

SOCIAL SECURITY  
ADMINISTRATION

OIG

## Protecting Personal Information



## Secure Your Identity

The Social Security Administration (SSA), like many government agencies and businesses, continues to expand its electronic services. With a few clicks online, citizens can apply for Social Security benefits, view their *Social Security Statement*, or request a new or replacement Social Security card, for example.

As you do more business with SSA and other entities online, it is increasingly important to protect your personal information. These electronic services are generally safe and secure, but if your personal information falls into the wrong hands, identity thieves could misuse that information and access your online accounts, with SSA and other entities.

Identity theft affects millions of people each year and can have serious financial and identity-related effects. Protect yourself by securing your personal information, understanding the threat of identity theft, and exercising caution.

Please see the back of this publication for **10 Tips to Protect Personal Information** and several actions to take if you suspect identity theft.

## 10 Tips to Protect Personal Information

1. Do not believe calls, emails, or texts saying you need to pay a fee to collect lottery winnings or to resolve an issue with the government. Stay up to date on current fraud scams at [oig.ssa.gov/newsroom/scam-awareness](https://oig.ssa.gov/newsroom/scam-awareness).
2. Do not trust caller-ID on your phone; government imposters will use legitimate numbers to mislead you. Be cautious when speaking with unknown callers, and if they threaten you, hang up.
3. Never give out your personal information over the phone or in an email to someone who asks for it. Social Security may contact you, but they won't threaten to arrest you, and if you need to make a payment, they will send you a letter.
4. Always protect your Social Security number. Don't carry your card in your wallet—and keep it in a safe place at home. Don't give it out unnecessarily or accidentally.
5. Shred any piece of paper that contains personal information such as your name, birth date, and Social Security number. Identity thieves look through trash for information.
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](http://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. Use sentences or phrases that you can easily recall.
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 you trust.

## Take Action If You Suspect Identity Theft

- Contact the Federal Trade Commission at [www.identitytheft.gov](http://www.identitytheft.gov).
- Place a fraud alert on your credit record 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](http://www.socialsecurity.gov/myaccount).
- Consider blocking online access to your Social Security accounts. Visit [https://secure.ssa.gov/acu/IPS\\_INTR/blockaccess](https://secure.ssa.gov/acu/IPS_INTR/blockaccess).

## Connect With Us

**Website:** [oig.ssa.gov](http://oig.ssa.gov) | **Twitter:** @TheSSAOIG | **YouTube:** @TheSSAOIG

**Instagram:** @TheSSAOIG | **Facebook:** [www.facebook.com/oigssa](http://www.facebook.com/oigssa)



Securing today  
and tomorrow

Social Security Administration  
Office of the Inspector General  
Publication No. OIG 85-017  
Protecting Personal Information  
Produced and published at U.S. taxpayer expense