTSIDE IN HURRICANE WEATHER.

If you evacuate to somewhere other than a public shelter, TAKE YOUR PET. If it is dangerous for you, it is dangerous for your pet.

If you MUST leave your pets behind:

- Ensure they have access to a safe room without windows, but with adequate ventilation (for instance, a bathroom or utility room.)
- Leave enough food for at least three days.
- A sufficient supply of water is critical.
- If your area might be flooded, provide access to elevated spaces or counters.
- Do not leave cats and dogs in the same space - even if they have been friends.

Links to Other Resources

- Humane Society of the United States
- Florida Department of Agriculture and Consumer Services
- Florida Division of Emergency Management
- National Weather Service

References:

Disaster Information

Prepare Your Pets for Disasters | Ready.gov

Be Prepared: Pet Safety in Emergencies | Healthy Pets, Healthy People | CDC

Disaster Preparedness | ASPCA

Could You Spot a Scam Under Pressure? The STOP Rule Can Help.

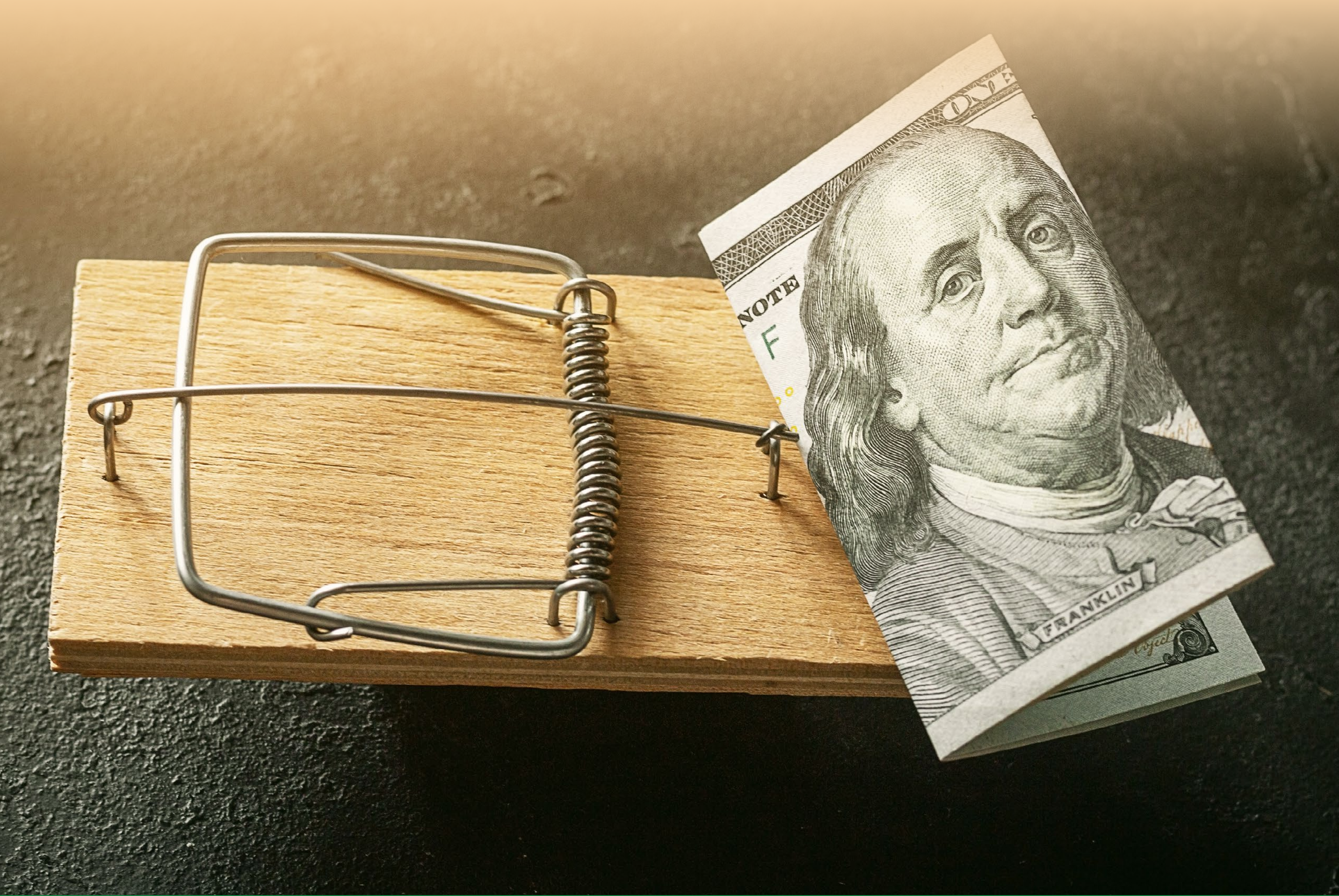
Scammers don't give you extra time to think. And that's intentional. Most scams begin with an unexpected message. It might be a phone call about a missed payment, a text claiming your account was hacked, or an email warning of legal trouble. The details change, but the pattern is consistent: sudden contact paired with a story that demands immediate action. That urgency is meant to trigger an emotional reaction that makes you less likely to question what you're hearing.

