Identity Theft Protection Strategies Guide

Practical Approaches to Safeguard Your Personal Information

This guide provides specific, actionable strategies to protect your personal information from identity theft. Each strategy includes what it is, why it matters, and detailed steps for implementation. Choose the strategies that best fit your personal situation to build a comprehensive protection plan.

Using This Guide

The strategies are organized into three categories: digital protection, physical document protection, and monitoring actions. Each strategy is rated by implementation difficulty:

- **Easy:** Simple to implement with minimal technical knowledge
- **Moderate:** Requires some technical knowledge or regular effort
- **Advanced:** Involves more complex setup or ongoing commitment

Start with strategies marked "Easy" and progressively add more as you build your protection habits.

Digital Protection Strategies

Use Strong, Unique Passwords Easy

What it is:

Creating complex, different passwords for each of your accounts to prevent unauthorized access if one account is compromised.

Why it matters:

If you use the same password across multiple accounts, a data breach at one website gives thieves access to all your accounts with that password. Strong, unique passwords significantly reduce this risk.

How to implement:

1. Create passwords with at least 12 characters, including uppercase and lowercase letters, numbers, and symbols
2. Avoid using personal information like names, birthdays, or common words
3. Use a different password for each account, especially financial and email accounts
4. Consider using a passphrase (a string of random words) for better security and memorability
5. Use a password manager to generate and store strong passwords

> *Tip: Start by changing passwords for your most important accounts: email, financial accounts, and social media.*

Recommended Resources:

- NIST Password Guidelines: pages.nist.gov/800-63-3
- Password managers: LastPass, Bitwarden, 1Password

Enable Two-Factor Authentication Easy

What it is:

Adding a second layer of security that requires not only a password but also a temporary code or authentication through a separate device.

Why it matters:

Even if someone obtains your password, they still can't access your account without the second factor. This significantly increases security, especially for important accounts.

How to implement:

1. Identify accounts that offer two-factor authentication (most major email, banking, and social media platforms do)
2. Access the security or privacy settings in each account
3. Look for "two-factor authentication," "2FA," or "multi-factor authentication"
4. Choose your preferred second factor: authenticator app (most secure), text message, or email
5. Follow the setup instructions for each account
6. Store any backup codes in a secure location

> *Tip: Authenticator apps (like Google Authenticator or Authy) are more secure than SMS text messages, which can be intercepted.*

Recommended Resources:

- 2FA Directory: twofactorauth.org
- Authenticator apps: Google Authenticator, Microsoft Authenticator, Authy

Manage Social Media Privacy Settings Moderate

What it is:

Configuring your privacy settings on social media platforms to limit what personal information is publicly visible.

Why it matters:

Social media profiles often contain valuable personal information identity thieves can use to answer security questions, target phishing attempts, or build a profile for synthetic identity theft.

How to implement:

1. Review and adjust privacy settings on all social media accounts
2. Limit personal information (birthdate, address, phone number) visibility to friends only or remove it entirely
3. Disable location tracking and geotagging in posts
4. Review and manage friend/follower lists regularly
5. Check which third-party apps have access to your social media accounts and remove unnecessary connections
6. Be selective about what you share, avoiding posting identification documents, travel plans, or financial information

> *Tip: Use social media platforms' "View As" features to see what information is visible to the public.*

Recommended Resources:

- FTC Social Media Privacy Guide: consumer.ftc.gov
- Platform-specific privacy guides (search for "[platform name] privacy settings guide")

Use Secure Internet Connections Moderate

What it is:

Taking precautions when connecting to the internet, especially on public Wi-Fi networks, to prevent data interception.

Why it matters:

Public Wi-Fi networks are vulnerable to eavesdropping attacks where criminals can intercept data transmitted between your device and websites, potentially capturing login credentials and personal information.

