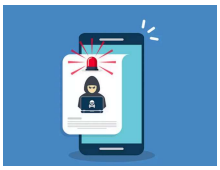
An official website of the United States government Here's how you know

MyCreditUnion.gov

Fraud Prevention Center

Is Your Financial Information Protected?

Each year, scammers and identity thieves steal billions of dollars from unsuspecting consumers. These criminals use various communication methods to steal information or trick consumers into handing over their money. Read below to learn how to recognize, report, and prevent fraud, common scams, identity theft, and cybercrimes.



Protect What's Yours

Learn different types of fraud, scams, and cybercrimes and how you can protect from, stop, and avoid them.

Frauds and Scams

According to the Federal Trade Commission (FTC), consumers lost nearly $8.8 billion to fraud in 2022. Of 2.4 million fraud reports, imposter scams were the most reported, followed by online shopping scams; prizes, sweepstakes, and lotteries; Investment scams; and business and job opportunities scams.

Common Types of Frauds and Scams

Type of Fraud/Scam	Description
Imposter Scams	Imposters pretend to be someone you know, like a family member or a friend, a representative from a government agency like the NCUA, IRS, or Social Security Administration, a tech support company, or a company you do business with. Imposters try to make you trust them in order to steal your personal information or ask you to buy a gift card, send digital currency, or transfer money. ***Be on guard.*** Government agencies, including NCUA, do not ask for money or your personal and financial information. When unsure whether they are who they say they are, DO NOT send money or share your information. Instead, terminate the communication and call the organization to authenticate the communication.
Online Shopping Scams	Online shoppers can be scammed in many ways: from not receiving products despite the payment to losing money and payment information to fake websites and apps. Scammers develop fake websites mimicking popular retailers' sites and take your money and payment information without delivering products. They also create counterfeit apps containing malware (malicious software) for the same reasons. ***Be on guard.*** Read refund and return policies prior to making a purchase. If your order didn't arrive or your refund request is denied, dispute the charges. Using a credit card for online purchases can make the dispute process much easier. Watch out for bogus websites and suspicious apps and only use official retailer websites and apps, which may offer stronger security. Also, monitor your credit and debit card transactions on a regular basis to increase the chance of spotting unauthorized purchases or withdrawals in the early stage of this fraud.
Prizes, Sweepstakes, and Lotteries	Scammers contact you claiming you won a prize, sweepstake, or lottery and then ask for money or your account information to cover taxes and other fees upfront. They might pretend to be from government agencies or claim you've won a foreign lottery, which is almost certainly a scam. ***Be on guard.*** Government agencies do not call to demand money or your financial information to collect a prize. Also, real sweepstakes are free and by chance. If you did not enter a lottery or sweepstakes or are unsure about the call, message, email, or letter, DO NOT send money or share your information. Instead, terminate the

Type of Fraud/Scam	Description
	communication and call the organization to authenticate the communication.
Investment Fraud	There are various types of investment fraud, including Ponzi schemes and pyramid scams. A Ponzi scheme is a fraudulent investment scam that pays earnings to earlier investors with money from new investors – similar to a pyramid scam. In many cases, scammers promise high investment returns without making an actual investment. Though they are called by different names, most investment scams share the same characteristics, such as guaranteed high returns with no risk and high-pressure sales tactics. ***Be on guard.*** Fraudsters often avoid putting the details about the investment in writing or call them confidential. If this is the case for you, consult with fiduciary financial advisors or just walk away. DO NOT rush into an investment opportunity without your own independent research. Talking with people you trust can help you see the offer more clearly. When suspicious, don't hesitate and report to as many agencies as apply: SEC, FINRA, CFTC, FBI, and FTC.
Business and Job Opportunity Scams	Scammers advertise job and business opportunities that sound too good to be true, such as doing minimal work with a high salary, pledging guaranteed income, or a proven business operation system. Scammers exploit your money and personal information by offering fake jobs or bogus coaching services, disguised as legitimate job offers, mentoring programs, or business opportunities. ***Be on guard.*** If it sounds too good, take your time and get a second opinion or talk to someone who has your best interests in mind. Before accepting a job offer, know that honest employers, including the federal government, will not ask for payment for the promise of a job. Before paying for a business opportunity, research the seller, the company, and the coach's credentials, and ask for the legally required 1-page disclosure document that tells any lawsuits against the seller, a cancellation or refund policy, and other information.
Fake Check Scams	Despite many variations, fake check scams involve two main components: 1) scammers send cashier's checks or money orders to you; and 2) they ask you to send part of the cashed money back to them in gift cards, money orders, or cryptocurrency. If you deposit the checks and they are later found to be fraudulent, you will likely be required to pay the deposited funds back to your credit union or bank. ***Be on guard.*** Cashier's checks are not cash and it can take weeks to