When people are startled or worried, the brain's threat response activates, narrowing focus and pushing you toward quick problem solving. In that moment, it becomes harder to slow down, notice inconsistencies, or recognize red flags. It is a temporary cognitive blindness that scammers rely on. This is why they often use phrases like "don't hang up," "act now," or "you will be arrested," hoping to keep you locked inside the emotional moment.

The good news is that you don't have to navigate that pressure on your own. The Federal Trade Commission created a practical worksheet called How I'll Avoid a Scam: My Action Plan that helps you prepare before a scammer ever contacts you. It gives you a place to list trusted people you can call and verified contact numbers for the companies and agencies you do business with.

You can download the FTC's worksheet here: https://consumer.gov/system/files/consumer_gov/pdf/1096A_HowIllAvoidAScam-Worksheet-Fillable.pdf

Pairing this worksheet with a simple decision making guide called the STOP rule can make a stressful moment much easier to manage. The STOP rule outlines what to do when something feels suspicious: Slow Down, Test the Story, Observe Warning Signs, and Protect Your Information and Money. The worksheet gives you the information you need to follow each step effectively.



S – Slow Down

When a message appears urgent or alarming, the most powerful response is to pause. Scammers count on quick reactions because those reactions bypass critical thinking. Slowing down interrupts that pattern and gives your brain time to shift from panic to problem solving. This is where the worksheet becomes useful. Instead of clicking a link or calling a number provided in the message, you can reach for your action plan. Seeing your prepared list reminds you that you don't have to decide anything immediately.

T – Test the Story

Once you've taken that pause, it's time to question the narrative you were given. If someone claims to be from your bank, utility company, credit card company, or another business, don't use the contact information they provided. Use the verified number you wrote on your worksheet which you already know belongs to the real organization. This prevents you from inadvertently contacting the scammer again. The worksheet also includes space for trusted friends, family members, neighbors, or caregivers who can serve as a sounding board. Sometimes simply saying the situation out loud to another person can help you notice that something does not sound right.

O – Observe Warning Signs

As you begin checking the story, look for the classic signs of a scam. Was the message unexpected? Is the caller pushing you to act immediately? Are they insisting that you keep the conversation secret? Are they demanding payment through gift cards, cryptocurrency, wire transfers, or payment apps? Are they asking for personal information like your Social Security number, bank account, or verification codes? Even messages that look professional or include personal details can be fraudulent, especially if they try to create urgency or pressure.

