FLORIDA CONSUMER
NEWSLETTER

April 2026

A publication of the Florida Department of Agriculture and Consumer Services

WHAT YOU NEED TO KNOW ABOUT CRYPTO

Cryptocurrency (crypto) was first launched publicly in 2009, in the form of Bitcoin. Since that time, more than 25,000 other cryptocurrencies have been introduced, and the form of digital currency continues to garner attention. What exactly is cryptocurrency? How is it used? Read on to find out the basic facts about this digital asset.

What Is It? Cryptocurrency is a virtual currency secured by cryptography (or code) and does not rely upon a central authority, such as a bank, to maintain it. Ownership and transaction records are held in a database format referred to as a block. Records, or blocks, are linked from one to the next with a hash (or unique identifier) to form a chain and distributed across a peer-to-peer network of computers, often public. The linked blocks are called a blockchain. Data within any of the blocks cannot be changed without modifying data in subsequent blocks, which would require permission throughout the network. Since the blockchain is decentralized and open-source, transactions are recorded throughout the network, verifiable in real time and can be audited inexpensively. There is no downtime waiting for a transaction to “clear,” and no fear of counterfeiting.

Is It Physical Currency? Crypto exists in coin or token form. Tokens are intangible assets on a blockchain, while coins may be tangible, virtual or digital. Bitcoin was the first introduced and is the most commonly traded. Other cryptos, referred to as altcoins, are Ethereum, Litecoin, and Solana, among the thousands of others. All of these are categorized by their respective function and technology; there are payment coins for transactions, utility tokens for smart contracts or platform access, and stablecoins which are tied to assets, as well as less used categories like privacy or meme coins.

How Do You Acquire It? Cryptocurrencies can be bought and sold in a cryptocurrency exchange, where you swap physical currency (dollars and cents) for virtual currency units held in a digital wallet. A digital wallet can be hardware, software, or a service which stores your public and private keys for digital transactions. Private keys are used to authorize spending and public keys are used for accepting funds.

What Can You Buy with It? Cryptocurrency payment coins can be used at numerous merchants online to purchase a myriad of goods from home repair items to real estate, including gift cards that can then be used at the designated merchant.

www.FloridaConsumerHelp.com
1-800-HELP-FLA(435-7352) • Mon-Fri, 8a.m. - 5p.m., EST • 1-800-FL-AYUDA(352-9832)

How Is It Backed? Fiat currencies, like the US dollar or euros, are backed by the strength of the economy rather than a physical commodity such as gold. Cryptocurrencies, however, are backed by the security of the blockchain, rarity of the currency, decentralization (or ease of transaction validation) and efficacy.

Is Crypto Taxed? The IRS considers cryptocurrency property, and it is subject to capital gains tax.

Is Crypto Safe? Since it is bought and sold on the internet, crypto comes with the usual risks of online purchases. When purchasing, do your research. Consider security, ease of use, assets held, and fees when selecting an exchange. Weigh your options with digital wallets, too. Hot wallets, which are connected to the internet, may allow faster trading and more convenience, but are more vulnerable to hacking, phishing and malware. Cold wallets, however, store your crypto offline in a physical digital storage device, thereby offering a higher degree of security. Beware of losing the device or damaging it, though, because you could permanently lose your funds stored on it.

Final Thoughts? Deciding on an investment takes careful thought and planning. Investing in cryptocurrencies is no different. Continue to research your options and, based on your findings, you can invest confidently as long as you make wise choices:

1. choose a storage method;
2. research coins before buying;
3. utilize a reputable exchange; and
4. always follow the usual cybersecurity rules.

References

Investopedia (n.d.) Blockchain Facts: What Is It, How It Works, and How It Can Be Used. Retrieved from Blockchain Facts: What Is It, How It Works, and How It Can Be Used

Charles Schwab (2025) What is Cryptocurrency and How Does It Work? Retrieved from What is Cryptocurrency & How Does It Work? (2025) | Charles Schwab

The Motley Fool (2025) What Is Cold Storage in Crypto? Retrieved from What Is Cold Storage in Crypto? | The Motley Fool

Fidelity (2025) How to Store Crypto Safely Retrieved from Is bitcoin safe? | How to safely buy and store cryptocurrencies

SIM SWAPPING: THE SCAM THAT CAN HIJACK YOUR BANK ACCOUNTS

Imagine waking up one morning and discovering that your phone suddenly has no signal. No calls. No texts. No data.

At first, it may seem like a simple service outage or network glitch. However, within hours, your bank accounts, social media profiles, email accounts, and even retirement funds could be taken over by criminals.

Even though your physical phone may still be in your hands, scammers can steal something far more valuable: control of your phone number. This number is often the key to verifying your identity for online banking, payment services, and other accounts.

Quick Fact
According to the FBI Internet Crime Complaint Center, SIM swap scams caused nearly $26 million in reported losses in the United States in 2024, and the number of victims continues to grow each year.

These scams allow criminals to intercept the codes used to access your financial and online accounts.

How the Scam Works
Criminals typically use two methods to gain control of a victim's phone number: SIM swapping and port-out fraud.

