
PALM BEACH GARDENS POLICE DEPARTMENT

CRIME PREVENTION UNIT

Fraud & Identity Theft

PROTECTING YOURSELF FROM FRAUD
AND FINANCIAL LOSS



WHAT IS IDENTITY THEFT

Definition: is the deliberate use of someone else's personal information, such as their name, Social Security number, credit card details, or other identifying data, without permission, typically to commit fraud or other illegal activities. The goal of identity theft is often to steal money, open credit accounts, or gain access to financial or medical resources by assuming the victim's identity.

Common Targets: Social Security number, credit card information, bank accounts, medical records, and other personal details.

Federal Trade Commission (FTC) Data (2024)

- The FTC received fraud reports from **2.6 million** consumers last year, nearly the same amount as 2023. The most commonly reported scam category was **imposter scams**. Losses to government imposter scams in particular increased \$171 million from 2023 to a total of \$789 million in 2024.
- **Online shopping** issues were the second most commonly reported in the fraud category. This was followed by business and job opportunities, where reported losses totaled \$750.6 million—up nearly \$250 million from 2023. The other most reported categories of fraud were investment-related reports and internet services.
- For the second consecutive year, **email** was the most common way that consumers reported being contacted by scammers. Phone calls were the second most commonly reported contact method for fraud in 2024, followed by text messages.

HOW DOES IDENTITY THEFT HAPPEN?



Someone steals your personal information and racks up bills in your name, using your Social Security, Medicare number, credit card, or medical insurance details.

These scammers can find your information in several ways, including:

- Stolen mail
- Data breaches
- Theft of a wallet or purse
- Vehicular burglary
- Purchasing/sharing on the dark web
- Oversharing online
- Phishing Scams
- Skimming and Card Cloning
- Dumpster diving
- Social engineering
- Public Wi-Fi

MAILBOXES

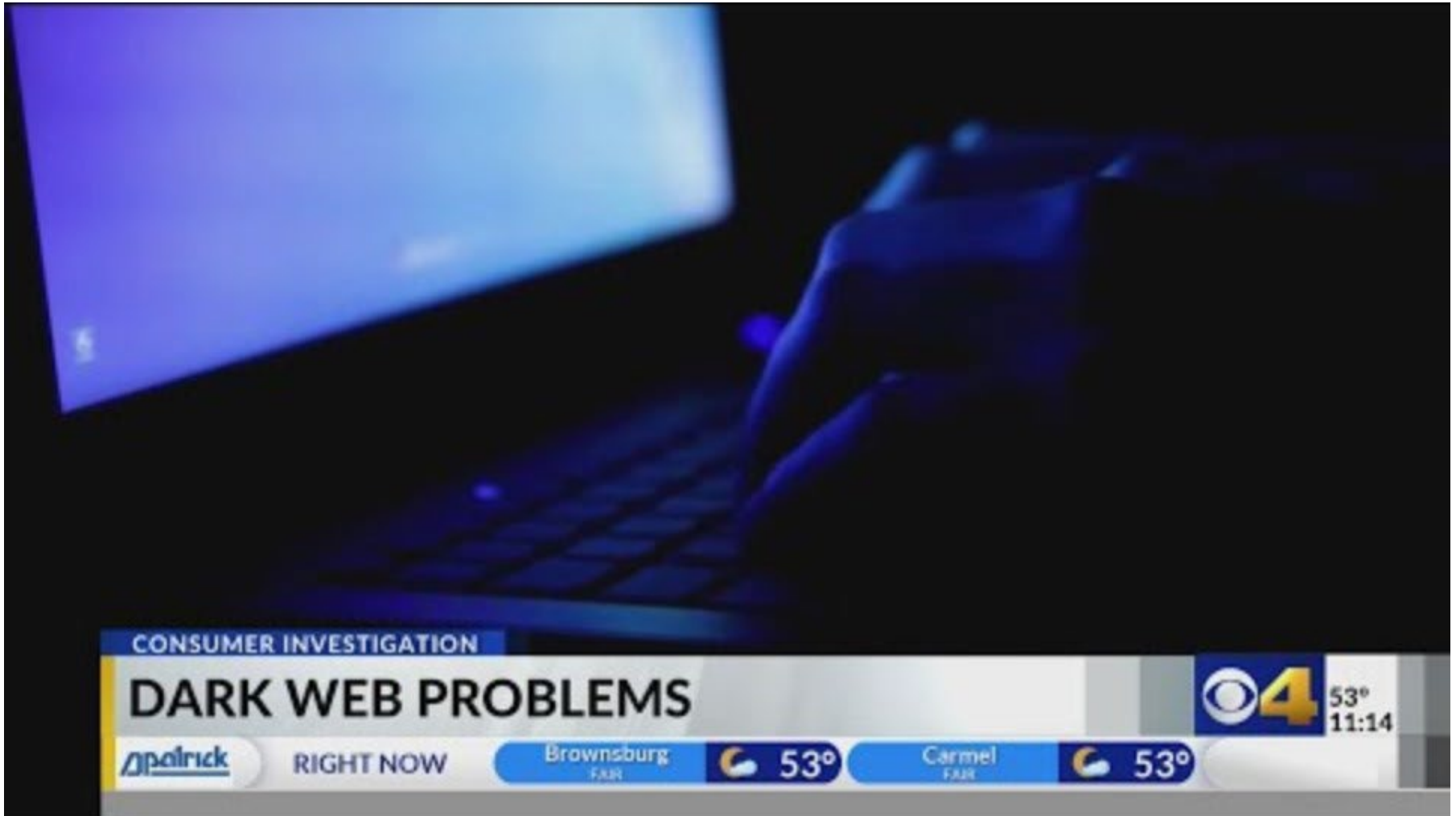
Many of the public access mailboxes throughout Palm Beach County, including Palm Beach Gardens, has been compromised.