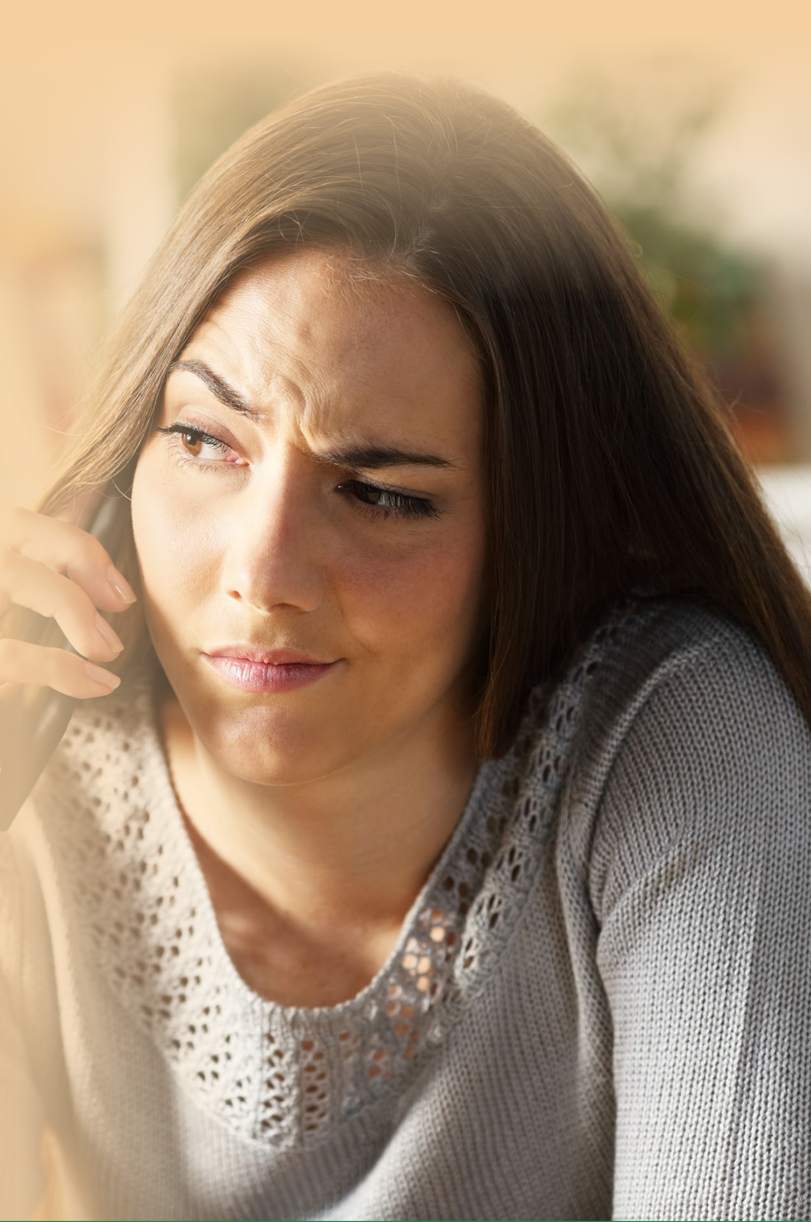
P – Protect Your Information and Money

The final step is to safeguard your personal and financial information. Don't send money or share sensitive details unless you're absolutely sure who you are communicating with. And don't rely on instructions from someone who contacted you unexpectedly. Your worksheet provides a safer alternative: stop the conversation, check your action plan, reach out to someone you trust, and verify the message using a phone number you know is legitimate. For example, if someone claiming to be your utility company threatens to shut off your power unless you pay immediately, hang up. Then use the number on your worksheet, not the number the caller gave you, to confirm whether the story is true.

Build Your Action Plan Before You Need It

Preparation is one of the most effective scam prevention tools. Completing the FTC worksheet allows you to create two important lists: people you trust and companies or agencies you do business with. This can include your bank, credit card companies, utility providers, insurance companies, online retailers, cell phone or internet carriers, or government agencies that scammers commonly impersonate, such as the IRS or Social Security. Once your lists are complete, keep the worksheet somewhere easy to reach: by your phone, saved digitally, or shared with a trusted friend or caregiver.

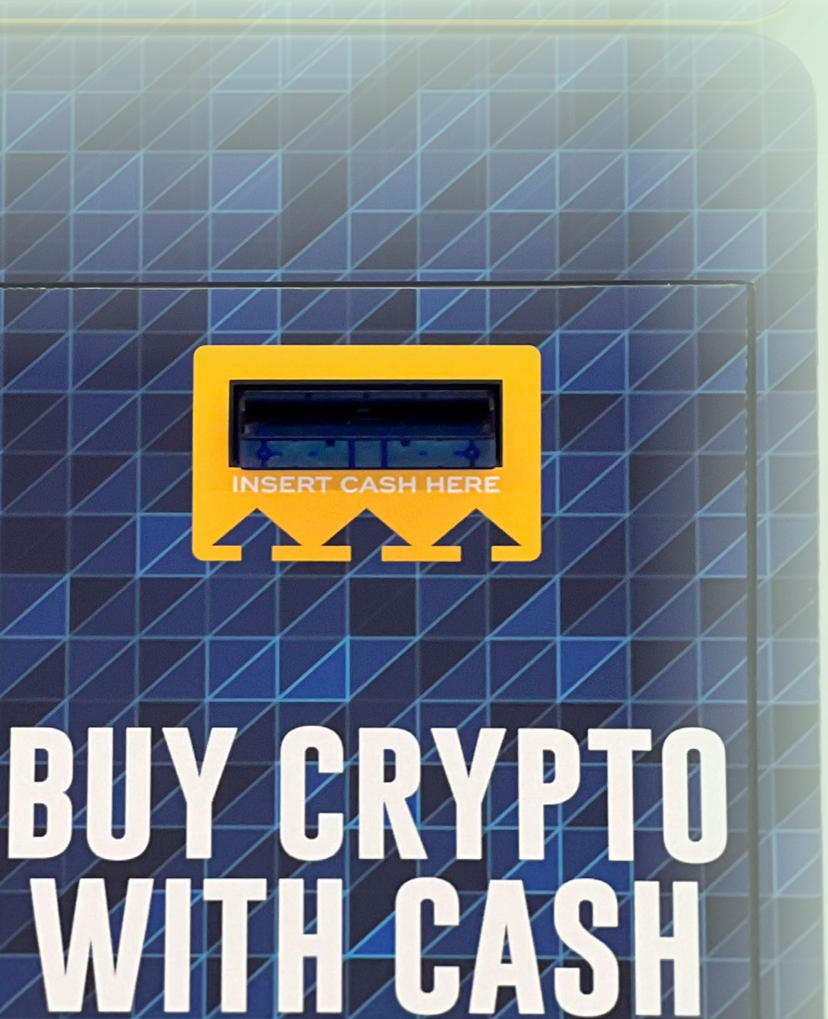
Scammers want you to stay inside the fear of the moment. The STOP rule and the FTC worksheet give you a way out of that moment. Slow down. Test the story. Observe the warning signs. Protect your information and money. A few minutes of verification can prevent a very expensive mistake.