SIM Swapping
A SIM card is a small chip inside your phone that stores your account's unique ID and links your number to your mobile account. In a SIM swapping attack, scammers trick the mobile carrier into activating a new SIM card linked to your phone number, effectively transferring your number to a device they control.
Many providers are now switching to embedded SIM cards (eSIMs), which are built directly into the device and cannot be removed. While this technology reduces certain risks, scammers may still attempt to take over accounts by tricking carriers into believing the phone number transfer request came from the legitimate account owner, a process known as social engineering.

Port-Out Scams
A port-out scam happens when a criminal fraudulently transfers your phone number to a different mobile provider. Normally, porting your number is a legitimate process when switching carriers or upgrading devices.

However, scammers can gather personal information about a victim and impersonate them when requesting the transfer. Once completed, the criminal receives all calls and texts meant for the victim, including two-factor authentication (2FA) codes and password reset messages.

With access to these codes, criminals can:
- Access bank accounts and transfer funds
- Apply for credit or loans in the victim's name
- Hijack social media accounts

How to Protect Yourself

1. **Add a Security PIN to Your Mobile Account**
   Most carriers allow customers to place a port-out or SIM transfer PIN. This adds an extra verification step to prevent unauthorized transfers.
2. **Use Authentication Apps Instead of Text Codes**
   Whenever possible, use authentication apps, biometrics, or security tokens instead of SMS verification. These methods are more secure against SIM swapping.
3. **Limit Personal Information Online**
   Scammers often gather details from social media to impersonate victims. Keep personal information private when possible.
4. **Watch for Phishing Messages**
   Do not provide personal information if someone calls, emails, or texts asking for it. If the caller claims to represent a business, hang up and contact the business directly using a trusted phone number.
5. **Stay Vigilant**
   Enable email and text alerts for financial and important accounts. Contact your bank or provider immediately if you notice any suspicious activity.
6. **Act Fast if Your Phone Loses Service**
   Many SIM swap attacks occur late at night while victims are sleeping. If your phone suddenly loses service without explanation:
   - Contact your mobile carrier immediately
   - Notify your financial institutions
   - Use Wi-Fi or a friend's phone to act quickly

Every minute counts, as scammers may attempt to access accounts within hours.

Your phone is no longer just a way to make calls, it is part of your **digital identity**. Protecting your phone number is just as important as protecting your wallet, your passwords, and your financial future.

References

Federal Communications Commission. (n.d.). Cell Phone Fraud. Retrieved from https://www.fcc.gov/consumers/guides/cell-phone-fraud

Federal Communications Commission. (n.d.). Port-Out Fraud Targets Your Private Accounts. Retrieved from https://www.fcc.gov/consumers/guides/port-out-fraud

Federal Bureau of Investigation. (2025). Internet Crime Complaint Center (IC3) 2024 Internet Crime Report. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf

RECLAIMING STOLEN GOODS FROM A PAWN SHOP

Imagine if you experienced a home burglary and items stolen included costly tools and heirloom jewelry. The theft was reported and you provided a detailed description of everything missing. Then you find out some of your property was sold at a local pawn shop. You are relieved that your property has been recovered . . . or has it? Will it all be returned to you? Read on to find out what you have to do to get your property back.

Florida court rulings have held that law enforcement may not recover stolen property from a pawnshop and return it to the owner, as the pawnbroker is allowed the opportunity of a hearing. What does this mean to you, as the owner of the property? There are two options: you may choose to buy your property from the pawnbroker or obtain a court order to have the property returned to you without cost.

The Florida Pawnbroking Act, section 539.001, Florida Statutes, outlines the steps that must be taken in order to recover your stolen items by court order. First, the pawnbroker must be notified of your intent to recover the items. This notice must include:

- the name and address of the pawn shop;
- your full name and contact phone number;
- a complete and accurate description of item(s), including serial numbers, if applicable;
- a copy of the law enforcement agency's report of the theft; and,
- a statement similar to the following:
  The law enforcement agency, (agency name), has determined through the course of a criminal investigation that on the following date, (date of pawn), my stolen personal property was pawned at your business. The control number from the pawn slip is: (control number). My personal property was pawned by (insert first AND last name of seller). I have included a copy of the police report with this notice. I would like the items returned to me AT NO COST.

The notice must be signed and dated by you, the owner of the property, and delivered by hand to be signed and dated by an employee of the pawnshop, or delivered by certified mail, return receipt requested. (You can download a fillable version of the notice here.)

If you have not reached an agreement with the pawnbroker within ten days after receipt of the notice, you will need to petition the court for a hearing, naming the pawnbroker as the defendant and perfecting service, both of which are no cost to you as the court's filing fee and sheriff's service fee are waived by statute.

Should the court find the property should be returned to you, you may recover all costs of the action from the pawnbroker, including any attorney fees.

All pawnshops in Florida are required to apply for and obtain a license each year from the Florida Department of Agriculture and Consumer Services (FDACS). Each pawnshop must maintain a net worth of at least $50,000 or file security in the form of a surety bond, letter of credit, or certificate of deposit in the amount of $10,000. FDACS is authorized to impose penalties of up to $5,000 for noncompliance of the law. For more information about pawnshops, visit our website.

