



Privacy Rights Clearinghouse

Empowering Consumers. Protecting Privacy.

Published on *Privacy Rights Clearinghouse* (<http://www.privacyrights.org>)

Today's Date: Apr 01, 2010

Source URL (retrieved on 2010-04-01 10:50): <http://www.privacyrights.org/scare-away-scammers>

Scare Away Scammers

Copyright © 2010

Privacy Rights Clearinghouse / UCAN

Posted February 8, 2010

Most people are aware of the dangers posed by scams that claim to be originating from a business. But what if you receive an e-mail, phone call, or letter claiming to come from a government agency? Many consumers are likely to assume that such communications are legitimate because they appear to come from the government.

Unfortunately, these types of scams do occur. Communications may claim to be from the IRS, the Social Security Administration, Medicare, your local Commissioner of Jurors, or other government agencies. Frequently, they may indicate that you are eligible for a refund or a benefit, or alternatively may state that you could be subject to a penalty (fine or arrest) or will suffer some financial consequences for failing to respond. Typically, they will seek to obtain your personal information such as your Social Security number. Don't fall for the trap!

As a general rule, most government agencies do not initiate communications by telephone or e-mail. So if you receive an unsolicited e-mail or phone call claiming to be from a government agency, it is likely to be a scam. Use caution and attempt to verify the communication by contacting the government agency through a known channel (for example, a phone number published in the telephone directory). Of course, if you have initiated contact with the government agency by e-mail or telephone, an e-mail or telephone response to your communication is likely to be legitimate.

Here are recent scams to keep in mind:

- The IRS has reminded consumers to avoid identity theft scams that use the IRS name, logo or website in an attempt to convince taxpayers that the scam is a genuine communication from the IRS. Scammers may use other federal agency names, such as the U.S. Department of the Treasury. The IRS does not discuss tax account matters with taxpayers by e-mail. The IRS also does not initiate taxpayer contact via unsolicited e-mail or ask for personal identifying or financial information by e-mail.
- One bogus e-mail which claims to come from the IRS tells the recipient that he or she is eligible to receive a tax refund. It instructs the recipient to click on a link contained in the e-mail to access and complete a form for the tax refund. The form requires the entry of personal and financial information. This refund scam is the most common one seen by the IRS. Taxpayers do not have to complete a special form to obtain a refund.
- Another phony e-mail which claims to be from the Social Security Administration (SSA) threatens that if you don't update your account information (on a bogus site), you will not receive a cost-of living increase.

- You may receive a letter claiming to be from SSA attempting to verify that your address or bank has changed, or that you have become ineligible for benefits. Such letters are likely to be legitimate if they do not request information. But it's always best to verify communications by calling SSA at 800-772-1213.
- A fraudulent phone caller claims to be from an officer of the court. You are advised that you failed to report for jury duty and that a warrant is out for your arrest. Of course, you never received a notice. To clear it up, the caller says he will need some verification information. Under fear of arrest, you are asked to provide your birth date, Social Security number, maybe even a credit card number.
- An e-mail that appears to be from the Federal Deposit Insurance Corporation (FDIC) tells recipients that the FDIC has taken control of your bank. The e-mail asks recipients to download an FDIC Insurance File to check their insurance coverage. The FDIC does not send unsolicited e-mails to consumers.

Remember to guard your personal information carefully. It's easy to get fooled by a phony letter, phone call, or e-mail. Think first before you reveal any information. If you are not certain of the legitimacy of a request for information, do not provide any personal information until you have verified the identity of the requester.

Source URL (retrieved on 2010-04-01 10:50): <http://www.privacyrights.org/scare-away-scammers>

Copyright © Privacy Rights Clearinghouse/UCAN. This copyrighted document may be copied and distributed for nonprofit, educational purposes only. For distribution, see our [copyright and reprint guidelines](#). The text of this document may not be altered without express authorization of the Privacy Rights Clearinghouse.