CRYPTOCURRENCY ATMS

Did you know that automatic teller machines (ATMs) have been around since 1969? There are roughly half a million traditional ATMs throughout the United States that allow withdrawals and deposits to our bank accounts. Crypto ATMs have appeared more recently in comparison to traditional ATMs and are sometimes being used by scammers to con honest people out of their money.

A crypto ATM lets you buy or sell cryptocurrency using cash or a debit card. These stand-alone kiosks look like regular bank machines but are not connected to bank accounts. Instead, they allow you to purchase digital currency and send it directly to a crypto wallet you specify. If you are interested in buying crypto, there are an estimated 30,000 machines in the States that can be found in convenience stores, drug stores, and other locations people frequent. However, many states are in the process of attempting to ban crypto ATMs because they are so often used to defraud.



The con starts in a typical "scammy" pattern: a phone call, text or email asking for money for an investment, a family member in trouble, a romantic interest, or even to secure one of your own accounts. The contact seems urgent and claims you have to act immediately to help or invest. The scammer then provides directions to a specific crypto ATM and instructions on how to deposit funds. They may even provide a barcode to direct the deposit (directly into their digital wallet, of course). The machine may or may not display a warning that these transactions are not reversible; regardless, the transaction cannot be reversed and is challenging to trace.

As with many scams, be suspicious of unsolicited contact conveying bank account issues or an emergency involving a family member or loved one. Authenticate any request for funds by contacting the source, such as your bank or family member. Requests for large amounts of cash to be deposited into a crypto ATM should be closely scrutinized. Talk to a trusted friend before acting on such a request. Also, know that using a crypto ATM will not safeguard your money.

When it comes to your money, be cautious, ask questions, and discuss matters with someone you trust before taking any action. If you feel you have been a victim of a scam, contact your local law enforcement agency. For information on other scams and fraud, visit Scams and Fraud - Florida Department of Agriculture & Consumer Services.

References:

https://dfpi.ca.gov/consumers/crypto/crypto-atm-scams/
https://wcfbank.com/beware-of-bitcoin-atms.html
States tighten reins on 'crypto ATMs' | ABA Banking Journal
Tennessee becomes second state to ban cryptocurrency ATMs; KPD says these scams are hard to investigate | wbir.com
How States Are Taking Aim at Combating Crypto ATM Fraud
TN ban on crypto ATMs takes effect July 1; Tennesseans lost $15M in 2025 | WREG.com

PUTTING THE SCREWS TO TAMPERING RUMORS

In early June 2026, headlines began circulating about a new scam at the gas pump – a simple screw. The stories indicated that scammers were installing hidden screws inside the nozzle cradle of gas pumps to keep the pump running after a transaction has been completed. Fortunately, that story has been proven to be unfounded.

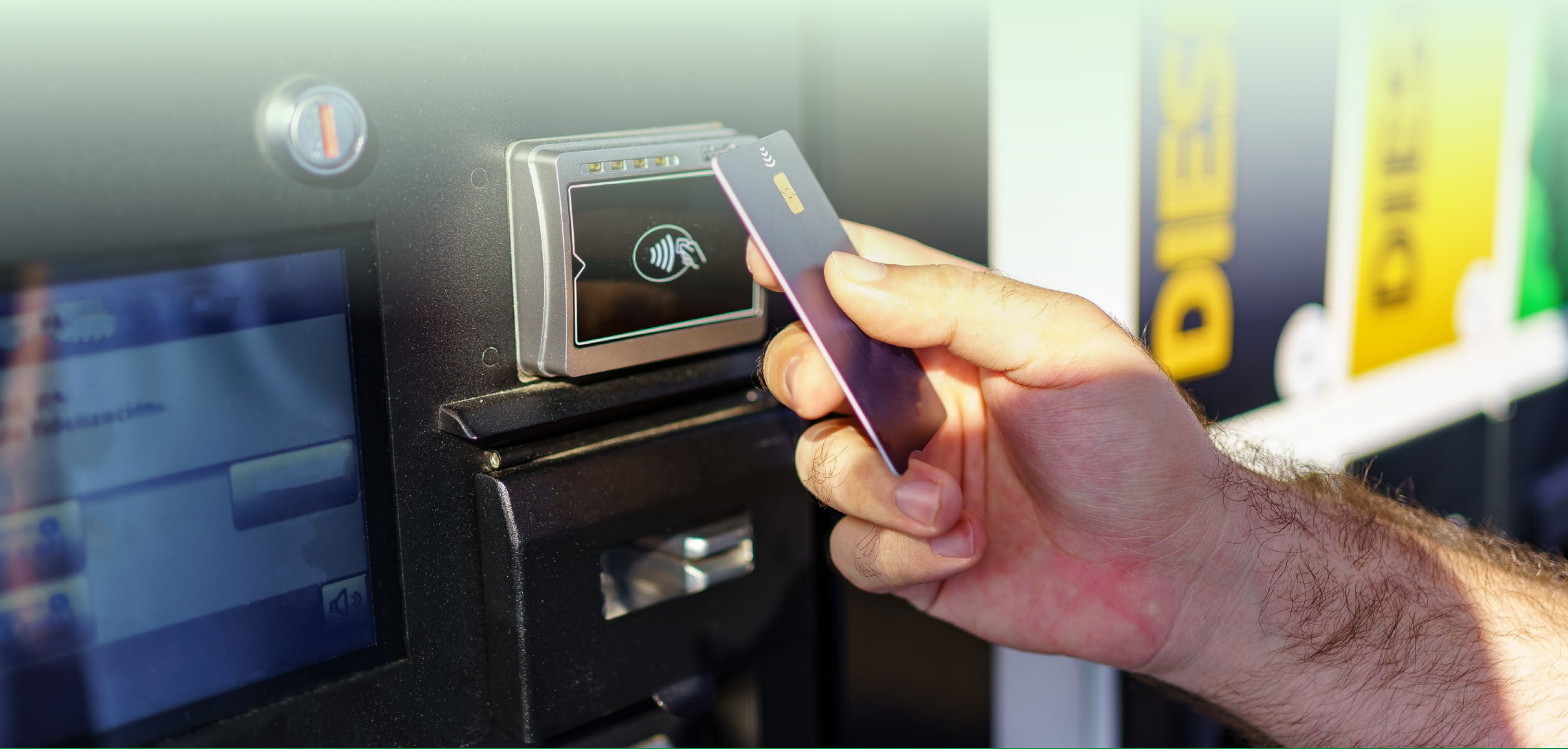
Timberville (Virginia) Police Department originally posted the warning to drivers to beware of the scam but have since removed the post from their social media. This type of scam seems plausible and could be considerably less expensive than installing card skimmers, leading multiple news outlets to report the supposed scam. After multiple reports to various regulatory agencies, it was determined the panic is unsubstantiated. Upon inspection of the complaints, it was found that some station owners may install a screw in a similar manner to correct a malfunctioning dispenser. The makeshift fix is temporary until a technician can properly repair the faulty gas pump.