MEDICARE FRAUD

In September 2025, the US Department of Justice (DOJ) announced the indictment of two Florida men charged with defrauding Medicare of $34.8 million. Later, in December, two health care executives were convicted of scamming another $34 million from Medicare Advantage. Following that, a laboratory owner from Lake Worth was convicted of perpetrating a Medicare fraud scheme of $52 million. That's over $120 million in taxpayer funds lost in Florida and that is only what has been discovered. Even more recent headlines reveal hundreds of millions of dollars in false hospice claims have been filed in California. Each of these situations involved billing Medicare for unneeded equipment, prescriptions, tests or services and were discovered only after the loss of millions of dollars. However, there are ways that Medicare enrollees and their caretakers can help to stop this fraud sooner.

The stories above have just come to light in the past six months and are representative of a widespread problem. Medicare fraud costs American taxpayers $60 billion each year and the effects are concerning. Not only does it waste taxpayer dollars, but it may also cause problems for the Medicare enrollees, too. False medical information may result in improper health care or even the denial of services which are needed and deserved.

Following are the ways in which Medicare enrollees or their caretakers can watch for and spot fraud, reporting issues as soon as possible.

- Talk to the doctor. When it comes to treatment and cost, enrollees have the right to understand exactly what costs will be billed to Medicare.
- Keep good records. Document all services received, including dates and the type of services and what condition it was used to treat. Keep any statements provided at appointment, especially if it provides billing codes; if not provided, ask for one.
- Check the mail. Or, better yet, check the online account. Create an account at https://www.medicare.gov/account/login and monitor your account whenever you have an appointment or receive goods or services. Statements with the same information are mailed to enrollees periodically.
  - o Medicare Summary Notices (MSN) are mailed twice per year. The MSN provides a summary of all claims filed during the previous month and how much was paid.
  - o An Explanation of Benefits (EOB) is similar to an MSN and is sent monthly to Medicare Advantage enrollees.

Review the account or statement to ensure dates, billing codes and amounts match. If the statement includes the name of a doctor not seen, treatment or equipment not received, or services not provided, contact the billing provider, who should report the error to Medicare, and the account will be noted with an update. If it is not reported by the provider, contact Medicare.

- Do not provide the enrollee's Medicare number to anyone other than the provider, which includes the doctor or medical facility.
- Do not accept "free" services in exchange for the Medicare enrollee's number.

If fraud is suspected call 1-800-MEDICARE (1-800-633-4227) or Report Medicare Fraud online. Taking an active role in their healthcare journey empowers Medicare enrollees to better understand their conditions and treatment, and helps prevent fraud, which benefits us all.

References

US Department of Justice. September 7, 2025. Office of Public Affairs | Two Florida Men Charged for $34.8M Fraud Scheme Targeting Medicare Beneficiaries | United States Department of Justice

US Department of Justice. January 7, 2026. Southern District of Florida | Two Healthcare Executives Convicted for Exploiting Elderly Medicare Advantage Beneficiaries in $34 Million Fraud Scheme | United States Department of Justice

US Department of Justice. January 29, 2026. Southern District of Florida | Florida Laboratory Owner Pleads Guilty to $52M Medicare Fraud Scheme Involving Genetic Tests | United States Department of Justice

CBS News. March 10, 2026. CBS News Investigation: Hundreds of LA hospices have multiple indicators of fraud

Fox News. March 12, 2026. 87-year-old doctor's Medicare number linked to $600M in fraud | Fox News

AARP. (undated) Help Stop Medicare Fraud

Medicare (undated) Reporting Medicare fraud & abuse | Medicare

HOW TO AVOID SCAMS WHILE APPLYING FOR ESTA

From Federal Trade Commission

It's that time of year when people start planning their spring and summer travels. If you have someone visiting you from another country (and they qualify for a visa waiver), they'll need to complete an Electronic System for Travel Authorization (ESTA) application through the official U.S. government website or app. To help them avoid a scam, be sure to let them know that they might come across ESTA lookalike sites trying to trick people into overpaying for the application. Here are some other things to share with visiting friends or family.

1. **The only place to apply is through the ESTA website or app**. Scammers have copycat websites that will likely overcharge you and might not even submit your paperwork, leaving you without the travel documents you need to enter the United States. Apply through the official website: esta.cbp.dhs.gov. Lookalike sites often have similar names, so look closely at the URL.
2. **The ESTA application fee is nonrefundable.** Applying for ESTA costs $10.27 and there are no refunds, whether you're approved or not. Any website that charges you more to apply — or says you can get a refund — isn't the real site. Know that, if your application is approved, you'll pay an additional $30 fee…and the official ESTA website only accepts credit and debit cards or PayPal. If someone charges you more or asks you to pay a different way, that's a scam.
3. **Application status information is online.** Not sure if you used the right website? Confirm that ESTA has the right information and get your application status on the ESTA website status lookup page.

For questions about your ESTA application, contact the U.S. Customs and Border Protection Traveler Communications Center at 1-202-325-8000.

Spot an ESTA scam? Report it to the FTC at ReportFraud.ftc.gov.

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. 04/2026