OSCPA
Oklahoma Society of CPAs

PROTECTING YOURSELF FROM FRAUD AND SCAMS

Scammers, fraudsters, and bad actors are constantly evolving their tactics to steal personal information and money from unsuspecting consumers. This guide provides an overview of common scams, identity theft risks, and fraud prevention strategies to help protect yourself and your family.

Common Ways Criminals Steal from You

Scams have adapted to modern technology, making them harder to detect. According to the Federal Trade Commission (FTC), thousands of fraud cases are reported each year. Here are the six most common methods criminals use to scam consumers:

Phone Scams

- Scammers use spoofing software to make calls appear legitimate.
- They often pose as government agencies, charities, or financial institutions.

Tip: Never share personal information or bank account details over the phone.

Internet Scams

- Social media quizzes can collect personal details used for security breaches.
- Fake crowdfunding pages or charity scams trick people into donating.

Tip: Ensure websites are secure (https://) before entering sensitive data.

Email Phishing

- Fraudulent emails mimic trusted organizations or people to steal information.

Tip: Never click on suspicious links or download unknown attachments.

Malicious Apps & Software

- Free apps can install malware on your device.

Tip: Always check developer legitimacy before downloading.

Text Message Scams (Smishing)

- Spam texts may include malicious links that install malware.

Tip: Do not respond to unknown senders and report spam by forwarding suspicious texts to 7726 (SPAM).

Credit Card Skimmers

- Skimmers at ATMs and gas pumps steal card information using attached devices.

Tip: Inspect card readers for tampering before using.

Exploring Identity Theft

Identity theft is a serious crime that can go undetected for years. It's estimated that over 1.3 million children are victims of identity theft annually. Here's how to recognize and prevent it:

Warning Signs of Identity Theft

- Unexpected bills or collection notices addressed to you or your child.
- Denied credit applications due to unknown accounts.
- IRS notices for unfiled taxes under your name.

Protecting Yourself and Your Children

- Regularly check credit reports with Equifax, Experian, and TransUnion.
- Use strong passwords and enable two-factor authentication.
- Shred documents containing personal information.
- Be cautious about sharing Social Security numbers.

Recovering from Identity Theft

- File a police report and report fraud to the FTC (identitytheft.gov).
- Notify financial institutions and request credit freezes if needed.
- Update all passwords and monitor accounts for unusual activity.

What You Need to Know about Utility Scams

Utility scams have become increasingly common, tricking consumers into making fraudulent payments under the threat of service disconnection.

How Utility Scams Work

- Scammers pose as utility representatives, calling from spoofed numbers.
- They demand immediate payment via prepaid debit cards or wire transfers.
- Some even visit homes, claiming to be from the utility company.

Protecting Yourself from Utility Scams

- Utility companies never demand immediate payment through prepaid cards.
- Always verify account details by calling the utility company directly.
- Report suspicious calls or visits to local authorities.

6 Tips to Keep You Safe When Shopping Online

With online shopping booming, it's crucial to ensure your financial data is secure. Follow these steps to shop safely:

1. Verify the Company and Website

- Research businesses on independent websites like bizrate.com and bbb.org.
- When in doubt, buy from reputable companies you trust.

2. Look for Signs of Security

- Ensure websites use "https" and have a padlock icon in the address bar.
- Keep your web browser updated for added security.

- Avoid using public Wi-Fi when possible.

3. Be Skeptical of Deals That Seem Too Good

- Unrealistically low prices can be a red flag for scams.
- Paying slightly more from a trusted site is safer than risking a fraudulent purchase.

4. Use Secure Payment Methods

- Credit cards offer better fraud protection than debit cards.
- Consider using PayPal, Venmo, Apple Pay, or virtual credit cards for added security.

5. Safeguard Your Passwords

- Use complex passwords combining letters, numbers, and symbols.
- Consider using a password manager to generate and store secure passwords.

6. Review Your Statements Regularly

- Check your credit card and bank statements for unauthorized transactions.
- If you spot suspicious charges, report them to your card issuer immediately.

Tips to Stay Safe and Prevent Fraud

Taking proactive measures can help protect you from becoming a victim of fraud. Here are some best practices:

- Monitor financial accounts regularly for unauthorized transactions.
- Never share sensitive information over the phone or email.
- Enable fraud alerts on bank accounts and credit cards.
- Keep personal information private on social media.
- Stay informed about new scams by following trusted sources like the FTC.

By staying vigilant and educated, you can significantly reduce the risk of falling victim to scams and identity theft. If you suspect fraud, report it immediately to the appropriate authorities.

Identity Theft Recovery Checklist

If you suspect or confirm that you have been a victim of identity theft, take these immediate steps to repair the damage and prevent further harm.

- [ ] **Act Quickly**
  - Time is critical when dealing with identity theft. Begin the recovery process as soon as you notice any suspicious activity.