While the warning itself is unfounded, the tips to avoid fraud at the pump are not without merit. Firstly, be selective in the pump you use. Use a pump within sight of the attendant, as it is less likely to be tampered with than one further away. If a pump appears to have any type of damage or modifications, choose another with no such drawbacks and report the damage to an attendant.

Skimmers are still a real concern at the pump, so monitoring your account closely after making a purchase by card can help protect your money. If your bank offers the option to lock your card when it's not in use, do so and unlock only when you're ready to make a purchase. Also, if you have an option to use a debit or credit transaction, always use credit, as you can dispute a fraudulent transaction much easier. Debit transactions are immediately deducted from your account.

References:

https://www.whsv.com/2026/06/09/gas-pumps-target-new-tampering-scam-consumer-experts-say/
https://www.msn.com/en-us/news/other/criminals-aren-t-using-screws-at-gas-pumps-to-scam-customers-despite-warnings/ar-AA25qMZf?ocid=BingNewsSerp
https://www.yahoo.com/news/us/articles/real-story-behind-viral-gas-151100514.html
https://www.news5cleveland.com/news/local-news/oh-cuyahoga/screwed-at-the-pump-viral-scam-turns-out-not-to-be-true



HOW TO DEAL WITH UNWANTED CALLS AND TEXTS

How to Deal with Unwanted Calls and Texts

You've registered on the Florida Do Not Call list and the National Do Not Call Registry, you don't sign up for random marketing campaigns, and you don't answer your phone if you don't recognize the number. But, if you're like most people, you still get at least one spam robocall or text every day. What can you do to diminish these nuisances?

Mark As Spam

If your phone provides the option to mark a text or call as spam, do it! Your phone learns the number, and blocks or silences future contact attempts, with calls often going straight to voicemail. In most cases, your carrier gets notified as well, labeling the number as a likely source of spam if enough people report it and blocking the number on a wider scale.

To ensure your carrier gets notified, forward spam texts to 7726, which spells "SPAM." Your carrier can analyze the number, content and any suspicious links. The more similar texts are reported, the better it is for everyone, as the carrier can block it across the network.

Forwarding on iPhone

- Long-press the message you want to report.
- Tap "more."
- Tap the forward arrow (a curved arrow) in the bottom-right corner.
- Enter 7726 in the "to" field.
- Press the send button.

