Preventing Identity Theft

In today's uber-connected online world, the risk of identity theft is hard to avoid. But there are ways to minimize identity theft risks and stay ahead of scammers and thieves who want your personal information.

Know the Risks

According to the Pew Research Center, nearly 30% of Americans were impacted by at least one of three kinds of major identity theft within the previous 12 months of being surveyed. The most common was fraudulent charges on their credit or debit card (21%), while 8% had someone take over their social media or email without their permission, and 6% had someone try to open a credit card or get a loan in their name.

Unfortunately, when scammers assume your identity, you may be liable for their debts and charges, or out whatever cash was spent.

Use Credit Card Protections

Use credit cards to limit your cash liability. Most credit card companies have zero-liability fraud protection policies, and federal law limits cardholder liability to $50, no matter how much was charged.

To benefit from this fraud protection, you need to report changes within 30 days. Make it a habit to regularly review transactions on your statements and immediately report any unauthorized purchases or transactions. It can be a hassle to deal with these issues, even if you aren't on the hook for charges. Better to minimize the risk with identity theft best practices.

- Be cautious about giving anyone, including friends and family, your key numbers and other financial information. Even if you can trust them with this info, they may be less careful with it than you.
- Choose unique PINs. Avoid using your Social Security number, birthdate, or variations that are easy to guess.
- Don't keep your PIN written down in your wallet.
- Keep a list of your relevant account numbers in a secure place. Include details on how to cancel or suspend cards if you lose them or suspect fraudulent activity.
- Tear up or shred receipts and bills before you throw them away.

Look for Security Signs

Before you shop or otherwise engage with a website, check for important security safeguards. Reputable companies use an SSL certificate to verify the website's identity and provide an encrypted connection.

Checking for an SSL certificate is simple—look for a lock symbol to the left of the company name and "https" in the URL.

Watch Your Links

Phishing links often imitate legitimate companies or websites as a way to procure your personal information. Before you click any link or attachment—even those from companies or people you know and trust—check for typos, misspellings, or other red flags. It's possible they were hacked and the link will allow scammers to access your info or download a virus to your device.

Be wary of pushy calls-to-action or limited-time offers that require your personal information. Deals that seem too good to be true often are.

Telemarketing Traps

Offers of free trips, discounted magazine subscriptions, and the like are the most common form of telemarketing. Sometimes, these calls are legit. Other times…not so much.

Fraudulent phone calls were the second-highest contact method used in fraud reports, according to the Federal Trade Commission (FTC) Consumer Sentinel Network. (Text was no.1). This category accounted for $203 million in money lost, with a median loss of $1,500.

Telemarketing fraud impacts all ages, but it's the top contact method for fraud reports for people ages 70-79 and 80 and older. The most common scams include business imposters, tech support scams, prizes, sweepstakes and lotteries, and government imposters.

If you receive an unsolicited phone call from a company you don't know, ask them to send you information in the mail about their products or offer. Even if the call is from a company you're familiar with or have done business with in the past, be careful about giving out personal information over the phone.

This includes your:

- Bank account information
- Credit card numbers
- Social Security number
- Report suspicious calls to the FTC by filing a consumer complaint form or calling the hotline, 1-877-FTC-HELP.

You can also add your number to the Do Not Call List, but keep in mind there are still millions of violations of numbers on the list.

Resources for Victims

To learn more about fraud and its impacts on your financial security, visit Fraud.org, the National Consumer League's Fraud Information Center website.

Contact your bank or credit card company if you think your account has been compromised. Then visit IdentityTheft.gov to report the theft and find out next steps.