YOUR IDENTITY

Your personal identity is made up of many parts, like a puzzle. Some pieces may already be public, but scammers are always looking for ways to get the rest. With enough information, they can steal your identity and use it for fraudulent purposes.

HOW TO FREEZE YOUR SOCIAL SECURITY NUMBER

If you're worried about identity theft, you can place a **"credit freeze"** on your Social Security number. This prevents criminals from opening new accounts in your name, even if they have your information.

To do this, you must contact each of the three major credit bureaus online or by phone.

- Equifax: 1-800-685-1111
- Experian: 1-888-397-3742
- TransUnion: 1-888-909-8872

MORE IDENTITY THEFT TIPS

IF YOU'RE TARGETED

- Stop responding immediately.
- Report to the Police Department.
- Report scams at reportfraud.ftc.gov.
- For mail fraud, contact the U.S. Postal Inspection Service.
- **Call your bank or credit card company right away if money was sent.**
- Enable two-factor authentication on your accounts.

RESOURCES

Fairfield Police Department
(203) 254-4800

Federal Trade Commission (FTC)
1-877-382-4357
ReportFraud.ftc.gov

Crime Complaint Center (IC3)
www.ic3.gov

AARP Fraud Watch Network
1-877-908-3360
aarp.org/fraudwatchnetwork

Better Business Bureau Scam Tracker
(203) 269-2700
bbb.org/scamtracker

Scam Protection

FAIRFIELD POLICE
TOWN OF FAIRFIELD
FOUNDED 1639
CONNECTICUT

TIPS TO PROTECT YOURSELF FROM INTERNET AND PHONE SCAMS

COMMON SCAMS

PHONE SCAMS
Calls pretending to be IRS, police, or utility companies.

EMAIL/INTERNET SCAMS
Fake invoices, phishing links, "urgent" account notices.

PRIZE & LOTTERY SCAMS
"You've won!" messages you never entered.

GRANDPARENT SCAMS
Pretending to be a loved one in trouble.

ROMANCE SCAMS
New dating relationships asking for money.

MAIL FRAUD
Fake checks, sweepstakes, or donation requests.

WHAT IS CRYPTOCURRENCY?

Cryptocurrency is digital money. It can be bought, sold, and transferred online using apps or exchanges. Unlike traditional money, cryptocurrency transactions are often harder to trace.

HOW SCAMMERS USE IT

Scammers may ask victims to buy cryptocurrency and send it to them as "payment" or as a way to "protect your money." Once the funds are sent, they cannot be reversed or recovered. This makes cryptocurrency a favorite tool for fraud, often used in romance scams, tech support scams, and investment fraud.

> I was scammed out of my life savings. Deep down, I suspected something was wrong, but I was too embarrassed to ask for help. **That hesitation cost me $250,000.** All my money.
>
> If I could give one piece of advice, it would be this: do not be ashamed. There are people who are ready and willing to help, including your friends, your family, and the police. If I had reached out sooner, I would not be in the situation I am today.
>
> - Karen B.
> Victim of a Dating Scam

> They convinced me I had many Amazon accounts involved in money laundering and my bank was trying to steal my identity.
>
> They said the only way to protect myself and my family was to withdraw cash and hand it over to someone who would come pick it up, and the Treasury Department would pay me back. They stayed on the phone with me the whole time, acting so kind and caring, that I truly believed they were helping me. I am smart, but I was manipulated by people who knew exactly what they were doing. The shame I feel is overwhelming.
>
> - Regina C.
> Victim of a fraudulent return Scam

CONVERSATION RED FLAGS

- Pressure to act immediately.
- Asked to pay with gift cards, wire transfer, or cryptocurrency.
- Caller/email refuses to provide verifiable contact info.
- Poor grammar, spelling, or formatting in emails.
- Promises or threats that don't make sense.
- Will ask you to withdraw money and remain on the phone.
- Caller or email uses intimidation, such as threatening arrest, loss of benefits, or legal action.
- Pressure to move communication to another platform (e.g., "Let's continue this on WhatsApp").
- Unusual payment instructions, such as depositing checks and then sending money elsewhere.

WHAT TO DO

- **Verify:** Hang up and call the official number. *Not the one they called from or provide over the phone/email.* **Do not trust the caller ID!**
- Call a trusted friend or police to ask if the situation makes sense.