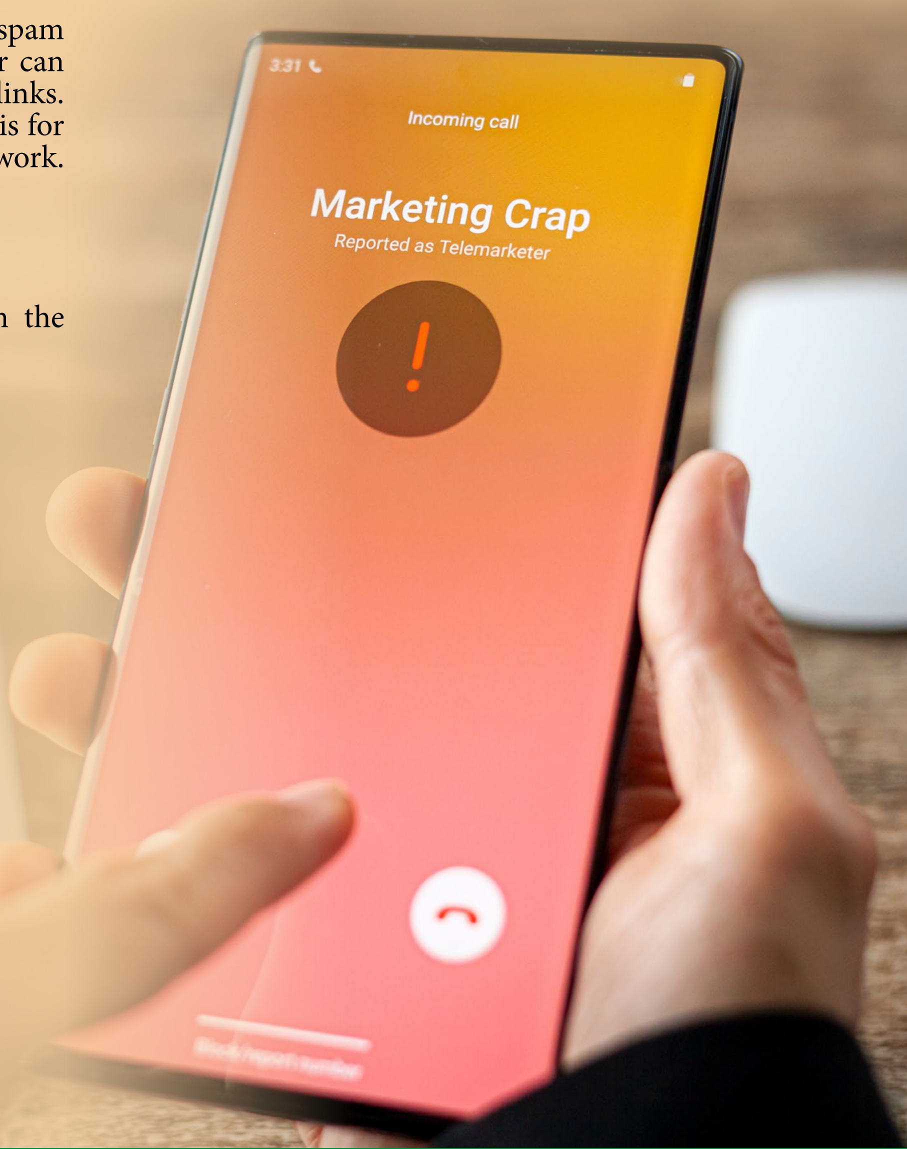
Forwarding on Android

- Tap and hold the message you want to report.
- Tap the three vertical dots in the upper right corner and select "forward."
- Enter 7726 in the recipient field.
- Tap send.

Do not reply to unsolicited texts with "STOP." This lets the originator, likely a scammer, know that your number is real. Your number may be sold to other scammers, and you might get even more texts.

If you continue to receive unwanted phone calls after you have registered, you can file a complaint with the Florida Department of Agriculture and Consumer Services and the Federal Communications Commission.

References:
Stop Unwanted Robocalls and Texts | Federal Communications Commission
Report Spam Messages | Verizon
WHAT THE TECH? What happens when you mark a text or call as spam, and what you should do instead | Local News | local3news.com



DON'T LET A FAKE CAPTCHA TRICK YOU INTO DOWNLOADING MALWARE

Most of us have seen CAPTCHA tests online. They are the small verification prompts that ask you to confirm you're human by clicking "I'm not a robot," selecting images, or completing a simple challenge. CAPTCHAs play an important role in preventing spams, protecting online polls, limiting automated ticket purchases, and enhancing websites' security. But because they are so common, many people don't think twice when one appears on a webpage.

Scammers are now taking advantage of this familiarity by creating fake CAPTCHA screens designed to trick people into following harmful instructions. Instead of asking you to complete a standard challenge, the fake CAPTCHA may tell you to press certain keys, copy and paste text, open a command window, allow notifications, or download something. These steps may appear routine or technical, but they can install malware on your device.