Type of Fraud/Scam	Description
	validate legitimacy. If the amount on the check is more than what it should be, void it and ask the sender to resend another check for the correct amount. Do not wire or send gift cards, money orders, or cryptocurrency. Your money is not protected in these transactions.
Check Washing Scams	Check washing scams involve changing the payee names and often the dollar amounts on checks and fraudulently depositing them. Occasionally, these checks are stolen from mailboxes and washed in chemicals to remove the ink. Learn more about check washing scams at United States Postal Inspection Service website. ***Be on guard.*** Retrieve your mail regularly instead of leaving it in your mailbox. Deposit your outgoing mail at your local Post Office or in blue collection boxes before the last pickup. If you're going on vacation, have your mail held at the Post Office or have it picked up by a friend or neighbor each day.
Disaster Fraud	Disaster fraud typically involves others trying to take advantage of the situation and examples include fake government employees and bogus charities. Fraudsters approach when you are vulnerable and in crisis to exploit your money and financial information while pretending to help with recovery. ***Be on guard.*** No FEMA, federal, or state workers will ask for or accept money from you when applying for disaster assistance. If someone wearing a FEMA jacket or shirt without an I.D., approaches, *do not* trust or offer any personal information and always ask to see an official I.D. Take your time and contact government agencies or local law enforcement to confirm identity and legitimacy of suspicious contacts.
Romance Scams	Scammers adopt a fake online identity and gain your affection and trust. They then manipulate you into believing that you have a romantic or close relationship with them. They make plans to meet in person, but it never happens because they often claim to be working outside the country. They ask for money for emergencies or trick you into providing your sensitive information. ***Be on guard.*** Scammers may use details about you shared on social media or dating sites before targeting you. Watch what you share on your social profiles. Also, a reverse image search of the person's photo may reveal whether your lover is real or fake. DO NOT send money, gift, or gift cards to your fake lover you haven't met in person.

Identity Theft

Identity theft happens when someone steals and uses your personal information without your permission to commit fraud. Thieves use your identity to fraudulently apply for credit, file taxes, get medical services or pretend to be you when arrested. These acts can damage your credit status and cost you time and money to restore your reputation.

How does identity theft happen?

Scammers may:

- Steal your wallet or purse to get IDs or credit or debit cards
- Take personal information from your electronic devices when using public Wi-Fi or USB charging stations
- Gain access to your personal information from a data breach
- Look through your social media accounts for identifying information
- Use "phishing" to get your personal information **(learn more in cybersecurity tab below)**
- Install skimmers (card readers that collect card numbers and PINs) at ATM machines, cash registers, or fuel pumps
- Divert mail from its intended recipients by submitting a change of address form
- Rummage through trash for credit union statements or other personal data
- Use different types of fraud and scams listed above

How can I protect myself against identity theft?

By taking the steps below, you can minimize your risks of identity theft.

1. **Review each of your three credit reports at least once a year**
    - Get your free credit reports from all three credit bureaus and review them thoroughly. All the information in your credit report should be about you and what you have done with your credit. If any suspicious or incorrect information is found, dispute it online or via mail.
2. **Read your credit card and credit union statements carefully and frequently**
    - Watch out for items you didn't purchase, services you didn't sign up for, and withdrawals you didn't make.
3. **Read the statements from your health insurance plan**
    - Review your medical bills for unrecognized charges and Explanation of Benefits statements for services you didn't receive.

4. **Protect documents with personal and financial information**
    - Keep any documents with your personal information in a safe place and shred them when you decide to get rid of them. Also, take your mail out of the mailbox daily. In case of being away from home, consider signing up for a hold mail service or forwarding service.

