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

WATCH OR WARNING?

Knowing the difference between a watch and a warning can help keep you safe. Whether a watch or warning, listen closely to instructions from local officials using a TV, radio, cell phone or other communication device.

Tropical Storm Watch: An announcement that tropical storm conditions (sustained winds of 39 of 73 mph) are possible within the specified area within 48 hours.

Tropical Storm Warning: An announcement that tropical storm conditions (sustained winds of 39 to 73 mph) are expected within the specified area within 36 hours.

Hurricane Watch: An announcement that hurricane conditions (sustained winds of 74 mph or higher) are possible somewhere within the specified area. Because hurricane preparedness activities become difficult once winds reach tropical storm force, the hurricane watch is issued 48 hours in advance of the anticipated onset of tropical storm force winds.

Hurricane Warning: An announcement that hurricane conditions (sustained winds of 74 mph or higher) are expected somewhere within the specified area. Because hurricane preparedness activities become difficult once winds reach tropical storm force, the hurricane warning is issued 36 hours in advance of the anticipated onset of tropical storm force winds.

Tornado Watch: Tornadoes are possible in and near the watch area. Be ready to act quickly if a warning is issued.

Tornado Warning: A tornado has been sighted or indicated by weather radar. Proceed to a safe room immediately.

Flood Watch: A Flood Watch is issued when conditions are favorable for flooding. It does not mean flooding will occur, but it is possible.

Flood Warning: A Flood Warning is issued when flooding is imminent or occurring.

Flash Flood Warning: A Flash Flood Warning is issued when a flash flood is imminent or occurring. If you are in a flood prone area, move immediately to high ground. A flash flood is a sudden, violent flood that can take minutes or hours to develop.

LOOKING FOR AN AMERICAN FLAG THAT'S MADE IN THE USA? HERE'S WHAT TO KNOW!

When it comes to buying an American flag, there are lots to choose from. Not all are Made in the USA. If you're searching for one that is, here's what to look out for.

Imported flags must have labels saying where they're made. So, if you're shopping in a store, check out the product label. Online, you might not find this information, especially if you're shopping for a smaller flag. Instead, look at where the seller's located — look for the address in the website's terms of service or privacy policy. If the store is overseas, there's a good chance its products are not Made in the USA. Also take the time to read reviews. Is the seller reputable? Search online for the seller's name plus terms like "review," "complaint," or "scam." See what other people have to say.

And what if a seller says their American flag "ships from the USA"? That doesn't necessarily mean it was made in the United States. Some stores ship imported products to U.S. distribution centers for storage and processing before sending them to you.

Finally, know that even if you shop carefully, scammers are out there. You might click "buy" and never get your flag. Or maybe a flag shows up, but it's not what you expected. Paying by credit card, if you can, helps protect you if you pay for something and it never comes. And if you think someone is trying to pass a flag off as Made in the USA when it's not, report it to the FTC at ReportFraud.ftc.gov.

For more advice on shopping safely, read Online Shopping.

HOW TO RECOGNIZE A FAKE GEEK SQUAD RENEWAL SCAM

Scammers are at it again, impersonating well-known businesses and trying to rip people off. This time they're pretending to be from Geek Squad, Best Buy's tech support service. Here's what we're hearing about the scam and what to do if you see it.

You get a text message or email that says you were or will be charged hundreds of dollars to renew your Geek Squad membership. If you want to dispute the charge or cancel your membership, the message says you must call a phone number within 24 hours.

If you call the number — which you should not do — the scammer might ask for remote access to your computer. If you give it to them, they can install spyware programs on your computer, steal your online banking credentials, and drain money from your bank account.

Some scammers may ask for your bank account information to refund your money, then fake a transaction and make it look like they accidentally refunded you too much. To pay them back, they tell you to buy gift cards and give them the gift card numbers and PINs.

Scammers send alarming messages like this to rattle you. Don't let them. If you think the message is legitimate, contact the company in question using a phone number you know is real. **Do not use the number included in the message.**

Also check your credit card or bank account for an unauthorized transaction. If you see one, report it to the institution and ask them to reverse it and give you back your money.

Find out what to do if you paid a scammer, or gave them your personal information or access to your computer.

If you see a scam, report it to the FTC at ReportFraud.ftc.gov.

