

# Fraud Vulnerability Assessment

---

Complete this assessment to identify your personal risk factors for different types of fraud and develop a customized protection plan.

## Part 1: Personal Vulnerability Assessment

Answer each question honestly to assess your vulnerability to different types of fraud.

### 1. Password Management

How do you manage your passwords for different accounts?

- I use the same password (or minor variations) for most or all of my accounts
- I have a few different passwords that I rotate between accounts
- I use unique passwords for financial/important accounts, but may reuse passwords for less critical sites
- I use a different, strong password for every account (or use a password manager)

### 2. Two-Factor Authentication

Do you use two-factor authentication (2FA) for your accounts?

- I don't use 2FA on any accounts
- I only use 2FA when it's required by the service
- I use 2FA on my financial accounts but not on other accounts
- I use 2FA on all accounts that offer it

### 3. Email Habits

How do you typically handle emails from unknown senders or with suspicious content?

- I open emails and attachments without much concern
- I'm cautious with attachments but often click on links in emails

- I avoid clicking on links or opening attachments from unknown senders
- I verify the sender and hover over links to check destinations before clicking, even from known senders

## 4. Social Media Privacy

How do you manage your social media privacy settings and information sharing?

- My profiles are public and I share personal details freely (birthdate, location, phone, etc.)
- My profiles are somewhat restricted but I still share personal milestones and information
- I have privacy settings enabled but accept friend/connection requests from people I don't know well
- I have strict privacy settings, limit personal information shared, and only connect with people I know

## 5. Financial Monitoring

How frequently do you review your financial statements and credit reports?

- I rarely check my financial statements or credit reports
- I occasionally check my bank statements but rarely review my credit report
- I regularly check my bank statements and review my credit report annually
- I monitor my financial accounts weekly and check my credit report several times a year

## 6. Public Wi-Fi Usage

How do you use public Wi-Fi networks?

- I regularly access financial accounts and make purchases on public Wi-Fi
- I sometimes log into sensitive accounts on public Wi-Fi when necessary
- I use public Wi-Fi but avoid accessing financial accounts or entering sensitive information
- I use a VPN when on public Wi-Fi or avoid public Wi-Fi entirely for sensitive activities

## **7. Phone Security**

How do you secure your smartphone?

- I don't use any passcode or biometric security on my phone
- I use a simple passcode (like 1234) or pattern lock
- I use a complex passcode or biometric security (fingerprint/face recognition)
- I use biometric security plus a strong passcode and keep my phone updated

## **8. Response to Unexpected Contacts**

How do you typically respond to unexpected calls, texts, or emails claiming to be from your bank, a government agency, or tech support?

- I usually respond and provide requested information if they seem legitimate
- I sometimes respond, especially if the issue seems urgent
- I'm generally suspicious but might respond if it seems very convincing
- I never respond directly - instead, I contact the organization through official channels I verify independently

## **9. Software Updates**

How do you handle software updates on your devices?

- I often ignore or delay updates indefinitely
- I eventually update when I'm reminded repeatedly
- I update most software regularly but may delay some updates
- I install security updates promptly and have automatic updates enabled when possible

## **10. Personal Information Protection**

How do you handle documents containing sensitive personal information?

- I throw them away without much thought

- I sometimes tear them up before throwing them away
  - I shred documents with sensitive information
  - I shred all documents with personal information and regularly purge digital records I don't need
- 

## Part 2: Vulnerability Profile Analysis

Based on your answers to the assessment questions, analyze your vulnerability profile in the key risk areas below.

### Account Security

**High Risk** **Medium Risk** **Low Risk**

Based on your password management and two-factor authentication practices (Questions 1-2)

### Online Behavior

**High Risk** **Medium Risk** **Low Risk**

Based on your email habits, public WiFi usage, and response to unexpected contacts (Questions 3, 6, 8)

### Information Sharing

**High Risk** **Medium Risk** **Low Risk**

Based on your social media privacy and document handling practices (Questions 4, 10)

### Monitoring & Maintenance

**High Risk** **Medium Risk** **Low Risk**

Based on your financial monitoring and software update practices (Questions 5, 9)

### Device Security

**High Risk** **Medium Risk** **Low Risk**

Based on your phone security practices (Question 7)

**Instructions:** Circle your risk level for each category based on your assessment responses. Focus on addressing "High Risk" areas first in your action plan.

## Part 3: Personalized Protection Recommendations

### Account Security Recommendations

**For High Risk:** Implement a password manager to create and store unique, strong passwords for all accounts. Enable two-factor authentication on all accounts that offer it, especially financial and email accounts.

**For Medium Risk:** Audit your existing passwords and update any that are weak or reused across multiple accounts. Enable two-factor authentication on your most sensitive accounts.

**For Low Risk:** Continue using unique passwords and 2FA. Consider using hardware security keys for maximum protection on critical accounts.

### Online Behavior Recommendations

**For High Risk:** Adopt a strict policy of never clicking links in unsolicited emails. Avoid conducting sensitive transactions on public WiFi. Always independently verify the identity of anyone contacting you about financial matters.

**For Medium Risk:** Hover over links to check destinations before clicking. Use a VPN when on public WiFi. Develop a verification process for unexpected communications.

**For Low Risk:** Maintain your cautious approach. Stay informed about new phishing tactics. Consider using email filtering tools for added protection.

## Information Sharing Recommendations

**For High Risk:** Review and restrict social media privacy settings. Limit personal information shared online. Start shredding documents with sensitive information. Be selective about friend/connection requests.

**For Medium Risk:** Audit your social media profiles to remove unnecessary personal details. Establish a system for securely storing or destroying sensitive documents.

**For Low Risk:** Periodically review your digital footprint and continue minimizing unnecessary information sharing.

## Monitoring & Maintenance Recommendations

**For High Risk:** Set up weekly reviews of financial accounts. Check your credit report from all three bureaus. Enable automatic software updates on all devices.

**For Medium Risk:** Create a schedule for regular financial monitoring. Set reminders to check your credit report three times a year. Prioritize security-related software updates.

**For Low Risk:** Consider using credit monitoring services for real-time alerts. Maintain your regular monitoring schedule.

## Device Security Recommendations

**For High Risk:** Set up strong passcodes and biometric security on all devices. Enable remote wiping capabilities. Install and configure reputable security software.

**For Medium Risk:** Strengthen existing security measures. Review app permissions on your devices. Enable automatic screen locking after short periods of inactivity.

**For Low Risk:** Maintain current security practices. Consider advanced protection like app-level security or encryption for sensitive data.

## Part 4: Personal Fraud Protection Action Plan

Based on your vulnerability profile and the recommendations, create your personalized action plan below. Focus on your highest risk areas first.

Risk Area	Current Risk Level	Action Steps	Priority	Target Date
Account Security	[H/M/L]		[H/M/L]	
Online Behavior	[H/M/L]		[H/M/L]	
Information Sharing	[H/M/L]		[H/M/L]	
Monitoring & Maintenance	[H/M/L]		[H/M/L]	
Device Security	[H/M/L]		[H/M/L]	

### Implementation Notes

## Progress Review Plan

When and how will you review your progress on this action plan?

## Additional Resources

- [IdentityTheft.gov](#) - Recovery plans and prevention tips from the FTC
- [FTC Identity Theft Resources](#) - Comprehensive guide to preventing identity theft
- [National Cybersecurity Alliance](#) - Tips and resources for online safety
- [AnnualCreditReport.com](#) - Free credit reports from all three bureaus
- [FTC Guide to Identity Theft Protection Services](#) - Information about monitoring services