5. **Guard your information online and on your phone**
    - Use a strong password and add multi-factor authentication for accounts that offer it. Do not give your personal information to anybody who calls, emails, or texts you.

What should I do when my identity is stolen?

It is important to act fast to stop further misuse of your identity. If your identity is stolen, you should take below steps right away:

***Step 1*: Call the companies where the fraud occurred and explain your identity has been stolen.** Ask to close or suspend the accounts. Don't forget to change login credentials for the accounts as well.

***Step 2*: Place a fraud alert and get your free credit reports.** A fraud alert is free, lasts for a year unless renewed, and makes it harder for scammers to open new accounts in your name. When you contact one of the three main credit bureaus to place a fraud alert, that company must tell the other two and you will be entitled to free copies of your credit reports. Review your reports thoroughly and make notes of any unrecognized accounts and transactions for identity theft and police reports.

***Step 3*: Report identity theft to the FTC and local police department.** An identity theft report and a police report document that you have been an identity theft victim.

***Step 4*: Close fraudulent accounts opened in your name and remove bogus charges from your accounts.** Call the fraud department of the companies where the fraud occurred, explain your identity has been stolen, provide the identity theft (and police reports), and request to close fraudulent accounts and remove bogus charges. Ask to send you a confirmation letter of the actions.

***Step 5*: Correct your credit report by sending an identity theft letter along with the identity theft report and proof of ID to all three credit bureaus.** If someone steals your identity, you have the right to remove fraudulent information from your credit report.

If you wish to add extra protection against fraud, consider placing an extended fraud alert or credit freeze to your credit report. While an extended fraud alert makes it harder for scammers to open new accounts for 7 years, a credit freeze limits access to your credit report for both you and others and lasts indefinitely unless you lift or remove it.

To learn more, visit IdentityTheft.gov.

Cybersecurity

Cybersecurity is the process of protecting networks, devices, and data from unauthorized use or criminal access to ensure integrity, confidentiality, and authentication of information. From the ways we communicate, use transportation, shop, bank online, and work remotely, our daily lives significantly rely on cybersecurity in our interconnected digital world. Because criminals from across the globe are constantly looking for new opportunities to attack our digital systems to exploit and cause damage, we have to stay vigilant.

Learn different types of cybercrimes and how you can protect from, stop, and avoid them.

Different Types of Cybercrimes

Type of Cybercrime	Description
Business Email Compromise (BEC)	In this scam, criminals target both businesses and individuals. It has evolved from a simple form of sending an email that appears to come from a business or individual you know and requesting a seemingly legitimate payment, often urgently, via a wire transfer, to compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. More recently, criminals receive funds from cryptocurrency platforms where they can quickly disperse the funds. ***Be on guard.*** Check the accuracy of email senders. If payments or payment changes are requested, verify with the intended recipient first. As soon as fraud is detected, contact the originating financial institution, and request a recall of the fund transfer as well as a Hold Harmless Letter or Letter of Indemnity.
Ransomware	Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, networks, or cell phone. Malware is installed in various ways, including through links and attachments in emails, downloads from malicious websites, or removable drives. Criminals hold your data hostage until the ransom is paid or pressure you for the ransom by threatening to destroy or release your data to the public. ***Be on guard.*** One way to prevent or minimize the risks is to conduct system and software scans using anti-virus and anti-malware programs. You can also make an offline backup of your data and update your operating systems and software on your devices

