



Watch Out For IRS Scams

Q: The IRS emailed me for personal info. Is this a scam?

A: Yes. The IRS says it will never email you for more information about your "economic stimulus" rebate check-or anything else. If you filed a federal tax form with the IRS, they will do the rest to handle your refund check.

One scam email on the internet looked remarkably like a real IRS website. It had the IRS blue logo, and said: "After the last annual calculations of your financial activity, we have determined that you are eligible to receive a tax refund of \$280.40. Please submit the tax refund request, and allow 3-4 days in order to process it. A refund can be delayed for a variety of reasons." The form then instructed you to fill in your Social Security number, your debit card number, expiration date, pin number, and your email.

If you submitted this information, a screen came up which told you to "please allow 3-6 business days for processing." You will receive a confirmation email once your request was processed." Once you submitted your information, you were linked back to the real IRS webpage.

If you go to the real www.irs.gov website, you will find an alert about these phony IRS emails. According to the IRS: "An e-mail claiming to come from the IRS about the 2008 Economic Stimulus Refund tells recipients to click on a link to fill out a form, apparently for direct deposit of the payment into their bank account. This appears to be an identity theft scheme to obtain recipients' personal and financial information so the scammers can clean out their victims' financial accounts. Taxpayers do not have to fill out a separate form to get a stimulus payment or have it directly deposited; all they had to do was file a tax return and provide direct deposit information on the return."

Consumers have also received scam phone calls, in which the caller impersonates an IRS employee. The caller asks the taxpayer for their Social Security and bank account numbers, claiming that the IRS needs the information to complete the processing of the taxpayer's payment. Another new scam notifies the recipient by email that his or her tax return will be audited.

Identity thieves use a victim's personal and financial 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. Most of these scams can be done electronically from a remote location-even overseas. People whose identities have been stolen can spend months or years cleaning up the mess thieves have made of their reputations and credit records. In the meantime, victims may lose job opportunities, may be refused loans, education, housing or cars, or even get arrested for crimes they didn't commit.

The IRS does not gather any information by phone. Filing a tax return is the only way to apply for a tax refund. You should ignore any unsolicited, tax-account related e-mails or phone calls from the "IRS."