

Consumer Education

Scammers impersonate the Social Security Administration

Your Social Security number is an important key for an identity thief. Scammers want it, and they think of all sorts of ways to trick you into giving it away.

Here at the Federal Trade Commission, we're getting reports about calls from scammers claiming to be from the Social Security Administration. They say there's been a computer problem, and they need to confirm your Social Security number. Other people have told us that they have come across spoof websites that look like the place where you would apply for a new Social Security card – but these websites are actually a setup to steal your personal information.

If you get a phone call or are directed to a website other than ssa.gov that is claiming to be associated with the Social Security Administration, don't respond. It's most likely a scam.

Here's some tips to deal with these government imposters:

- Don't give the caller your information. Never give out or confirm sensitive information like your bank account, credit card, or Social Security number – unless you know who you're dealing with. If someone has contacted you, you can't be sure who they are.
- Don't trust a name or number. Con artists use official-sounding names to make you trust them. To make their call seem legitimate, scammers use internet technology to spoof their area code – so although it may seem they are calling from Washington, DC, they could be calling from anywhere in the world.
- Check with the Social Security Administration. The SSA has a warning about <u>these</u> <u>scams</u> and suggests you contact them directly at 1-800-772-1213 to verify the reason for the contact and the person's identity prior to providing any information to the caller.

If you come across one of these scams, please report it to the Social Security Administration's Fraud Hotline at 1-800-269-0271/1-866-501-2101 (TTY) and then <u>tell the FTC about it</u>.

Source: American Bankers Association