FLORIDA CONSUMER
NEWSLETTER
October 2024
A publication of the Florida Department of Agriculture and Consumer Services

PROTECTING PERSONAL INFO ON YOUR PHONE

Imagine carrying a written copy of all your conversations with you everywhere you went. Or copies of your account numbers, usernames, and passwords. Or photos and videos of loved ones and special moments. I bet you'd do just about everything in your power to protect all that valuable information.

Your mobile phone holds all that stuff — and maybe more. Are you doing everything in your power to keep it from ending up in the wrong hands? Here are four things you can do ***today*** to protect the personal information on your phone.

1. **Lock it.** Keep prying eyes out of your phone by setting it to automatically lock when you're not using it and create a PIN or passcode to unlock it. Longer passcodes are better, so use at least six digits. After you've set it up, you might be able to unlock your phone with your fingerprint, your face, or your iris.
2. **Update it.** Your phone's operating system has security features built into it, and phone manufacturers regularly push out free updates to protect you against security threats. Set your phone to automatically update the operating system to stay up with the latest protections. As an added security measure, you should update any apps you have on your phone and delete any apps you do not use.
3. **Back it up.** The convenience and portability of our phone puts it in peril. We might break or lose it, or an opportunistic criminal might steal it. Backing up your phone to the cloud or an external drive allows you to recover your information if something goes wrong.
4. **Track it.** Turning on the feature that helps you track a lost or stolen phone also lets you remotely lock or erase your phone if you think it has been stolen.

An ounce of prevention is worth a pound of cure. So, take a few precautions today to prevent the headache of dealing with a lost or stolen phone tomorrow.

IDENTITY THEFT

A wide range of information constitutes private personal information, including a person's name, address, date of birth, Social Security number, driver license number, credit card and bank account numbers, and even fingerprints and iris scans. These components of your personal identity are vulnerable to theft, both online and offline, and can be used to commit identity theft.

Identity theft, as defined by federal law, occurs when someone uses or attempts to use the private personal information of another person to commit fraud, typically for economic gain. There are several red flags that can alert you to the possibility that someone has stolen your identity:

- Being denied access to credit.
- Finding suspicious charges on bank or credit card statements.
- Receiving notice that private personal information has been compromised in a data breach.
- Receiving notice from a bank or creditor indicating suspicious account activity has occurred.
- Noticing that you have stopped receiving credit card bills.
- Finding errors in a credit report, such as a loan or account not opened by you.
- Encountering issues with medical insurance, such as denial of coverage or receiving bills for a treatment never performed.
- Receiving a bill for products or services that were never ordered or never received.
- Being denied state or federal benefits because you are listed as already having received them.
- Having a tax return rejected by the IRS because a refund has already been claimed or the reported income does not match IRS records.
- Receiving calls from a debt collector regarding a debt not owed.

Identity theft can negatively affect your credit, get you sued for debts that are not yours, result in incorrect and potentially health-threatening information being added to your medical records, and may even get you arrested. It is important to pay attention to the red flags, to know the types of identity theft, and to be proactive when you suspect identity theft has occurred.