Type of Cybercrime	Description
	frequently. If you fall victim to this crime, file a report regardless of whether you have paid the ransom or not.
Spoofing	Scammers deliberately falsify an email address, sender name, phone number, or website URL and manipulate you into believing that it is from a trusted source. Once you seem engaged, they lead you to download malware, send money, or share personal, financial, and other sensitive information. Spoofing is often used in connection with other crimes. ***Be on guard.*** Scammers tweak little things – often a letter, symbol, or number. DO NOT click on or download anything unless they are verified to be from legitimate sources. Additionally, if a call comes from an unknown number or the caller (or a recording) asks you questions or to hit a button, DO NOT hang on, just hang up.
Phishing	Scammers send an email, text, or message on social media that appears to be from a legitimate business and lure you into providing your information by visiting a website that looks almost identical to the real one. Once you click the link, you may be asked to provide sensitive information for verification purposes, such as your Social Security number, login credentials, mother's maiden name, or place of birth. Once the information is provided, scammers use it to access your accounts to steal money or sell your information to other scammers. ***Be on guard.*** Businesses and financial institutions would never call you first to verify your account information or to ask for sensitive information. DO NOT click links in emails or messages. If you believe the contact may be legitimate, contact the business or visit the official website yourself. Never provide your personal and sensitive information in response to an unsolicited request over the phone or the Internet. If you feel suspicious of or fall victim to Phishing, alert the situation to your credit union and other financial institutions and file a report with FTC.
Technical Support Impersonation Scams	Criminals pose as service representatives of a company's technical or computer repair service and ask you to contact them through email or by phone about a highly priced, soon-to-renew subscription. Once you contact them, they convince you to grant full control access to your computer for technical support and a refund. With the granted access, criminals steal your sensitive information and conduct unauthorized wire transfers of funds from your accounts. Almost half the victims who report this crime are over 60 years old.

Type of Cybercrime	Description
	Be on guard. When you receive email about unsolicited services or services you didn't sign up, resist the pressure to act quickly, search online for the company, and initiate the communication from your end. Do not send wire transfers to someone you have only spoken to online or via phone. Also, do not download unfamiliar software or grant remote access to unknown persons or entities.

Basics of Cyber Hygiene

Cyber hygiene refers to the practices and steps taken to protect your digital assets and information from unauthorized access and cyber threats. By practicing good cyber hygiene, you can ensure the safety and security of your digital assets and information online.

1. **Turn on Multifactor Authentication**
   Multifactor authentication, also known as two-factor authentication, or MFA, is a highly effective security measure that requires an extra form of identification, on top of your password, when trying to access your digital assets and information. Most websites now offer this security feature such as a PIN, fingerprint, confirmation text, and authentication application. Once prompted, opt in!
2. **Update Your Software**
   Criminals take advantage of well-known problems and vulnerabilities. Network defenders work hard to fix them, but their work heavily relies on you installing the latest fixes. Keeping your devices up to date with the latest security patches and utilizing automatic updates for operating systems, antivirus software, and applications will help protect your digital assets and information from cybercrime.
3. **Recognize and Report Phishing**
   Phishing is the number one way our information gets compromised, and we are more likely to fall for phishing than we think. Be cautious of unsolicited phishing emails, texts, and calls that ask for personal and sensitive information. Don't click on links or attachments from unknown sources and avoid sharing sensitive information or credentials over the phone or email, unless necessary. If suspicious, trust your instincts and think before you click!
4. **Use Strong Passwords**
   Strong passwords are critical to protecting your digital assets and information. Make sure your password is long, unique, random, and including all four-character types. Password managers are a powerful tool to create passwords and they make storing passwords and user IDs much easy!

Fraud Report Cheat Sheet

If you find out you've been scammed, there may still be something that can be done to stop the further damage.

Where to report

If you suspect a fraud, scam, identity theft, or cybercrime, report to as many agencies as possible.

What to Report	Where to Report
Report anything you think may be identity theft – in a scam, cybercrime, or data breach – and get a recovery plan.	Identitytheft.gov
Report unwanted calls from telemarketers and register your number on the national do not call registry.	Donotcall.gov
Report anything you think may be a fraud, scam, or bad business practice.	Reportfraud.ftc.gov
Report any suspected cybercrime.	Ic3.gov
Report a suspected investment fraud or a problem with your investments.	Sec.gov
Report a potentially fraudulent, illegal, or unethical investment activity.	Finra.org
Report a violation of the Commodity Exchange Act or Commission regulations.	Cftc.gov
Report a suspected financial/economic crime or fraud (e.g., mortgage fraud or investment fraud).	Fbi.gov
Report any fraud related to natural or man-made disasters.	Justice.gov

Related Resources

- Credit Reports & Credit Scores
- Checking and Credit Cards
- Understanding your Credit Card Statement
- Identitytheft.gov

- Reportfraud.ftc.gov
- Fbi.gov

Last updated on 11/29/23