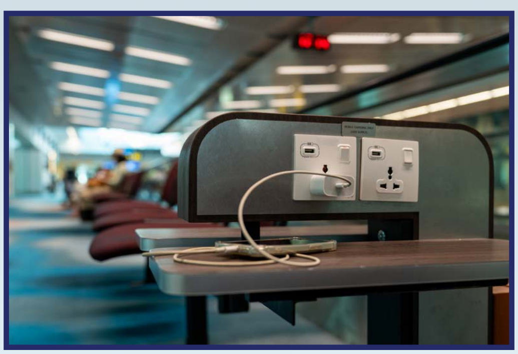
DEVICE SECURITY WHEN TRAVELING

If you are planning to travel soon, you'll likely be taking your cell phone or other portable device, like your tablet, or multiple electronic devices. Even with biometrics, such as fingerprints and facial recognition, and passcodes, passwords, and patterns to keep your information safe, you could still be vulnerable to data or identity theft.

Bluetooth Security

Bluetooth is used to connect your mobile devices to wireless headsets, enable hands-free calling while you drive, and even listen to your favorite playlist in the car. A user must allow a Bluetooth connection before data is shared, (called "pairing") which provides some degree of data security, but does put your personal data at risk. When using Bluetooth, there are a few steps you can take to safeguard your data:

- Turn off Bluetooth when you're not using it. When you keep it active, hackers can discover other devices which have been connected before, then spoof those devices to gain access to your data.
- If you rent a car and pair your mobile device with it, be sure to unpair and clear all personal data when returning the car. Do the same if you are selling a car with Bluetooth.
- To prevent unknown devices from discovering your Bluetooth connection, use Bluetooth in "hidden: mode, not "discoverable" mode.



What Is Juice Jacking?

Those charging stations you find at airports, restaurants and hotel lobbies may be convenient, but you could be opening yourself to cyber theft. This activity is known as "juice jacking."

Public-use USB charging stations could possibly load malware onto your device while charging, giving thieves direct access to your personal data and passwords. That data can then be sold online to other devious criminals or used to access your online accounts.

Public-use USB charging stations could possibly load malware onto your device while charging, giving thieves direct access to your personal data and passwords. That data can then be sold online to other devious criminals or used to access your online accounts.

How can you guard your devices against juice jacking?

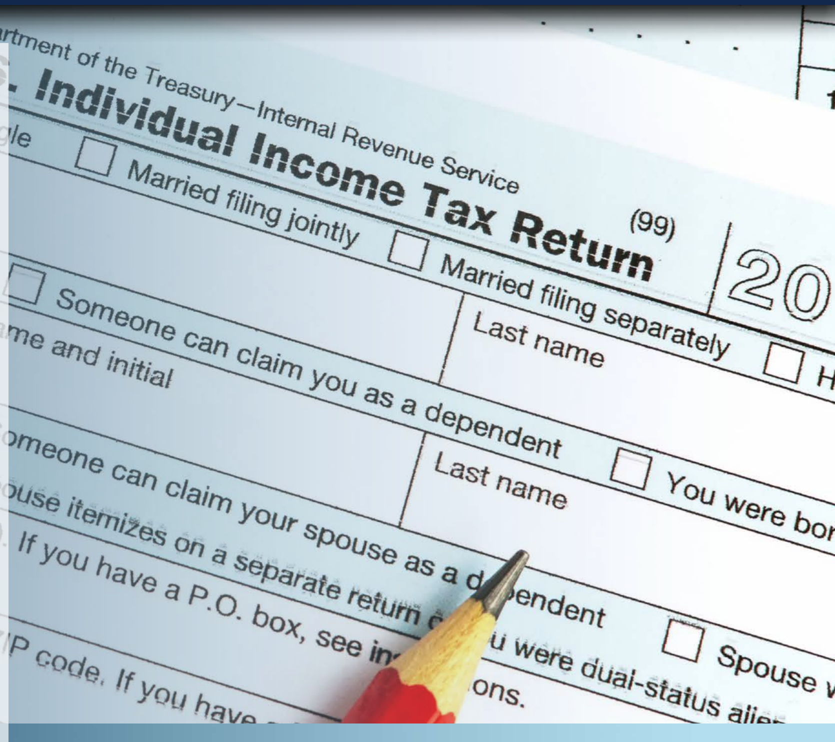
- Use AC power outlets when charging; bring your own charging brick and cords and charge your items using a standard wall outlet.
- Use an external battery. Using an external, rechargeable battery allows you to charge on the go.
- Use a charge-only cable. These cables prevent data from sending or receiving while charging. Make sure you buy from a trusted provider.
- Use caution. When charging your device in a public-use charging station, if you see a prompt asking if you want to "share data" or "trust this computer" or "charge only," make sure to select "charge only."