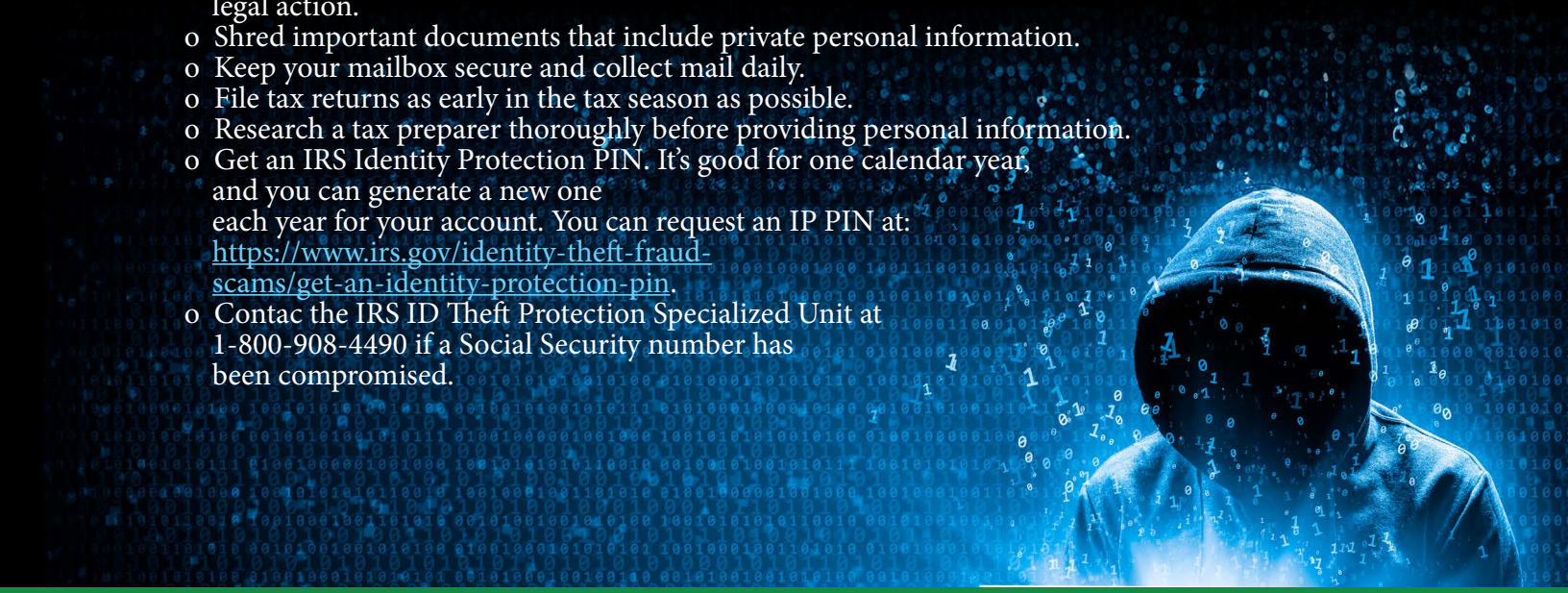
TYPES OF IDENTITY THEFT

Broadly speaking, identity theft is the fraudulent use of someone else's private personal information for some form of personal gain. It's important to understand the different types of identity theft, how they occur, and what you can do to protect yourself and your personal information.

These are some of the most common types of identity theft and steps you can take to combat them:

- **Financial Identity Theft.** This is the most common form of identity theft. It is a type of scam where someone uses your personal information to take over your financial accounts, such as credit cards, bank accounts, and Social Security number.
  What can you do?
  - o Protect your account numbers and passwords. Do not give your personal identification number (PIN) or password to anyone who asks, and do not keep them written down anywhere. Turn off the 'Save Password' feature in any internet browsers you use. Also, make sure to use different passcodes for your financial accounts and other sites you use online. Consider using a password manager to store all your passwords securely.
  - o Monitor your bank and credit card accounts on at least a monthly basis and check for activity you have not authorized. If you see something suspicious, contact your bank or credit card company immediately.
  - o If an identity thief uses your Social Security number to establish new credit accounts, you may not ever receive a bill or statement. Make a habit of visiting AnnualCreditReport.com at least once a year to access a free credit report from each of the three nationwide consumer reporting agencies. Contact the individual agencies (Equifax, Experian, and TransUnion) to see if they offer free reports more often and to find more information about placing a credit freeze on your account to control who can access your credit information.

- **Tax Identity Theft.** This occurs when someone other than the taxpayer files a fraudulent return using the taxpayer's Social Security number and personal information to receive a refund; fraudulently uses a taxpayer's Social Security umber to get a job, causing problems for the victim when his or her income does not match what has bene reported to the Internal Revenue Service (IRS); or fraudulently claims a taxpayer's child as a dependent, preventing that child from being rightfully claimed as a dependent on the taxpayer's annual return. Tax identity thieves may access personal information by going through trash cans in search of bills and documents containing sensitive information, posing as the IRS claiming to be contacting the individual about an issue with a tax return, or posing as a legitimate tax preparer for the purpose of accessing personal information.
  What can I do?
  - o Never provide any personal information in response to an unsolicited phone call, email, social media message or text message. The IRS will not contact consumers using these methods and won't threaten legal action.
  - o Shred important documents that include private personal information.
  - o Keep your mailbox secure and collect mail daily.
  - o File tax returns as early in the tax season as possible.
  - o Research a tax preparer thoroughly before providing personal information.
  - o Get an IRS Identity Protection PIN. It's good for one calendar year, and you can generate a new one each year for your account. You can request an IP PIN at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.
  - o Contac the IRS ID Theft Protection Specialized Unit at 1-800-908-4490 if a Social Security number has been compromised.



