

10 Tips to Protect Personal Information

1. Hang up on callers who want money or personal information to resolve a legal problem or pay you lottery winnings. Stay up to date on scams at oig.ssa.gov/scam.
2. Don't trust caller ID on your phone; government imposters will use legitimate numbers to mislead you. Be cautious with unknown callers, and if they threaten you, hang up.
3. Don't give your personal information over the phone or in an email. Social Security may contact you, but they won't threaten to arrest you. If you owe money, Social Security will send you a letter.
4. Don't carry your Social Security card in your wallet—keep it in a safe place at home.
5. Shred any piece of 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 a free credit report from each of the three credit bureaus every year. Visit www.annualcreditreport.com.
8. Install and maintain strong anti-virus software on all of your electronic devices.
9. Make your passwords complicated so others cannot easily access your accounts.
10. Don't click on links sent in an unsolicited email or text message—type in the web address yourself. Only provide information on secure websites you trust.

Take Action If You Suspect Identity Theft

- Contact the Federal Trade Commission at www.identitytheft.gov.
- Place a fraud alert and/or a credit freeze on your records with one of the three credit bureaus:
 - Equifax (1-866-349-5191)
 - Experian (1-888-397-3742)
 - TransUnion (1-800-680-7289)
- Contact your financial providers (banks, credit card companies, etc.) to question or dispute irregular transactions.
- Check your Social Security earnings statement online to make sure your reported wages are correct. Visit www.socialsecurity.gov/myaccount.

Connect With Us

Website: oig.ssa.gov | **Twitter:** @TheSSAOIG | **YouTube:** @TheSSAOIG

Instagram: @TheSSAOIG | **Facebook:** www.facebook.com/oigssa

