10 Ways to Protect Your Personal Information

August 19, 2021 • By Darlynda Bogle, Acting Deputy Commissioner for Communications

Last Updated: August 19, 2021

Fraudsters don't go on vacation—so it's necessary for you and your loved ones to stay vigilant year round. Identity theft affects millions of people each year and can cause serious financial and identity-related issues. Protect yourself by securing your personal information, understanding the threat of identity theft, and exercising caution. We have a list of 10 things you can start doing now to protect yourself and your loved ones.

1. Don't believe calls, emails, texts, or any message that say you need to immediately pay to resolve a **problem**, such as legal trouble with the government or a virus on your computer, or even to collect a **prize**, like lottery or sweepstakes winnings. Legitimate businesses will not force you to make a payment over the phone as the *only* option, and will not require payment by prepaid debit card, gift card, Internet currency, or by mailing cash.

2. Protect your Social Security number by keeping your card in a safe place at home. Don't carry it around with you or provide your number unnecessarily.

3. Be careful when you speak with unknown callers. Scammers may use legitimate phone numbers or the real names of officials to mislead you. If they threaten you or make you feel scared, hang up.

4. Never give out your personal or financial information in response to an unsolicited call or message. And don't post it on social media.

5. Shred paper that contains personal information, such as your name, birth date, and Social Security number.

6. Regularly check your financial accounts for suspicious transactions.

7. Request and check a free credit report from each of the three credit bureaus every year: TransUnion, Equifax, and Experian.

8. Install and maintain strong anti-virus software on all your devices—including your smartphone, personal computer, and tablet. Don't fall for tech support scams, including pop-up warnings. If you need help fixing a problem on your computer, take it to someone you know and trust.

9. Create strong passwords so others can't easily access your accounts. Use different passwords for different accounts so if a hacker compromises one account, they can't access other accounts. Check out the Federal Trade Commission's (FTC) password checklist for tips.

10. Never click on a link sent in an unsolicited email or text message—type in the web address yourself. Only provide information on secure websites.

Stay smart. Stop scams.

We encourage you to create your own personal *my* Social Security account to track your earnings record. Contact Social Security if you find suspicious work activity on your record–you could be a victim of identity theft. You can find more information and report identity theft to the FTC on their Identity Theft website. Please share this information with your family and friends—and post it on social media.

Tags: fraud, my Social Security, my Social Security account, scams, telephone scams

See Comments

About the Author

Darlynda Bogle, Acting Deputy Commissioner for Communications

Darlynda Bogle, Acting Deputy Commissioner for Communications