- **Medical Identity Theft.** This involves a fraudster using your personal information to receive health care in your name.
  What can I do?
  - Review any Explanation of Benefits statements you receive from your health insurer for mistakes or unfamiliar charges. If you see activity you don't recognize, report it to your insurance company.
  - Check with your doctor to ensure your medical records are accurate. If you start getting bills for medical services you didn't receive, call the provider and dispute the charges.
  - Ask questions before you give out your medical information. Some doctor's offices might ask for your Social Security number to identify you. Ask if they can use a different identifier or just the last four digits of your Social Security number. If another organization asks for information like your health insurance account number or Medicare number, or for details about your health, ask these questions first:
    - Why do you need it?
    - How will you protect it?
    - Will you share it? If so, with whom?

- **Criminal Identity Theft.** This type occurs when someone who has been arrested provides your personal information to law enforcement. You generally won't be able to detect criminal ID theft until consequences arise – for instance, a speeding ticket goes unpaid and a judge issues a bench warrant for your arrest.
  What can I do?
  - Consider limiting the amount of personal information you share on social media, as you never know who might access it.
  - Always use strong passwords and two-factor authentication. Make sure that you use secure, complex, and unique passwords for every account and device.
  - Keep physical IDs secure at all times. To stay safe, only carry the cards and documents that you need with you and make sure you keep a running list of what's in your wallet or purse (in case it's stolen).
  - Don't use public Wi-Fi. Hackers can easily hack public Wi-Fi and intercept any data that you enter on a site, including passwords and account details.

- **Child Identity Theft.** Children are particularly at risk for identity theft because there is currently no other credit history associated with their Social Security numbers. This allows criminals to easily create fraudulent identities using the stolen information. Even more enticing to criminals is the fact that a child's stolen identity may not be discovered for years until the child turns 18 and applies for an apartment, student loan, or their first credit card.
  What can I do?
  - Place a security freeze on your child's credit reports. When you request a security freeze from each of the three national credit bureaus (Experian, TransUnion and Equifax), they create a credit report for your child and then lock it down, so that any lender who attempts to process an application that uses your child's credentials will be denied access to their credit history.
  - Safeguard children's Social Security numbers. You should never share a child's Social Security number with anyone who doesn't have a very good reason for having it—which means it's smart to ask anyone who requests it why they need it. Keep your child's Social Security card in a secure place such as a safety deposit box and memorize the number so you don't have to write it down anywhere.
  - Avoid oversharing on social media. Identity thieves comb social media for personal information—from birthdays and addresses to clues about security questions such as "What's your first pet's name?" or "Where did you go to elementary school?" Minimizing the amount of information you share about your kids, limiting your sharing options to "friends" (rather than "public") and confining your circle of "friends" to people you trust and know personally can reduce the risk of exposing children's personal information.
  - Monitor your child's social media and other online activity. Think carefully and do research before you allow a minor child to have a social media account attached to their real name. Insist that they make you part of their shared network so you can monitor what they're sharing and with whom. Explain to your children why you're concerned, and advise them on the kinds of information they should never disclose.

Teach your children well. It's important for kids to understand identity theft risks. Find age-appropriate ways to talk to children about the topic. Make them aware that phone calls, text messages and emails aren't always from who they purport to be, and that they should check with you before responding to any of those that seek personal information. Let them know it's OK to hang up on an adult who asks for sensitive information, no matter who they claim to be.