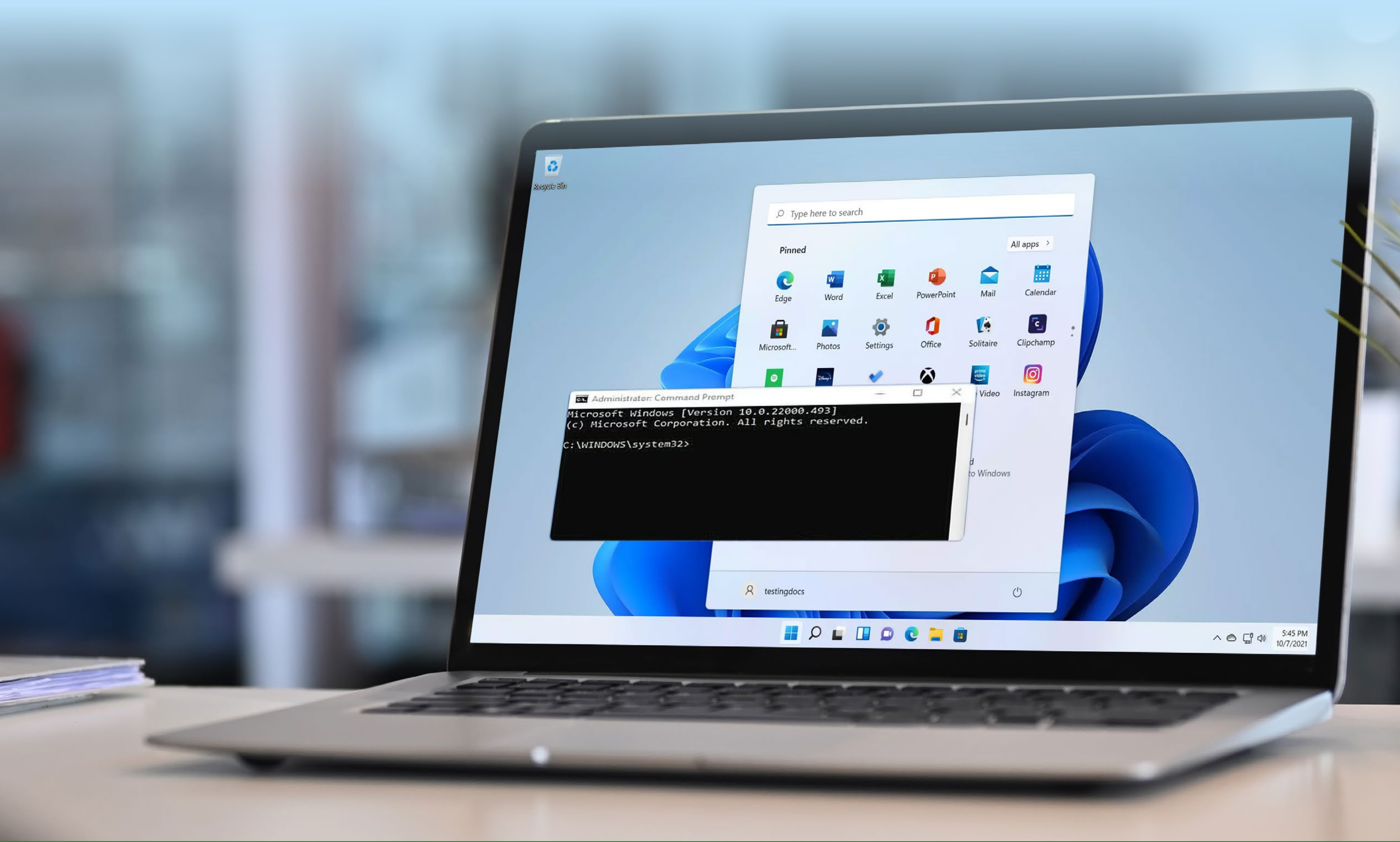
Once malware is on a device, scammers may be able to steal passwords, access online accounts, collect personal information, or monitor your activity.

How the scam works

This scam often starts when someone clicks a link, visits a compromised site, follows an online ad, or attempts to access a file that appears legitimate. Then, a verification screen appears, claiming that a CAPTCHA must be completed to proceed.

The page may look convincing and may use familiar wording like "Verify you are human" or "I'm not a robot." But instead of a typical on screen challenge, the page provides unusual instructions such as:

- Pressing specific key combinations;
- Copying and pasting commands;
- Opening the Run dialog or a terminal window;
- Clicking "Allow" to enable browser notifications;
- Downloading a file, extension, or "update."



These are all red flags. A legitimate CAPTCHA should verify you directly on the webpage. It will never require you to run commands, adjust system settings, download software, or paste unfamiliar text.

What to do if you see a suspicious CAPTCHA

If a CAPTCHA asks you to do anything beyond clicking or selecting images, stop immediately. Close the browser tab or window. If you arrived there through a link in an email, text message, pop up, or ad, avoid clicking it again.

Keeping your device, browser, and security software up to date also helps protect you from these types of scams.

If you already followed the instructions

If you believe you may have interacted with a fake CAPTCHA:

- Disconnect your device from the internet;
- Run a scan using trusted security software;
- Change your passwords from a different, secure device, especially for banking, email, and shopping accounts;
- Turn on multi factor authentication whenever possible;
- Watch your accounts for unusual activity;
- Report the scam to the Federal Trade Commission at ReportFraud.ftc.gov.