How to implement:

1. Avoid using public Wi-Fi for sensitive transactions (banking, shopping, accessing financial accounts)
2. Use a Virtual Private Network (VPN) when connecting to public Wi-Fi
3. Ensure websites use HTTPS (look for a padlock icon in the browser address bar)
4. Disable auto-connect features for Wi-Fi on your devices
5. Use your mobile data connection instead of public Wi-Fi for sensitive transactions
6. Forget public networks after using them

> *Tip: Some VPN services offer free versions with limited data, which can be sufficient for occasional sensitive transactions on public Wi-Fi.*

Recommended Resources:

- FTC advice on public Wi-Fi: consumer.ftc.gov
- VPN comparison sites: CNET, PCMag, Consumer Reports

Recognize and Avoid Phishing Attempts Moderate

What it is:

Developing the skills to identify and avoid fraudulent communications attempting to steal personal information or account credentials.

Why it matters:

Phishing is one of the most common ways identity thieves obtain personal information, often by impersonating trusted companies or creating a false sense of urgency that leads victims to share sensitive data.

How to implement:

1. Be suspicious of unexpected emails or messages, especially those creating urgency
2. Check sender email addresses carefully for subtle misspellings (e.g., amaz0n.com vs amazon.com)
3. Hover over links before clicking to preview the actual destination URL
4. Don't click on links in suspicious messages—instead, navigate directly to the company's website
5. Be wary of messages with generic greetings, poor grammar, or spelling errors
6. Never provide sensitive information in response to an unsolicited email or message
7. Report phishing attempts to the organization being impersonated and to phishing@uce.gov

> *Tip: If you're unsure about a communication, contact the company directly using contact information from their official website, not from the suspicious message.*

Recommended Resources:

- Phishing examples: consumer.ftc.gov
- Phishing quiz: phishingquiz.withgoogle.com

Physical Document Protection Strategies

Shred Sensitive Documents Easy

What it is:

Destroying documents containing personal information before disposal to prevent dumpster diving.

Why it matters:

Discarded documents like bank statements, credit card offers, utility bills, and medical statements contain valuable personal information that identity thieves can use to access your accounts or open new ones in your name.

How to implement:

1. Purchase a cross-cut or micro-cut shredder (more secure than strip-cut shredders)
2. Shred documents containing:
   - Social Security numbers
   - Account numbers
   - Birthdates
   - Signatures
   - Pre-approved credit offers
   - Medical statements
   - Pay stubs
   - Tax documents
   - Utility bills
   - Expired ID cards
3. For items that can't be shredded, like credit cards, cut them into multiple pieces
4. Consider community shredding events if you don't have a shredder

> *Tip: If you don't have a shredder, many office supply stores, shipping centers, and banks offer shredding services for a small fee.*

Secure Your Mail Easy

What it is:

Taking steps to protect incoming and outgoing mail from theft.

Why it matters:

Mail theft is a common source of identity theft, as mail often contains sensitive information like bank statements, tax documents, and credit card offers. Thieves may also steal mail to obtain new credit cards or checks sent to you.

How to implement:

1. Use a locked mailbox or a mail slot that deposits mail directly into your home
2. Collect mail promptly after delivery
3. Put a hold on mail delivery when traveling (USPS Hold Mail Service)
4. Drop outgoing mail containing sensitive information directly at the post office or in a secure collection box
5. Consider using a P.O. Box for receiving sensitive mail
6. Sign up for Informed Delivery from USPS to receive daily emails showing what mail is scheduled for delivery
7. Switch to electronic statements and payments where possible to reduce sensitive mail

> *Tip: If you see unknown transactions on your accounts or stop receiving certain regular mail, it could be a sign of mail theft. Report suspected mail theft to the U.S. Postal Inspection Service at 1-877-876-2455.*

Recommended Resources:

- USPS Informed Delivery: informeddelivery.usps.com
- USPS Hold Mail Service: holdmail.usps.com

Secure Physical Documents Moderate

What it is:

Properly storing important documents to prevent unauthorized access and theft.

Why it matters:

Physical documents containing sensitive information can be stolen during home break-ins or by visitors, contractors, or even family members with access to your home. Proper storage prevents this source of identity theft.