Criminals are accessing these mailboxes and stealing checks. Once the checks are in their hands, they wash them and fraudulently fill them out for thousands of dollars.

It is highly recommended to use other forms of secured payment.



IDENTITY THEFT



CONSUMER INVESTIGATION

DARK WEB PROBLEMS

patrick

RIGHT NOW

Brownsburg
FAIR

53°

Carmel
FAIR

53°

CBS 4

53°
11:14

VICTIMIZATION OF SENIOR CITIZENS

- Senior citizens are most likely to have a “nest egg,” to own their home, and/or to have excellent credit—all of which make them attractive to con artists.
- Older Americans are less likely to report a fraud because they don’t know who to report it to, are too ashamed, don’t know they have been scammed, or because they are concerned that relatives may think the victims no longer have the mental capacity to take care of their own financial affairs.
- In criminal cases when an elderly victim does report the crime, they often make poor witnesses. Con artists know the effects of age on memory, and they are counting on elderly victims not being able to supply enough detailed information to investigators. In addition, the victims’ realization that they have been swindled may take weeks—or more likely, months—after contact with the fraudster. This extended time frame makes it even more difficult to remember details from the events.

GRANDPARENT SCAMS

Its Friday night and you get a call: “Grandpa, I have been arrested for DUI and I need \$2,000 dollars for bail. Please don’t tell my mom or dad.” The caller usually creates a sense of urgency and tells you to keep it a secret from the rest of the family.

Scammers often ask for payment in the form of a prepaid gift card, rest assure that no legitimate business or government will request payment over the phone in the form of a gift card. With the ongoing advancement of **artificial intelligence**, these scams are very difficult to identify.

When presented with a telephone call like this, here is what you can do:

- Investigate: Ensure the number matches the phone number of the family member or relative. If you are unsure, call another family member to confirm.
- Even if the caller begs you to keep it private, **trust your instinct** to verify with the parents or a spouse.
- Lastly, share your knowledge of these scams to others, **education is power!**

GRANDPARENT SCAM

ARTIFICIAL INTELLIGENCE SCAMS

AI scams use artificial intelligence, including deepfake technology, chatbots, and voice manipulation tools, to impersonate real people or create convincing fraudulent scenarios in order to steal money or personal information.

Common Techniques Used:

- **Deepfakes:** AI-generated fake videos or audio that mimic real people, often used to impersonate family members, celebrities, or business executives.
- **AI Chatbots:** Fraudulent customer service bots that impersonate legitimate companies to steal login credentials or payment information.
- **Voice Cloning:** AI can replicate someone's voice, allowing scammers to trick individuals into thinking they're talking to a trusted friend or family member.



ARTIFICIAL INTELLIGENCE SCAMS



IRS SCAMS

An official website of the United States Government

IRS

Help | News | English | Charities & Nonprofits | Tax Pros

File | Pay | Refunds | Credits & Deductions | Forms & Instructions | Search

Home / News / Tax scams/Consumer alerts

Tax scams/Consumer alerts

English | Español | 中文(简体) | 中文(繁體) | 한국어 | Русский | Tiếng Việt | Kreyòl Ayisyen

Topics in the news Thousands of people have lost millions of dollars and their personal information to tax scams. Scammers use the regular mail, telephone and email to set up individuals, businesses, payroll and tax professionals.

News releases The IRS **doesn't initiate** contact with taxpayers by email, text messages or social media channels to request personal or financial information. Know the telltale signs of a scam and [how to know if it's really the IRS](#).

