

# Protecting Your Assets

## Is Your Identity Safe? What To Do If It's Not

by Mariana Raymond of Truecaller

(NAPS)—Identity theft is becoming more common, affecting people from all walks of life—but you can protect yourself.

### The Problem

Scammers are always finding new ways to steal personal information, often leaving their victims with financial losses and a sense of violation.

### An Answer

Staying informed can make a big difference in keeping yourself safe. Here's what you should know:

### How Identity Theft Happens

Most identity theft happens online. Often when someone clicks links from text messages, emails, or even is catfished. The link you click could lead you to a fake website to input credentials or have you install an app that can retrieve your passwords to important accounts.

### Identity Theft Scams on the Rise

- **Synthetic Identity Theft:** With synthetic identity theft, scammers mix real and fake information to create a new, false identity. They might use a real Social Security number alongside made-up details. This lets them open bank accounts, get credit cards, or even apply for loans—using a fake identity that feels all too real.
- **Medical Identity Theft:** Medical identity theft happens when someone uses your personal medical information to access healthcare services, prescription drugs, or medical devices. This can leave you with unexpected medical bills or inaccurate records, which can complicate future treatments. It's a frustrating situation, but knowing what to look for can help.
- **Account Takeover Fraud:** In account takeover fraud, scammers take control of your online accounts, such as banking, email, or social media. This often happens through phishing emails, weak passwords, or data breaches. Once inside, they can drain your funds or steal even more personal details. It's scary, but there are ways to protect yourself.
- **Deepfake and AI-driven Identity Theft:** As technology advances, criminals use tools such as artificial intelligence (AI) to create deepfakes—fake videos or voices that look and sound just like real people. They can use these to trick others into believing they are someone else. It's a high-tech problem, but you don't need to be a tech expert to fight back.

### Ways to Protect Yourself

No solution is foolproof, but there are 7 steps you can take to protect yourself and lower the chances of becoming a victim:

**1. Use a Caller ID & Scam Blocking app:** The Truecaller app helps identify unknown calls and messages, and will even identify scam numbers in real time. People around the world actively report numbers as scams and write



**Identity theft can happen to anyone, but you can take steps to protect yourself.**

comments about their experience, and you can see statistics about scammers' call patterns.

**2. Use Strong and Unique Passwords:** Use passwords that are tough to crack—mix letters, numbers, and symbols. Avoid reusing passwords across accounts. A password manager can be a handy tool to create and store them safely.

**3. Enable Multi-Factor Authentication (MFA):** MFA adds an extra layer of security to your accounts. After entering your password, you'll need to verify your identity again, like with a code sent to your phone. It's like adding a second lock on your door, making it harder for scammers to break in.

**4. Monitor Your Credit Regularly:** Keep an eye on your credit reports for anything unusual, such as new accounts you didn't open. It's one of the quickest ways to spot identity theft early. Many places offer free credit monitoring services, so take advantage of them.

**5. Consider Identity Theft Protection Services:** Some services can keep an eye on your personal information and alert you if they spot something suspicious. While they can't prevent identity theft, they can make the recovery process smoother if it happens to you.

**6. Secure Your Devices:** Keep your phone, computer, and other devices updated with the latest security patches. Use antivirus software and strong passwords to keep hackers out. It's a simple habit that can go a long way.

**7. Shred Important Documents:** Even in today's digital age, physical paperwork can still be a goldmine for thieves. Shred any documents with personal information—bank statements or medical bills—before you toss them out.

Staying informed about the latest scams and being careful with your information can make a big difference. And if you do become a victim, don't panic. Report it to the authorities or your credit bureau right away. They can help you limit the damage and start the recovery process.

### Learn More

For further facts and tips, visit [www.truecaller.com](http://www.truecaller.com).