Personal Identity Protection Plan

Your Customized Strategy to Prevent Identity Theft

This template will help you create a comprehensive plan to protect your personal information and reduce the risk of identity theft. Fill in each section with your specific strategies and information. Keep this plan in a secure location and review it at least once a year to ensure it remains current.

Personal Information Inventory

Create an inventory of accounts and personal information that need protection. This helps you identify what needs to be monitored and secured.

Date Created/Updated:

Financial Accounts to Monitor

Account Type	Institution	Monitoring Method	Frequency
e.g., Checking Account	e.g., First National Bank	e.g., Mobile app alerts	e.g., Weekly

Identity Documents to Protect

Document Type	Storage Location	Security Measures
e.g., Social Security Card	e.g., Home safe	e.g., Locked, limited access
e.g., Birth Certificate		

Document Type	Storage Location	Security Measures
e.g., Passport		

Digital Security Strategies

Document your strategies for protecting your digital presence and online accounts.

Password Management Strategy:

Describe how you create, store, and manage your passwords. Example: Use a password manager to generate and store unique passwords for each account.

Two-Factor Authentication Plan:

List which accounts have 2FA enabled and which ones still need it. Example: Enabled on email, banking, and social media accounts.

Account Security Checklist

- [ ] Use a password manager
- [ ] Unique password for each account
- [ ] Passwords 12+ characters
- [ ] Two-factor authentication on email
- [ ] Two-factor authentication on financial accounts
- [ ] Secure mobile phone with password/biometrics
- [ ] Automatic software updates enabled
- [ ] Security questions use non-public answers
- [ ] Use secure, private Wi-Fi network
- [ ] Use VPN when on public Wi-Fi

Device Security Plan:

Describe how you secure your computers, phones, and other devices. Example: Lock screen PIN on all devices, encryption enabled on laptop, regular software updates.

Social Media Privacy Settings:

Document your privacy settings on social media platforms. Example: Facebook - Friends only can see posts, limited personal information shared publicly, location sharing disabled.

Physical Document Security

Outline your strategies for protecting physical documents and information.

Mail Security Practices:

Describe how you secure incoming and outgoing mail. Example: Use a locked mailbox, collect mail promptly, sign up for Informed Delivery from USPS.

Document Disposal Methods:

Describe how you dispose of sensitive documents. Example: Cross-cut shredder for any documents with personal information, shred credit card offers immediately.

Secure Storage Solutions:

Describe where and how you store important documents. Example: Fireproof home safe for vital documents, locked filing cabinet for financial statements.

Physical Security Checklist

- [ ] Secure mailbox or PO box
- [ ] Cross-cut shredder for documents
- [ ] Fireproof safe for vital documents
- [ ] Mail held when traveling
- [ ] Limited access to home office/files
- [ ] USPS Informed Delivery service
- [ ] Minimal documents carried in wallet/purse
- [ ] Opt out of paper statements when possible

Monitoring and Prevention Plan

Establish a regular schedule for monitoring your accounts and credit.

Credit Report Monitoring Schedule:

Describe your plan for checking credit reports. Example: Check one bureau every 4 months via AnnualCreditReport.com (Equifax in January, Experian in May, TransUnion in September).

Financial Account Review Schedule:

Describe how often you review your financial accounts. Example: Weekly check of banking transactions, monthly review of credit card statements, quarterly review of investment accounts.

Credit Freeze Status:

Document your credit freeze status with each bureau. Example: Credit freezes active with all three bureaus, PINs stored in password manager.

Credit Monitoring Services:

List any credit monitoring services you use. Example: Credit Karma for TransUnion and Equifax monitoring, free monitoring through credit card company.

Monitoring Checklist

- [ ] Regular credit report checks
- [ ] Credit freezes in place
- [ ] Account alerts for large transactions
- [ ] Credit/debit card activity alerts
- [ ] Opted out of pre-approved credit offers
- [ ] Annual check of medical records/benefits
- [ ] Review Social Security statement annually
- [ ] Check tax records/refund status yearly

Response Plan

Prepare a plan of action in case identity theft occurs despite your prevention efforts.

Important Contact Information:

List key contact information for banks, credit card companies, credit bureaus, etc. Example: ABC Bank Fraud Department: 1-800-123-4567, Account #: XXX1234 (last 4 digits only).

Immediate Response Actions:

List specific steps you will take if you discover identity theft. Example: 1) Contact affected company, 2) Place fraud alert, 3) Report to FTC at IdentityTheft.gov, etc.

Key Response Resources:

- **FTC Identity Theft Report:** IdentityTheft.gov or 1-877-438-4338
- **Credit Bureaus:**
  - Equifax: 1-800-685-1111 or equifax.com
  - Experian: 1-888-397-3742 or experian.com
  - TransUnion: 1-888-909-8872 or transunion.com
- **To place a fraud alert:** Contact one credit bureau (they'll notify the others)
- **To place a credit freeze:** Contact each bureau individually

Annual Review Schedule

Set a schedule to review and update this plan regularly to ensure it remains current.

Plan Review Dates:

Set specific dates to review this plan each year. Example: I will review and update this plan every January 15th and July 15th.

Date Reviewed	Changes Made	Next Review Date

Keep this plan in a secure location and update it regularly.