Multimedia center

If you receive a threatening call claiming to be from the IRS, remember that the IRS will never demand immediate payment, ask for personal information over the phone, or threaten arrest—always verify the claim by contacting the IRS directly using their official website or phone number.

IRS SCAMS

CRYPTO CURRENCY



ONLY USE REPUTABLE CRYPTOCURRENCY EXCHANGES AND WALLETS WITH STRONG SECURITY ANYONE AND AVOID UNVERIFIED PLATFORMS.



ENABLE TWO-FACTOR AUTHENTICATION (2FA) ON ALL YOUR CRYPTOCURRENCY ACCOUNTS TO ADD AN EXTRA LAYER OF PROTECTION AGAINST UNAUTHORIZED ACCESS.



NEVER SHARE YOUR PRIVATE KEYS OR RECOVERY PHRASES WITH ANYONE AND STORE THEM SECURELY OFFLINE TO PREVENT THEFT.



BE CAUTIOUS WHEN USING CRYPTO **ATM MACHINES**, ENSURING THE MACHINE IS FROM A TRUSTED PROVIDER AND LOCATED IN A SECURE, WELL-LIT AREA.



AVOID UNSOLICITED INVESTMENT OFFERS AND BE SKEPTICAL OF "TOO GOOD TO BE TRUE" DEALS OR SOCIAL MEDIA PROMOTIONS PROMISING QUICK, HIGH RETURNS ON CRYPTO INVESTMENTS.

SOCIAL MEDIA

Review Your Privacy Settings

- **Adjust Privacy Settings:** Set your social media accounts to private or restrict access to only trusted individuals. This limits the exposure of your personal details.
- **Limit Profile Information:** Avoid sharing sensitive personal information like your full birthdate, home address, or phone number publicly on social media.

Stay Alert to Scams and Fake Contests

- **Watch Out for Prize Scams:** Scammers often pose as companies offering free prizes, gifts, or cash in exchange for personal information. If it seems too good to be true, it probably is.
- **Avoid Clicking on Suspicious Ads:** Ads on social media platforms that offer too-good-to-be-true deals can sometimes be scams designed to steal your information.

Be Cautious of Oversharing

- **Think Before You Post:** Avoid sharing detailed personal information such as your vacation plans, pet names, or daily routines, which can be used to answer security questions or guess passwords.
- **Share Selectively:** Even with friends, be mindful of what you share. Personal details such as family members' names, school names, and locations can be exploited by scammers.

Be Mindful of Geotagging

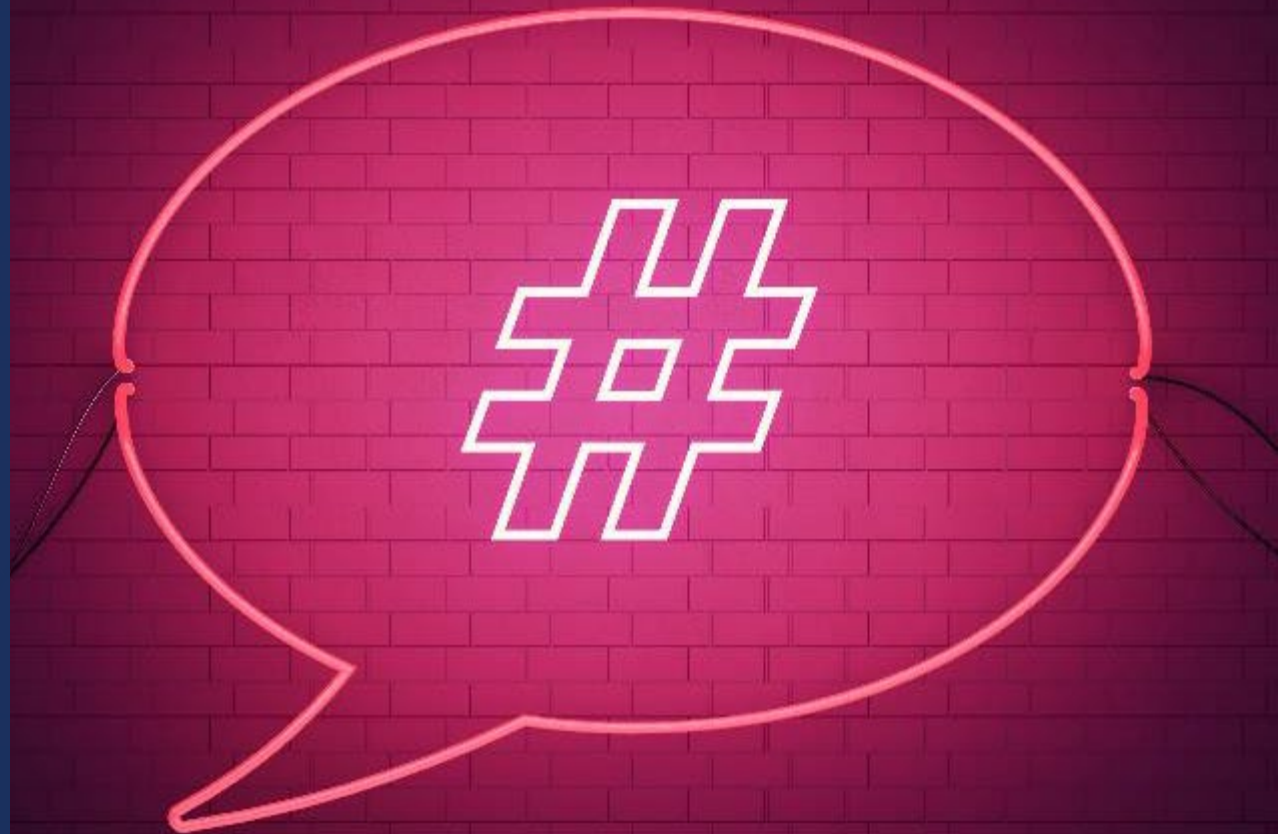
- **Disable Geotagging:** Avoid sharing your location in real-time, especially when posting photos or updates. Geotagging your posts can provide information that criminals can use to track your movements or learn your home address.
- **Share Your Location Privately:** If you want to share a location, do so after you've left the area to avoid revealing where you are in real-time.

