

April 9, 2008

ALERT FROM THE SYKESVILLE POLICE DEPARTMENT

IRS REBATE SCAMS ON THE INCREASE

Most of you are aware that the United States Congress has been working on an economic stimulus package that will issue Americans tax rebate checks. Unfortunately, once the word about that spread, hackers started taking full advantage.

At the end of January 2008, the IRS (Internal Revenue Service) began sending out warnings concerning rebate scams. The warnings stated that identity thieves are already working on using the tax rebates as a way to obtain personal and financial information from the public.

As of right now, it appears their biggest tactic is contacting people via the telephone saying they will not receive their rebate until they provide banking information for direct deposit. Always remember that tax agencies will never call to request information over the phone. They do not work that way. Also, legislation has not been passed that would allow that. Therefore, if you ever receive a phone call like that, do *NOT* give out any of your information. If you do, you will be just another scam victim.

The IRS stated the threats are coming via e-mail as well. The e-mail message will appear to be from a tax agency and will ask you to complete a form that is supposedly needed to receive your rebate. Of course, the form asks for all of your personal information. Beware; if you complete the form, your information will fall into the wrong hands. Another version of the e-mail scam involves a notification that a person's rebate will be audited. The message asks you to click on a link to complete the forms needed for the process, which of course, requires all your personal and bank account information.

This scam is even going as far as e-mailing businesses and accountants telling them to download information about tax law changes. Once they do that, information is put onto their computer giving the hacker(s) remote access to the computer's hard drive. That action could put multiple peoples' information at risk.

There's also another version of the telephone scam where the caller claims to be an IRS agent. They tell the individual that he or she has not cashed the rebate check and their bank account number must be confirmed first. That's all a little crazy don't you think?

Therefore, do *NOT* click on any suspicious links you may receive in your e-mail and do *NOT* give out any personal information over the phone unless you are 100 percent sure of its legitimacy. If you receive a questionable e-mail you can always contact the IRS address at phishing@irs.gov. And, as always, use common sense to avoid any problems.