

Press Release
SUPERAntiSpyware.com
P.O. Box 40161
Eugene, OR 97404

For Immediate Release
April 5th, 2011

Press Contact
Joe Norton
joe.norton@superantispyware.com
541-607-6553 x 114

Tax Season “Primetime” for Identity Stealing Malware

Keep your personal information safe this tax season by following these basic guidelines and doing a “self-check” for free with SUPERAntiSpyware.

EUGENE, OR (April 5th, 2011) – SUPERAntiSpyware.com, a Pacific Northwest developer of state-of-the-art security software, wants to remind users that tax season is a time of increased attacks from identity stealing spyware and malware. Due to the sensitive nature of the information used to e-file, malware authors significantly increase their activity during this time in hopes of leveraging stolen data to withdraw money from bank accounts, make fraudulent credit card charges, and perform other malicious acts.

Before and during tax preparation time it's important to do a few things to help protect yourself online:

- Make sure your operating system and essential applications are up-to-date.
- Run a full-system scan regularly, at least once a week during this period of increased spyware and malware activity.
- Be extra cautious before visiting websites that you haven't visited before. Think before you click!
- Run multiple layers of security software. SUPERAntiSpyware is a proven and effective solution that will co-exist well with other security software. A single solution is not enough, especially during this period of increased malware activity – scan your system for free with SUPERAntiSpyware.

If you have already filed your taxes then don't breathe that sigh of relief yet! Malware authors are notorious for sending “fake” and “fraudulent” refund notifications or notifications that there is an error on your taxes. These notices often serve as a method to steal your personal information or infect your computer.

Some tips to thwart these activities include:

- Manually erase, or use privacy software, to delete sensitive data from your system. Malware can't leak important information if it is not on the computer.
- Be on the lookout for spam email impersonating government or bank officials asking for sensitive information - a low-tech, yet common form of attack known as phishing.
- As always, don't open emails – especially files or attachments – from people you don't know.

“We always see an abundance of phishing and infection e-mails during tax season” said Nick Skrepetos, founder of SUPERAntiSpyware.com. “It's important to protect your personal information as identity theft is on the rise and in a tough economy you can never be too protected.”

SUPERAntiSpyware Free and Professional Editions will detect and remove millions of the toughest of spyware infections. SUPERAntiSpyware definitions are updated many times per day to protect users against the latest zero-day threats. Download SUPERAntiSpyware from www.superantispyware.com

About SUPERAntiSpyware.com

Founded in 2004, SUPERAntiSpyware.com is led by Nick Skrepetos, a 30 year industry veteran, who is also the creator of the popular SUPERAdBlocker and SUPERFileRecover series of products.

Contact SUPERAntiSpyware.com by e-mail at info@superantispyware.com