Fraud Protection Checklist

Use this comprehensive checklist to protect yourself from common types of consumer fraud. Items are organized by priority to help you focus on the most important protection measures first.

How to use this checklist: Check off items as you complete them. Start with high-priority items (red border), then progress to medium-priority (orange border) and low-priority (green border) items. Schedule regular reviews of this checklist to maintain your protection.

Account Security

- [ ] **Enable two-factor authentication on financial accounts** High Priority

  Set up two-factor authentication (2FA) on all bank, credit card, investment, and payment app accounts. This adds an extra layer of security by requiring a second verification method beyond your password.

- [ ] **Use unique passwords for financial accounts** High Priority

  Create strong, unique passwords for each financial account. Never reuse passwords across multiple accounts, especially for banking, credit cards, or investment platforms.

- [ ] **Secure your email account** High Priority

  Enable 2FA on your email account and use a strong, unique password. Your email is often the recovery method for other accounts, making it a prime target for hackers.

- [ ] **Use a password manager** Medium Priority

  Implement a reputable password manager to generate, store, and manage strong, unique passwords for all your accounts. This makes it practical to use different passwords for every service.

- [ ] **Set up login alerts** Medium Priority

  Configure notifications for account logins where available. This allows you to quickly identify unauthorized access attempts.

- [ ] **Regularly update security questions and answers** Low Priority

  Periodically review and update security questions for your accounts. Avoid using answers that could be easily found on social media or through public records.

Financial Monitoring

- [ ] **Review financial statements weekly** High Priority

  Check bank and credit card statements at least weekly to identify unauthorized transactions. Report any suspicious activity immediately to your financial institution.

- [ ] **Check your credit reports regularly** High Priority

  Review your credit reports from all three major bureaus (Equifax, Experian, and TransUnion) at least once every four months. You're entitled to one free report from each bureau annually through AnnualCreditReport.com.

- [ ] **Set up transaction alerts** Medium Priority

  Configure notifications for transactions above a certain amount or for specific types of transactions (e.g., online purchases, international transactions).

- [ ] **Consider a credit freeze** Medium Priority

  Place a credit freeze with all three major credit bureaus to prevent new credit accounts from being opened in your name. This can be especially important if you're not actively applying for credit.

- [ ] **Evaluate credit monitoring services** Low Priority

  Consider using a credit monitoring service that provides real-time alerts for changes to your credit report, suspicious activity, or potential identity theft.

Online Behavior

- [ ] **Never click links in unsolicited emails** High Priority

  Avoid clicking links in unexpected emails, especially those claiming to be from financial institutions, government agencies, or companies you do business with. Instead, navigate to the organization's website directly by typing the URL in your browser.

- [ ] **Verify communications through official channels** High Priority

  If you receive a message claiming to be from your bank, a government agency, or another organization, contact them directly using the phone number on their official website or the back of your credit/debit card to verify its authenticity.

- [ ] **Use secure, encrypted connections** Medium Priority

  Ensure websites use HTTPS (look for a padlock icon in the address bar) before entering personal or financial information. Avoid conducting sensitive transactions on public WiFi networks.

- [ ] **Be cautious with downloads** Medium Priority

  Only download files and applications from trusted sources. Be especially wary of email attachments, even if they appear to come from someone you know.

- [ ] **Use a VPN for sensitive transactions** Low Priority

  Consider using a Virtual Private Network (VPN) when accessing financial accounts or conducting sensitive transactions, especially when using public WiFi networks.

Device Security

- [ ] **Keep devices updated** High Priority

  Install security updates for your operating system, browsers, and apps promptly. These updates often patch security vulnerabilities that could be exploited by fraudsters.

- [ ] **Secure your mobile devices** High Priority

  Enable strong passcodes, facial recognition, or fingerprint authentication on all devices. Configure automatic screen locking after a short period of inactivity.

- [ ] **Install reputable security software** Medium Priority

  Use trusted antivirus and anti-malware software on your devices. Enable regular scans to detect and remove potential threats.

- [ ] **Review app permissions** Medium Priority

  Regularly review the permissions granted to apps on your devices. Remove unnecessary apps and limit permissions to only what each app needs to function.

- [ ] **Enable remote wiping capabilities** Low Priority

  Set up the ability to remotely erase data from your devices if they are lost or stolen (e.g., Find My iPhone for Apple devices, Find My Device for Android).

Information Sharing

- [ ] **Limit personal information on social media** High Priority

  Review your social media privacy settings and limit the personal information you share publicly. Avoid posting details that could be used to answer security questions or steal your identity (birth date, hometown, schools attended, etc.).

- [ ] **Shred sensitive documents** High Priority

  Use a cross-cut shredder to destroy documents containing personal information before discarding them, including financial statements, pre-approved credit offers, and medical records.

- [ ] **Be cautious with mail** Medium Priority

  Collect mail promptly and consider using a locked mailbox or post office box. Put a hold on mail delivery when traveling. Opt for electronic statements where possible.

- [ ] **Review data sharing settings** Medium Priority

  Regularly review and adjust privacy settings on financial accounts, shopping websites, and apps to limit data sharing and marketing use of your information.

- [ ] **Opt out of pre-screened credit offers** Low Priority

  Visit OptOutPrescreen.com or call 1-888-5-OPTOUT to stop receiving pre-approved credit card and insurance offers by mail, which can be a target for identity thieves.

Education and Awareness

- [ ] **Stay informed about current scams** High Priority

  Regularly check reliable sources like the FTC Consumer Information website (consumer.ftc.gov) or sign up for scam alerts to stay updated on new and emerging fraud tactics.

- [ ] **Educate family members** Medium Priority

  Share fraud prevention strategies with family members, especially those who may be more vulnerable to scams like elderly relatives or younger siblings.

- [ ] **Report scams** Low Priority

  Report suspected scams to the appropriate authorities such as the FTC (reportfraud.ftc.gov), the FBI's Internet Crime Complaint Center (IC3.gov), or your state attorney general's office.

Emergency Response Plan

- [ ] **Create a contact list for fraud reporting** High Priority

  Compile contact information for your financial institutions, credit bureaus, and fraud reporting agencies so you can act quickly if you suspect fraud or identity theft.

- [ ] **Know the steps to take if you're a victim** Medium Priority

  Familiarize yourself with immediate actions to take if you suspect fraud, including contacting financial institutions, placing fraud alerts, filing reports, and documenting all communications.

- [ ] **Create a system for tracking fraud resolution** Low Priority

  Develop a method to document all fraud-related communications, including dates, contact names, and action items to help streamline the resolution process if fraud occurs.

Key Resources

- **FTC Identity Theft Website:** IdentityTheft.gov
- **Free Credit Reports:** AnnualCreditReport.com
- **FTC Scam Alerts:** consumer.ftc.gov/features/scam-alerts
- **Report Fraud:** ReportFraud.ftc.gov
- **Credit Bureau Fraud Alerts:**
  - Equifax: 1-800-525-6285
  - Experian: 1-888-397-3742
  - TransUnion: 1-800-680-7289

Remember: Fraud prevention is an ongoing process, not a one-time action. Schedule quarterly reviews of this checklist to ensure your protection measures remain current and effective. Adapt your protection strategies as technology, personal circumstances, and fraud tactics evolve.