

The Internal Revenue Service has issued an alert, warning that the IRS name and logo is being used by fraudsters attempting to access the taxpayer financial information through e-mail, telephone, and cell phone text messaging.

Note: The IRS does not ask for personal identifying or financial information via unsolicited e-mail, telephone calls, or text messaging.

The following scams are being used to trick taxpayers into divulging financial account information for fraudulent purposes:

- Taxpayers receive a phone calls telling them that they are eligible for a sizable rebate for filing their taxes early, and they are told to provide their financial account information for direct deposit.
- Taxpayers receive e-mails that claim they are eligible for a tax refund of a specific amount, and they are instructed to click on the link in the e-mail to access the refund claim form, which requires them to disclose financial account information.
- E-mail notifications addressed to individual taxpayers claim that their tax returns will be audited. The individual is instructed to click on the link within the e-mail and complete forms disclosing personal and financial account information.
- Businesses, accountants, and “Treasury” managers are receiving bogus e-mails regarding tax law changes. To obtain information on publications for businesses, estates taxes, excise taxes, exempt organizations, as well as IRAs and other retirement plans, the recipient is instructed to click on a series of links. The IRS suspects that clicking on these links downloads “malware” onto the recipient’s computer, which can be used to search for financial records and other private information.
- A person claiming to be an IRS employee telephones taxpayers to say the IRS has mailed them a check that has not been cashed. The caller then asks for verification of financial account information.

Loss Prevention Recommendations:

If you receive an unsolicited e-mail purporting to be from the IRS, take the following steps:

- Do not open any attachments to the e-mail; they could contain malicious code that will infect your computer.
- Forward a questionable e-mail claiming to be from the IRS to phishing@irs.gov.
- Use instructions contained in an article online at www.irs.gov titled “[How to Protect Yourself from Suspicious E-Mails or Phishing Schemes.](#)”
- Contact the IRS at 800-829-1040 to determine whether the IRS is trying to contact you about a tax refund.
- Remember that taxpayers do not have to complete a special form to obtain a refund.
- If you have received this, or a similar hoax, please file a complaint at www.ic3.gov.
- A good resource for this topic is [Anti-Phishing Working Group](#).
- If you have been the victim of a spoof e-mail or Web site, you should contact your local law enforcement, a U.S. Postal Inspector, or the FBI.