ONLINE DATING SCAMS

You connect with someone on a dating site, and before long, they suggest moving the conversation off the platform to phone calls. They quickly express deep affection for you but claim to live far away or are stationed overseas. Eventually, they ask for financial help, such as money for a plane ticket or repairs to their car, so they can visit you.

What to avoid:

1. Don't send any money, **ever**. You will not get it back and they will always ask for more.
2. Trust your instincts when meeting a stranger, never let your guard down.
3. Oversharing personal information



CYBERSTALKING

To engage in a course of conduct to communicate, or to cause to be communicated, directly or indirectly, words, images, or language by or through the use of electronic mail or electronic communication, directed at or pertaining to a specific person

Examples:

Report ongoing harassment to your local police department.

Unwanted emails or text messages

Phone calls

Trying to hack personal accounts and use for exploitation

Posting inappropriate or private information on social media about the subject

DEED FRAUD - HOMES

Check Property Appraisal

- Verify under the parcel for owner details

Criminal Process (how its done)

- Files a **Quality Warranty Deed** to initiate the process of swapping owners
- Typically uses a fictitious ID, lawyer, and notary to pass the documents through the legal system
- It is unknown what the intent changes but however, it is speculated it will lead to fraudulently obtained loans against the home as the asset.

Property Characteristics (target homes)

- Homes valued at over a million and paid-off

Civil Attorney's Role (first step after notifying the police)

- **Quiet Title Deed** to transfer home back to original homeowner
- **Title typically remains the same**; only the deed changes but check to ensure it hasn't changed.

Growing Trend

- Notable increase in this process, state and local officials are working toward a resolution

Add a property fraud alert here:

<https://www.mypalmbeachclerk.com/services/property-fraud-alert>



BEST PRACTICES

1. Use strong, unique passwords for each of your accounts and change them regularly to prevent unauthorized access.
2. Enable two-factor authentication (2FA) on your accounts to add an extra layer of security.
3. Add spending alerts to your accounts.
4. Shred documents containing personal information before disposing of them to protect against dumpster divers.
5. Avoid clicking on suspicious links in emails, texts, or messages to protect yourself from phishing scams.
6. Shop only on secure websites with “https://” in the URL and a padlock symbol before entering payment details.
7. Freeze your credit to prevent unauthorized credit checks and new accounts being opened in your name.
8. Limit personal information shared on social media to reduce the risk of it being used to steal your identity.
9. Install and regularly update antivirus software on all your devices to defend against malware and viruses.
10. Check your financial statements regularly for unfamiliar transactions and report them immediately.
11. Crypto is typically use for anonymous payment, use extreme caution when dealing with these types of payment.
12. Don't send personal checks in the mail, utilize other forms of secured payment.
13. Try not to answer numbers you don't recognize.
14. Use a credit card at the gas pump, look for tap to pay to skip the zip code

If you believe you have received a call from someone trying to obtain money from you, please report it to the Federal Trade Commission:

Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or go online to [ftc.gov/complaint](https://www.ftc.gov/complaint)

If you were scammed and have sent money, please contact your local police department.



QUESTIONS?

PALM BEACH GARDENS POLICE DEPARTMENT
10500 N MILITARY TRAIL, PALM BEACH GARDENS, FL 33410
NON-EMERGENCY 561-799-4445