- [ ] **File a Police Report (if applicable)**
  - Report identity theft to your local law enforcement agency.
  - Request a copy of the police report to provide to financial institutions and credit bureaus, as needed.

- [ ] **Notify All Financial Institutions Involved**
  - Contact your bank and credit card issuers to report unauthorized transactions.
  - Request to close or freeze compromised accounts.
  - Ask for new account numbers and debit/credit cards if needed.

- [ ] **File Your Taxes as Early as Possible**
  - If someone has used your Social Security number for fraudulent tax returns, early filing can prevent tax fraud.
  - Report tax-related identity theft to the IRS at identitytheft.gov or call (800) 908-4490.

- [ ] **Create an Identity Theft File**
  - Keep copies of all reports, emails, letters, and conversations related to your case.
  - Document every action taken, including dates and contact information.

- [ ] **Change All Passwords**
  - Update passwords for all financial, email, and online shopping accounts.
  - Use strong, unique passwords and enable two-factor authentication where possible.

- [ ] **Obtain New Credit Cards and Destroy Old Ones**
  - Request replacement credit and debit cards from your financial institutions.
  - Cut up and securely dispose of old cards.

- [ ] **Monitor Unusual Activity**
  - Keep an eye on your mail for unfamiliar bills or collection notices.
  - Regularly check your Social Security account for unauthorized claims.
  - Review your health insurance statements for fraudulent medical charges.

- [ ] **Contact the Three Credit Reporting Agencies**
  - Request a credit report from each agency and review it for fraudulent accounts:
    - Equifax (www.equifax.com)
    - Experian (www.experian.com)
    - TransUnion (www.transunion.com)
  - Ask them to remove any fraudulent files associated with your child's Social Security number, if applicable.

- [ ] **Place a Fraud Alert on Your Credit Report**
  - Contact one of the three credit bureaus to place a fraud alert, which lasts for one year and makes it harder for fraudsters to open new accounts in your name.

☐ **File a Fraud Report with the FTC**

- Submit a report at identitytheft.gov or call (877) 438-4338.
- Use the FTC Identity Theft Affidavit to dispute fraudulent accounts.

Fraud Prevention Checklist

Protect yourself from scams and fraud by following these essential steps:

- [ ] **Register with the National Do Not Call Registry**
  - Register your number on the **National Do Not Call Registry** at donotcall.gov or by calling (888) 382-1222.

- [ ] **Create Spam Filters for Your Inbox**
  - Create spam filters using your email settings to minimize fraudulent emails.

- [ ] **Delete Mobile Apps and Update App Permissions**
  - Check app permissions—if an app requests unnecessary access (e.g., a flashlight app asking for contacts), avoid it.

- [ ] **Report Suspicious Text Messages**
  - If you receive a suspicious message, forward it to 7726 (SPAM) to report it.

- [ ] **Set Up Fraud Alerts for Your Credit Cards**
  - Set up fraud alerts with your bank and credit card providers. Review your statements regularly for unauthorized transactions.
  - You can also explore freezing or locking accounts you no longer use or require a passcode before completing purchases.

- [ ] **Report Fraud Immediately**
  - If you suspect fraud, report it to the Federal Trade Commission (FTC) at ReportFraud.ftc.gov.
  - Contact your bank and credit card companies to report fraudulent transactions.
  - Place a fraud alert on your credit report through Equifax, Experian, or TransUnion.

By following these steps, you can significantly reduce your risk of falling victim to scams and fraud. Stay vigilant, educate yourself, and report suspicious activities to protect yourself and others.

Identity Theft Prevention Checklist

Take these steps to protect yourself and your family from identity theft:

- [ ] **Secure Personal Information**
  - Store important documents in a safe location.
  - Use a crosscut or microcut shredder for sensitive papers.
  - Do not share Social Security numbers unless necessary and with a trusted party.
  - Ask how schools and medical offices store and dispose of you or your child's information.

- [ ] **Monitor Financial and Credit Activity**
  - Regularly check your bank and credit card statements for unusual activity.
  - Obtain a credit report for your child before they turn 16 to catch fraud early.
  - Freeze your credit with credit bureaus to prevent unauthorized accounts.

- [ ] **Protect Online Privacy**
  - Teach children to keep personal details off social media.
  - Avoid sharing full birth dates, school names, pet names, or other security question answers online.
  - Secure your computer and mobile device with strong passwords and update software regularly.
  - Never open email attachments or click links from unknown sources.

- [ ] **Enhance Home Security**
  - Keep wallets, ID cards, and credit cards in a secure place.
  - Shred all documents containing sensitive information before disposal.
  - Do not give out personal information over the phone unless you initiated the call to the business's confirmed phone number.

- [ ] **Additional Protection Measures**
  - Mark "Photo ID Required" on the back of credit cards.
  - Destroy unwanted credit card offers to prevent fraudsters from using them.
  - Before giving out your Social Security number, ask why it's needed and if an alternative identifier is available.

By staying vigilant and proactive, you can minimize the risk of identity theft and fraud.