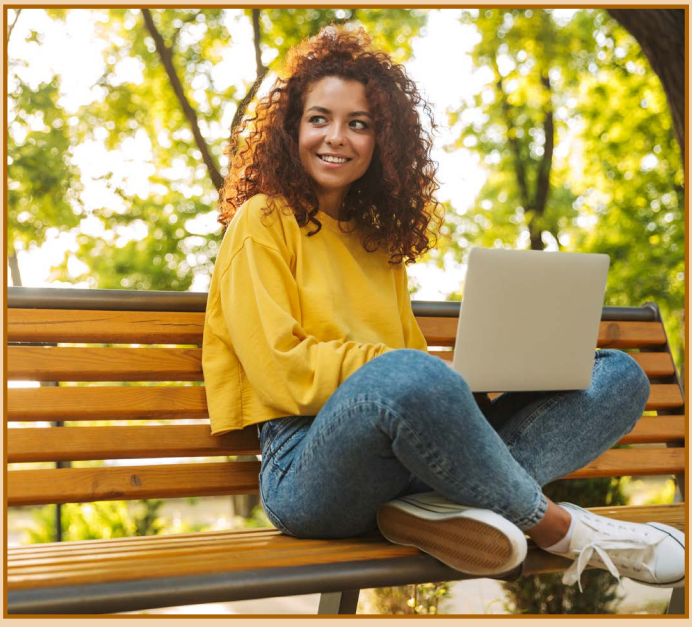
RECOVERING FROM IDENTITY THEFT

After discovering you are a victim of identity theft, you want to act quickly to limit the damage and close or report any accounts that the identity thieves are using. Review the following steps, and always take detailed notes of who you contacted, the actions you have taken, and when you took each action.

1. File a report with law enforcement. Under Section 817.568(18), Florida Statutes, you may file a report in the location where the theft occurred or in the city or county in which they reside. When filing, you should provide as much documentation as possible, including copies of debt collection letters, statements showing fraudulent charges, credit reports and any other evidence you may have. Request a copy of the police report to provide as documentation to creditors and credit reporting agencies.
2. File a report with the fraud department of the three major credit bureaus and request they place a fraud alert on your credit report. You should also order copies of your credit reports to determine whether there are additional fraudulent accounts listed in your name.
3. Visit IdentityTheft.gov to file a report with the Federal Trade Commission and get a recovery plan.
4. Contact the fraud department of each of your creditors and report the identity theft, even if your account at that creditor has not been compromised. Close the accounts you believe have been compromised and follow-up in writing immediately. The Federal Trade Commission provides an Identity Theft Affidavit, a standardized form used to report new accounts fraudulently opened in your name. Check with the company to see if they accept this form. If not, request that they send you their fraud dispute form.
5. Contact the fraud department at your bank or financial institution. If you suspect your accounts have been compromised, cancel your checking and savings accounts, and obtain new account numbers.

Identity theft is a crime that can take a toll on the financial health of the victim and the victim's family, but it doesn't stop there. Identity theft can feel deeply personal and can have an emotional impact on you and your family. The recovery process may be long and complicated, leaving victims feeling overwhelmed with feelings of loss, helplessness, anger, isolation, betrayal, rage, and even embarrassment. The emotional trauma can be increased if the identity thief is a family member or someone you considered a friend. It's important to remember that no one deserves to be the victim of a crime and there is no shame in asking for help.
While victims of identity theft must focus on clearing their identity, experts recommend that they also make time to heal the emotional wounds associated with being a crime victim. Here are a few coping tips to help with that process:

- Recognize your emotions.
- Be consistent and organized.
- Don't forget the rest of your life.
- Accentuate the positives.
- Take time for yourself.
- Be kind to yourself.
- Exercise.
- Set limits.



PHISHING SCAMS DON'T TAKE THE BAIT

By Alexandra House, Public Affairs and Digital Media Intern, FTC

Have you ever gotten a text or email warning you that something is wrong with an account online? Maybe it says your streaming account is about to be suspended unless you respond quickly. It might even have a link that will supposedly fix your account's problems. The message looks real. But is it?

Your first instinct might be to click to solve your problems. Don't click. There's likely nothing wrong. Instead, it might be a phishing scam. That's when scammers pose as well-known companies to get you to give up sensitive information via text or email. A phishing email might:

- say they've noticed some suspicious activity or log-in attempts — they haven't
- claim there's a problem with your account or your payment information — there isn't
- say you need to confirm some personal or financial information — you don't

While real companies might send you emails or text messages, they won't do things like send a link to update your payment information. Only scammers do that. Even opening a link in an unexpected text or email can expose you to scammers — even if you don't enter any sensitive info.

So, don't click on any links in unexpected emails or texts. If you're concerned, contact the company directly using a link you already use or a phone number you know is correct. And if you think you've given someone your Social Security, credit card, or bank account number, report it at IdentityTheft.gov and get a recovery plan. If you clicked on a link in an unexpected email, update your security software and run a scan to look for viruses and malware.

Then report the phishing scam. Tell the FTC at ReportFraud.ftc.gov, forward suspicious texts to SPAM (7726), and forward suspicious emails to ReportPhishing@apwg.org.

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.