How to implement:

1. Store important documents in a fireproof, lockable safe or file cabinet, including:
   - Social Security cards
   - Birth certificates
   - Passports
   - Tax returns
   - Financial statements
   - Medical records
   - Property deeds
   - Insurance policies
2. Keep only what you need—securely destroy outdated documents
3. Consider digital backup of important documents, encrypted and password-protected
4. For extremely important documents like birth certificates, consider a bank safe deposit box
5. Take inventory of what documents you have and where they are stored
6. Limit who has access to areas where sensitive documents are stored

> *Tip: Create a document retention schedule—keep tax records for 7 years, pay stubs until you receive your W-2, and receipts for major purchases as long as you own the items.*

Monitoring Strategies

Monitor Financial Statements Easy

What it is:

Regularly reviewing bank statements, credit card statements, and financial accounts to detect unauthorized transactions quickly.

Why it matters:

Early detection of fraudulent activity limits damage and simplifies the recovery process. Most financial institutions limit your liability for unauthorized transactions if they're reported promptly.

How to implement:

1. Review all bank and credit card statements as soon as they arrive
2. Set up online account access to check transactions more frequently
3. Enable transaction alerts for all accounts (email or text notifications for large purchases, foreign transactions, or when your balance falls below a certain amount)
4. Keep receipts and match them against statement charges
5. Check account balances weekly to catch unauthorized activity
6. Report suspicious transactions immediately
7. Create a schedule for regular account review (e.g., every Sunday evening)

> *Tip: Pay special attention to small charges—identity thieves often make small test purchases to verify a stolen card works before making larger purchases.*

Check Credit Reports Regularly Moderate

What it is:

Reviewing your credit reports from all three major credit bureaus to detect unauthorized accounts, inquiries, or other suspicious activity.

Why it matters:

Your credit report shows all accounts opened in your name, so it can reveal identity theft that might not be visible on your existing account statements, such as new accounts opened by thieves.

How to implement:

1. Request free credit reports from all three major credit bureaus (Equifax, Experian, and TransUnion) through the official site AnnualCreditReport.com
2. Check each report for:
   - Accounts you didn't open
   - Credit inquiries you didn't authorize
   - Addresses where you've never lived
   - Employers you haven't worked for
   - Incorrect personal information
   - Public records you don't recognize
3. Stagger your requests throughout the year (one bureau every four months) for more frequent monitoring
4. Create a calendar reminder for when to request each report
5. Report any discrepancies immediately to the credit bureau and affected creditors

> *Tip: During COVID-19, the credit bureaus offered free weekly online reports instead of annual ones. Check AnnualCreditReport.com for the most current availability.*

Recommended Resources:

- AnnualCreditReport.com (official site): annualcreditreport.com
- FTC credit report guide: consumer.ftc.gov

Consider a Credit Freeze Advanced

What it is:

A security measure that restricts access to your credit report, preventing most lenders from accessing it without your explicit permission.

Why it matters:

Since most creditors need to check your credit report before approving new accounts, a credit freeze helps prevent identity thieves from opening new accounts in your name, even if they have your personal information.

How to implement:

1. Contact each of the three major credit bureaus separately to place a freeze:
    - Equifax: 1-888-766-0008 or equifax.com/personal/credit-report-services
    - Experian: 1-888-397-3742 or experian.com/freeze
    - TransUnion: 1-888-909-8872 or transunion.com/credit-freeze
2. Be prepared to provide your name, address, date of birth, Social Security number, and other personal information
3. Create a PIN or password for each bureau to use when you want to lift the freeze
4. Store these PINs securely
5. Temporarily lift the freeze when applying for credit or services that require a credit check
6. Remember to allow several days for freezes to be lifted when planning credit applications

> *Tip: Credit freezes are now free nationwide. Consider also freezing the credit reports of your children to protect them from child identity theft.*

Recommended Resources:

- FTC guide to credit freezes: consumer.ftc.gov

Creating Your Custom Protection Plan

To develop an effective identity theft protection plan:

1. Assess your current vulnerabilities and habits
2. Select strategies from each category (digital, physical, monitoring)

3. Start with a few easy strategies and gradually implement more
4. Create a schedule for recurring protection activities
5. Review and update your protection plan regularly

Remember that consistent implementation of a few strategies is more effective than inconsistent implementation of many strategies.