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.

(over)
About Our Organization

10 Tips to Protect Personal Information

1. 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.
2. 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 will have your information in their records and won't ask for it.
3. Understand that, generally, no government agency or reputable company will call you unexpectedly and request your personal information, or request fees for services in the form of wire transfers or gift cards.
4. 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.
5. Regularly check your financial accounts for suspicious transactions.
6. Request a free credit report from each of the three credit bureaus every year. Visit www.annualcreditreport.com.
7. Install and maintain strong anti-virus software on all of your computing devices.
8. Make your passwords complicated so others cannot easily access your accounts. Use sentences or phrases that you can easily recall.
9. 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.
10. 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.

Take Action If You Suspect Identity Theft

- Contact the Federal Trade Commission at 1-877-ID-THEFT (438-4338) or visit 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 flag irregular transactions.
- Check your Social Security earnings statement online to make sure your reported wages are correct. Visit www.socialsecurity.gov/myaccount.
- Block electronic access to your Social Security accounts. Visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess.

Connect With Us

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

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