Public Wi-Fi

If you choose to use public Wi-Fi networks to access the internet when you travel, do so with caution. Hackers can access the connection and gain introduction to data on your device and in your online accounts. You can use the following tips to mitigate the risk:

- Verify the available Wi-Fi hotspots. Check with establishment staff to ensure you are using the correct hotspot, not a fraudster trying to steal your data.
- Look for "https" when sharing data over any network. Websites beginning with "https" encrypt your data when it's transmitted.
- Install a (reputable) app on your device to force web browsers to utilize encryption when connecting to websites.
- Ensure your device does not automatically connect to nearby Wi-Fi networks when in range.
- Use a VPN (virtual private network) if you frequently use public hotspots. VPN encrypts all transmissions between the internet and your device.
- Use your data plan rather than a hotspot when communicating sensitive information over the internet.

PROTECTING YOUR PERSONAL INFORMATION



When it comes to protecting your identity, you might think about keeping usernames to yourself, using strong passwords, and reviewing your statements. That's all great. But it's also important to think about what you do with documents or digital files that contain your financial information. So, let's look at what you should keep and lock up, and what you should shred or delete.

Keep for a Year

- Bank statements
- Pay stubs
- Undisputed medical bills
- Credit card and utility bills
- Deposited checks

If you can access these documents electronically, consider shredding your paper copies.

Keep for at Least Three Years

- Income tax returns
- Tax-related documents, like canceled checks, receipts, W-2s, and 1099s
- Records related to selling a home

In some cases, the IRS recommends keeping tax returns and tax-related documents for longer than three years. If you can access these documents electronically, consider shredding your paper copies.

Keep While You Own

- The title to your vehicle
- The title or deed to your home
- Documents related to mortgage or vehicle loans
- Home improvement receipts
- Rental agreements and leases
- Sales receipts and warranty information for major appliances

Keep Forever

And lock up:

- Birth certificate or adoption papers
- Social Security cards
- Valid passports and citizenship or residency papers
- Marriage licenses and divorce decrees
- Military records
- Wills, living wills, powers of attorney, and retirement and pension plans
- Death certificates of family members
- Vital health records (especially those that pre-date electronic health records)

Shred

- ATM receipts
- Offers of credit or insurance
- Cleared checks (after 14 days)
- Credit reports
- Prescription information for medicines you no longer take
- Expired warranties
- Expired credit cards, driver's licenses, and other forms of identification

When it's time to dispose of documents with your personal or financial information, shred them. If you don't have a shredder, look for a local shred day in your community.
Find out what else you can do to protect yourself from identity theft.

FACEBOOK AND SOCIAL INVESTMENT SCAMS

Facebook parent company Meta was recently urged to curtail the rise of investment scams on Facebook and WhatsApp by a bipartisan coalition of 42 attorneys general throughout the US.

The scam targets Facebook users with ads featuring renowned investors, like Warren Buffett or Elon Musk, who offer the user the opportunity to become a member of an investment chat group through WhatsApp, a Meta-owned messaging app. However, those famous investors are not a part of the chat group and the recommendations to buy penny stocks are from bad actors hoping to profit off the pump-and-dump scheme. The purchase of these stocks increases the value ("pump"), then the instigator sells the securities at an artificially high price ("dump"), which causes the worth to dive.

If you are thinking of investing, remember the following tips:

- Thoroughly research prior to investing. Search the company name or cryptocurrency name online using additional terms like "review," "scam," or "complaint" in the search bar.
- Never give your account information (credit card or bank account) until you look into the investment.
- Be leery of investment proposals on social media platforms.
- Do not trust investment tips or secrets in online messages boards. Linked sites may be bogus websites pushing what appears to be opportunities to invest.
- Avoid pushy sales pitches to "invest now."
- Use caution with celebrity endorsements. Do your research rather than be swayed by a name dropper.
- If someone claims to know a "better way" to invest, don't trust them.

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. 07/2025