# Beginner's Guide To Identity Theft Protection

*Guide · Credit Freezes, Dark-Web Monitoring, SSN Hygiene, And The Recovery Plan If You're Already A Victim.*

**Who this is for: anyone who's worried about identity theft but isn't sure what actually helps. This guide covers the full prevention stack — most of which is free — plus what to do if you're already a victim.**

## How Identity Theft Actually Happens

Identity theft isn't usually high-tech. The most common paths:

- **Data breaches** — your info is leaked from a service you used. Sold on the dark web. Reused by criminals.
- **Phishing** — you give up info thinking you're talking to a legitimate company.
- **Mail theft** — physical mail with sensitive info (tax docs, bank statements) intercepted.
- **Wallet / phone theft** — physical theft, then exploitation of what's stored.
- **Tax fraud** — someone files your tax return first to collect the refund.
- **Medical fraud** — someone uses your insurance for treatment.
- **Synthetic identity** — your SSN combined with fake details to create a new identity for credit fraud.

## Prevention — The Free Stack

### 1. Freeze Your Credit At All 3 Bureaus

The single most powerful free defence. A credit freeze blocks new credit accounts from being opened in your name. Existing accounts work normally. To open new credit yourself, you temporarily 'thaw' the freeze — usually instant via the bureau's website. Free for everyone since 2018. Set this up today, in 15 minutes total:

- **Equifax:** equifax.com/credit-report-services/credit-freeze
- **Experian:** experian.com/freeze
- **TransUnion:** transunion.com/credit-freeze
- **Bonus bureaus:** Innovis (innovis.com) and ChexSystems (chexsystems.com).

Save the freeze PIN / password for each bureau in your password manager.

### 2. Monitor For Breaches

Three free services tell you when your data appears in a breach:

- **Have I Been Pwned (haveibeenpwned.com)** — sign up notifications for every email you use.
- **Mozilla Monitor** — same data, friendlier interface.
- **Google Password Checkup** — checks every Chrome-saved password against breach databases.

### 3. Protect Your SSN

- Never give SSN over phone or email unless you initiated the call to a known number.
- Remove SSN card from wallet. Store in fire safe.
- Don't share SSN on intake forms unless legally required (medical, employment, financial).
- Get an IRS Identity Protection PIN (free, prevents tax-return fraud) at irs.gov/ippin.
- Lock your SSN with the Social Security Administration's online portal.

### 4. Annual Credit Report Pulls

annualcreditreport.com gives you free reports from all 3 bureaus once a year (more frequent during economic downturns). Stagger them: pull one bureau every 4 months and you have continuous monitoring without paying. Review every line for unfamiliar accounts.

## Prevention — Paid Identity Protection (Worth It?)

Paid services like Aura, IdentityIQ, LifeLock, and Identity Guard offer dark-web monitoring (data sold before becoming public), SSN monitoring, court-records monitoring, and identity-theft insurance ($1M-$5M is typical). Cost: $10-30/month.

Worth it if:

- You've been a victim before (recurrence risk is high).
- You have elderly parents to monitor (huge value).
- Your SSN is in known breaches and you can't get a new one.
- You don't have time / discipline for manual monitoring.

Probably overkill if you have credit frozen, MFA on everything, and disciplined manual monitoring.

## Family Coverage

- **Spouse** — same coverage as yours.
- **Kids** — freeze their credit until age 18 (free, prevents child identity theft).
- **Elderly parents** — paid identity protection often makes sense for them; harder to do DIY.
- **College kids** — independent monitoring; they're high-target.

## If You're Already A Victim — Recovery Plan

### First 24 Hours

1. **Freeze your credit** at all 3 bureaus if not already done.
2. **File an identity theft report** at IdentityTheft.gov. Generates an FTC affidavit you'll need.
3. **Place fraud alerts** on credit reports.
4. **Contact the institutions involved** using numbers from official websites — never anything in suspicious emails.
5. **Change passwords** on email, bank, brokerage, primary social. Enable authenticator-app MFA.
6. **Document everything** — dates, names, case numbers.

### First Week

- Pull free credit reports from all 3 bureaus and review every line.
- Dispute unfamiliar accounts in writing.
- If tax return rejected, file IRS Form 14039.
- If unemployment claim filed in your name, contact your state's labour department.
- If medical: check Explanation of Benefits for unfamiliar claims, file disputes.
- Consider professional help: identity-theft restoration services or an attorney for serious cases.

### Following Months

- Track all interactions: every call, every letter, every dispute. You'll reference these for months.
- Continue pulling credit reports more frequently (monthly via free services if available).
- Watch for new fraud (recurrence is common).
- When the case is closed, move to ongoing monitoring (paid IDP often makes sense post-incident).

## Where To Go Next

- **Use the Identity Theft Risk Scorecard** — score your exposure across 5 vectors.
- **Use the Identity Theft Prevention Checklist** — full prevention stack.
- **Use the Identity Theft Warning Signs Cheat Sheet** — early-warning signals.