Financial Planning Solutions, LLC
Creating your ideal tomorrow while living well today™

How To Protect Your Information, Credit, or Assets From Theft

---

1. Watch Out for Phishing

Phishing scams often arrive via email, text, or phone call, pretending to be from trusted institutions. These messages may urge you to click a link or provide personal information.

- **How to protect yourself: Never click on suspicious links or provide information unless you're absolutely sure of the sender's identity.**

👉 FTC Guide to Recognizing and Avoiding Phishing Scams

---

2. Enable Two-Factor Authentication (2FA)

Two-factor authentication adds an extra layer of security by requiring a second form of identification (like a code sent to your phone) in addition to your password.

- **How to protect yourself: Enable 2FA on all accounts that offer it, especially email, banking, and social media.**

👉 How to Turn On 2FA (CISA.gov)

---

3. Freeze Your Credit

Freezing your credit prevents thieves from opening new accounts in your name—even if they have your personal information. You can freeze your credit for free through each of the three major credit bureaus and unfreeze if applying for credit.

- **How to protect yourself: Freeze your credit with Experian, Equifax, and TransUnion. You can lift the freeze temporarily if you apply for new credit.**

👉 FTC Guide on How to Freeze Your Credit

(Continued)

4. Secure Your Bank and Investment Accounts

Hackers may try to access financial accounts by exploiting weak passwords or compromised devices.

- **How to protect yourself:**
  - **Use strong, unique passwords.**
  - **Enable 2FA. (Two Factor Authorization)**
  - **Review your account activity regularly. (At least weekly and notify the institution if you see anything)**
  - **Avoid public Wi-Fi for banking or other sites that have your sensitive information.**

👉 How to Protect Online Bank Accounts

---

5. Guard Against IRS Identity Theft

Tax identity theft occurs when someone uses your Social Security number to file a tax return and claim your refund.

- **How to protect yourself:**
  - **File your taxes early.**
  - **Use a secure preparer or platform.**
  - **Consider getting an IRS Identity Protection PIN (IP PIN).**

👉 IRS Identity Theft Central

---

6. Monitor Your Accounts and Credit

Stay vigilant by checking your credit reports and financial accounts regularly for suspicious activity.

- **How to protect yourself:**
  - **Review your credit reports at least once a year.**
  - **Set up alerts with your financial institutions.**

👉 **AnnualCreditReport.com – Get Your Free Reports** **(This is the only free legitimate site you should use)**

(Continued)

7. Use Trusted Security Software

Good antivirus and anti-malware software can protect your devices from threats.

- **How to protect yourself: Keep software updated and install trusted security apps on your phone and computer.**

Consumer Reports: Best Antivirus Software

---

8. Download a recent Social Security Statement

Even if you are years away from collecting Social Security, we feel it is a good practice to have an active log in to the Social Security site as well as download a PDF of your statement. This will allow us to review it and discover any potential discrepancies.

Go to www.ssa.gov/myaccount and create an account if you haven't done so already. We strongly recommend setting up a Two - Factor Authorization which will send you a code to your cell. Once created and logged in, you will see a way to view and save your statement. Also, you will see a link to replace your Social Security Card. If you have misplaced yours, we recommend requesting a replacement. Do not laminate this card as that could render your card invalid.