Stimulus Scams

Don't fall for Stimulus Scams!

The economic stimulus package has given scam artists a new angle. These scammers are taking advantage of the hype surrounding the President's Economic Stimulus package.

Don't get scammed! Learn how to protect yourself.

Direct Mail – *taking advantage of the word "RECESSION"*

Consumers are receiving direct mail marked "private and confidential", usually where a return address should be. The letter inside says something like "RECESSION RELIEF", and there is a check, made out to you. You are asked to deposit the check and send in a small processing fee… then you'll get your full "RELIEF" check.

The letter is designed to confuse because, when you read beyond the bolded word "RECESSION", you see that the check is purportedly for prize money that you've won. It has nothing to do with the recession or the President's economic stimulus plan.

The underlying message of the scam is: "here's how to get your piece of the President's stimulus package. All you need to do is give us a small amount of personal information and/or send in a small payment, and you'll get a big amount of money back." Not true! This is a variation on the Nigerian check scam that's designed to take advantage of people's desperation and hope to get something from the government. Don't fall for it! xx

Making Work Pay Refund Scam

According to the IRS, this phishing e-mail, which claims to come from the IRS, references the president and the Making Work Pay provision of the 2009 economic recovery law. It says that there is a refundable credit available to workers, consumers and retirees that can be paid into the recipient's bank account if the recipient registers their account information with the IRS. The e-mail contains links to register the account and to claim the tax refund.

In reality, most taxpayers receive their Making Work Pay tax credit, which was designed for wage earners, in their paychecks as a result of decreased tax withholding, not as a lump sum distribution from a federal fund. Additionally, consumers and retirees who are not wage earners are not eligible for this tax credit.

What to Do

The IRS does not initiate taxpayer contact via unsolicited e-mail or ask for personal identifying or financial information via e-mail. If you receive a suspicious e-mail claiming to come from the IRS, take the following steps:

- Do not open any attachments to the e-mail, in case they contain malicious code that will infect your computer.

- Do not click on any links, for the same reason. Also, be aware that the links often connect to a phony IRS Web site that appears authentic and then prompts the victim for personal identifiers, bank or credit card account numbers or PINs. The phony Web sites appear legitimate because the appearance and much of the content are directly copied from an actual page on the IRS Web site and then modified by the scammers for their own purposes.

- Contact the IRS at 1-800-829-1040 to determine whether the IRS is trying to contact you.

- Forward the suspicious e-mail or url address to the IRS mailbox phishing@irs.gov, then delete the e-mail from your inbox.

Genuine IRS Web site

The only genuine IRS Web site is IRS.gov. All IRS.gov Web page addresses begin with http://www.irs.gov/. Anyone wishing to access the IRS Web site should initiate contact by typing the IRS.gov address into their Internet address window, rather than clicking on a link in an e-mail. xx

Phishing – bogus e-mails promising expedited payments of "*stimulus checks*"

Some e-mails request bank account numbers; others request a small credit card payment. Still others have links that download dangerous software when they are clicked on.

These e-mail messages may seem to come from a government agency, and they may ask you to "verify" that you qualify for a payment. When you go to the website, it looks official, sometimes with a picture of President Obama.

These are another variation of the Nigerian scams suggesting that "you are heir to deceased king in Nigeria and send money (to get your money)". But, these news scams suggest that "you are entitled to some economic stimulus money".

First, **there are no stimulus checks** as part of President Obama's plan.

Second, if you provide your information, these con artists will drain your bank account dry and be gone in a flash. Even worse, you may fall victim to identify theft down the road.

Some of the messages are even more insidious. Just clicking on the links contained in the e-mail launches malicious software or spyware, programs that can take personal information, like credit card numbers from personal computers. xx

Phony Grants – websites promising that they can get you money from the "*stimulus fund*"

These websites look very official. They use deceptive names and may include images of President Obama or Vice President Biden, so the sites appear to be legitimate. They are not! These grants do not exist.

The stimulus money will be distributed to government agencies and nonprofit groups. Individuals will not get the money directly.

What can you do to protect yourself?

- Check out a business before parting with any money. Research the company on the Internet, but be careful of false websites and blogs with testimonials. Talk to friends and family. Review the Better Business Bureau's reliability reports.
- Never click on links or open e-mail attachments from people you don't know.
- If the e-mail offers jobs, contact the company's human resources department to make sure the job openings really exist.
- Do not provide personal information in e-mail forms.
- If you do fall for a potential scam, double check your credit card statements for unauthorized charges and dispute the charges with the company.
- Contact your bank and local police department as well.