The bottom line

CAPTCHAs are meant to confirm you're human, not to make you enter commands, change settings, or install software. When in doubt, remember: **a real CAPTCHA stays on the webpage. If it asks you to do something on your device, it is probably a scam.**

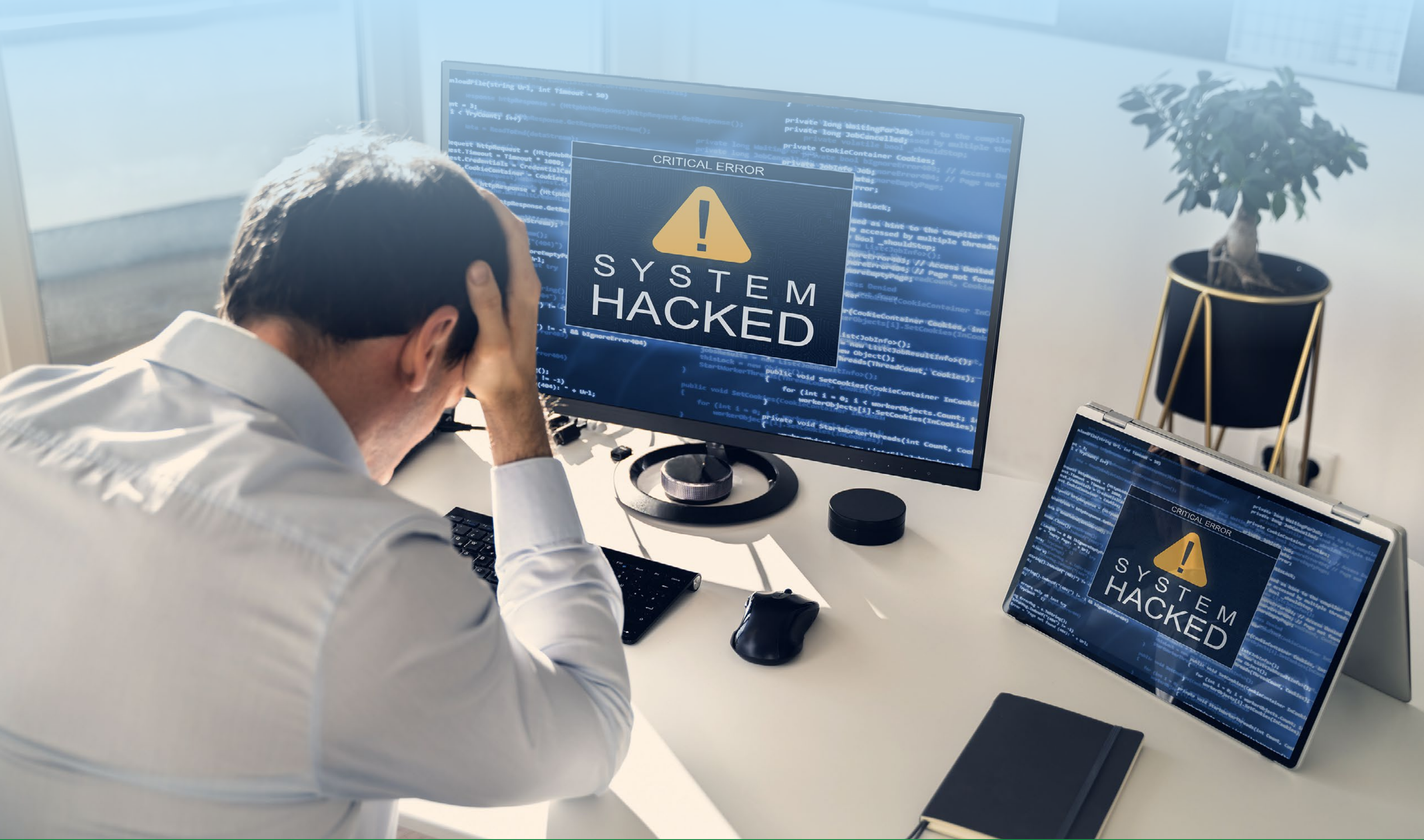
References

Arntz, P. (2025, March 10). Fake CAPTCHA websites hijack your clipboard to install information stealers. Malwarebytes. https://www.malwarebytes.com/blog/news/2025/03/fake-captcha-websites-hijack-your-clipboard-to-install-information-stealers

Federal Trade Commission. (2026, June 8). How to spot a CAPTCHA scam. https://consumer.ftc.gov/consumer-alerts/2026/06/how-spot-captcha-scam

Federal Trade Commission. (2026, March 2). Welcome to NCPW 2026. https://consumer.ftc.gov/consumer-alerts/2026/03/welcome-ncpw-2026

Microsoft Threat Intelligence. (2025, August 21). Think before you Click(Fix): Analyzing the ClickFix social engineering technique. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/



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.

FDACS-P-00030 Rev. 07/2026