# Suspicious e-Mails and Identity Theft

The Internal Revenue Service has issued several recent consumer warnings on the fraudulent use of the IRS name or logo by scammers trying to gain access to consumers' financial information in order to steal their identity and assets. When identity theft takes place over the Internet, it is called phishing.

## Suspicious e-Mail/Phishing

Phishing (as in "fishing for information" and "hooking" victims) is a scam where Internet fraudsters send e-mail messages to trick unsuspecting victims into revealing personal and financial information that can be used to steal the victims' identity. Current scams include phony e-mails which claim to come from the IRS and which lure the victims into the scam by telling them that they are due a tax refund.

### Phishing and Other Schemes Using the IRS Name

The IRS periodically alerts taxpayers to, and maintains a list of, phishing schemes using the IRS name, logo or Web site clone. If you've received an e-mail, phone call or fax claiming to come from the IRS that seemed a little suspicious, you just may find it on this list.

### Recent News Releases

- IR-2016-166 National Tax Security Week Concludes; IRS, Security Summit Partners Continues Work to Protect Taxpayers in 2017
- IR-2016-164 IRS Warns Taxpayers of Numerous Tax Scams Nationwide; Provides Summary of Most Recent Schemes
- IR-2016-163 Protect Your Clients: Security Summit Partners Warn Tax Pros of Cybercriminals, Launch New Awareness Tips
- IR-2016-160 IRS, Security Summit Partners Remind Taxpayers to Recognize Phishing Scams
- IR-2016-158 IRS, Security Summit Partners, Remind Taxpayers to Protect Themselves Online
- IR-2016-156 IRS, Partners Announce "National Tax Security Awareness Week" beginning Dec. 5
- IR-2016-145 IRS Warns Tax Professionals of New e-Services Email Scam
- IR-2016-123 IRS and Security Summit Partners Warn of Fake Tax Bills
- IR-2016-99 IRS Warns Taxpayers of Summer Surge in Automated Phone Scam Calls; Requests for Fake Tax Payments Using iTunes Gift Cards
- IR-2016-81 IRS Warns of Latest Scam Variation Involving Bogus "Federal Student Tax
- IR-2016-55 IRS Warns Washington D.C., Maryland, Virginia Residents of New Phishing Scam Targeting National Capital Area
- IR-2016-40 Consumer Alert: Scammers Change Tactics, Once Again
- IR-2016-29 IRS Wraps Up the "Dirty Dozen" List of Tax Scams for 2016

- IR-2015-114 IRS Warns Consumers of Possible Scams Relating to South Carolina Flood Victim Relief

**Recent Fact Sheets**

- FS-2016-23 Tax Professionals: Protect Your Clients; Protect Yourself from Identity Theft
- FS-2016-21 Security Summit Partners Update Identity Theft Initiatives for 2017
- FS-2014-3, IRS Criminal Investigation Combats Identity Theft Refund Fraud
- FS-2014-2, Tips for Taxpayers, Victims about Identity Theft and Tax Returns
- FS-2014-1, IRS Combats Identity Theft and Refund Fraud on Many Fronts

**Videos**

- Phishing — Malware: English | text

**Publications**

- Publication 4523, Beware of Phishing Schemes (English/Spanish)

**Articles**

- Taxpayer Guide to Identity Theft
- Sample of a suspicious/phishing e-mail
- Is it a phishing Web site?
- How to Protect Yourself from Suspicious E-Mails or Phishing Schemes

## You Can Help Shut Down Phishing Schemes

The good news is that you can help shut down these schemes and prevent others from being victimized.

If you receive a suspicious e-mail that claims to come from the IRS, you can relay that e-mail to a new IRS mailbox, phishing@irs.gov.

Follow instructions in the link below for sending the bogus e-mail to ensure that it retains critical elements found in the original e-mail. The IRS can use the information, URLs and links in the suspicious e-mails you send to trace the hosting Web site and alert authorities to help shut down the fraudulent sites.

- phishing@irs.gov
- Instructions for submitting phishing e-mails to IRS

Unfortunately, due to the expected volume, the IRS will not be able to acknowledge receipt or respond to you.

## Identity Theft

Identity theft can be committed through e-mail (phishing) or other means, such as regular mail, fax or telephone, or even by going through someone's trash.

Identity theft occurs when someone uses your personal information such as your name, Social Security number or other identifying information without your permission to commit fraud or other crimes. Typically, identity thieves use someone's personal data to empty the victim's financial accounts, run up charges on the victim's existing credit cards, apply for new loans, credit cards, services or benefits in the victim's name, file fraudulent tax returns or even commit crimes. People whose identities have been stolen can spend months or years — and their hard-earned money — cleaning up the mess thieves have made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans, education, housing or cars, or even get arrested for crimes they didn't commit.

- Publication 4524, Security Awareness-Identity Theft Flyer
- Publication 4535, Identity Theft Prevention and Victim Assistance (English/Spanish)
- Identity Theft Companion Learning Guide , What Law Enforcement is Doing to Stop the Thieves
- Identity Theft and Your Tax Records

## Employment Verification Contacts

You may receive a call from an IRS employee requesting verification of income and/or withholding information that has been reported to the IRS through other means. This contact may be made through a telephone call or a faxed request.

If you receive a telephone call or a fax from someone claiming to be with the IRS and you are not comfortable providing the information, you should contact our customer service line at 1-800-829-4933 to verify the validity of the call or fax. You may then contact the IRS employee who requested the information and provide the required information.

## Recent Schemes

The IRS periodically alerts taxpayers to schemes that fraudulently use the IRS name, logo or Web site clone to to gain access to consumers' financial information in order to steal their identity and assets. The scams may take place through e-mail, fax or phone. The IRS also maintains a list of phishing and other schemes.

## To Report Fraud

For other than phishing schemes, you may report the fraudulent misuse of the IRS name, logo, forms or other IRS property by calling the TIGTA toll-free hotline at 1-800-366-4484 or visiting the TIGTA Web site.

## Other Federal Resources

For more information on understanding and preventing identity theft and suspicious e-mails (phishing), or dealing with their aftermath, check out the following federal resources:

- Department of the Treasury's identity theft page
- Federal Trade Commission's (FTC) consumer Web site
- FTC's OnGuardOnLine Web site
- Firstgov
- Social Security Administration (SSA)