

FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Division of Consumer & Business Education

Seeing Through Stimulus Scams

With talk of stimulus plans ruling the news, it's no surprise a new round of stimulus scams are afoot.

Here's how it goes: The email says you're eligible to get an economic stimulus payment. You just have to send back a form or submit one online to get it. The message might appear to come from a rebate company or look like it's straight from the Internal Revenue Service (IRS).

But the promise of stimulus money in return for a fee or financial information is always a scam, according to the Federal Trade Commission (FTC), the nation's consumer protection agency.

There's more than one way to perpetuate a stimulus scam. Some scam artists ask you to send a small processing fee, supposedly to get a much larger check in return. That's money you'll never see again. Others skip the fee, and instead, ask for your bank account number so they can "deposit" your check. Then, they use the information to clean out your account or open new ones using your identifying information.

Some stimulus scams encourage you to click on links, open attached forms, or call phony toll-free numbers. But simply clicking the link or opening the document can install harmful software, like spyware, on your computer. The result could be your personal information ending up in the hands of an identity thief.

If you get a message offering you money from the stimulus program in exchange for your personal information, ignore it, delete it, or throw it out. The IRS doesn't send emails like this asking for personal information, and rebate companies claiming to have stimulus payments for you should not be trusted, regardless of how plausible the script sounds or how official the forms look.

When a stimulus plan does involve a check to you (it may not), you won't need to fill out a separate form in an email or give out personal information — like account numbers or your Social Security number — to someone who calls you out of the blue.

If you get an unexpected email from someone claiming to be from the IRS and asking you to call a number or email back personal information, forward it to phishing@irs.gov, then delete it without clicking on any links or opening any attachments. If you think you are the target of a scam, you also can file a complaint with the FTC at ftc.gov/complaint.

If you need to reach an agency like the IRS, don't use phone numbers or links included in an email. Always type the web address directly into your browser, and look up any *url* you aren't sure about. Use phone numbers listed on agency websites or in other reliable sources, like the Blue Pages in your phone directory.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

February 2009