

White Paper

Online Filing, Tax Software, and Keylogger Vulnerability

02/03/06

Index

<i>Section</i>	<i>Page</i>
Overview	3
Obstacles to Securing Electronic Tax Preparation	4
About Keyloggers	5
Steps to Securing Electronic Tax Preparation	6
Mitigating Vulnerabilities at Tax Time	7
Resources	7
Conclusion	8
About XoftSpySE	9
About ParetoLogic, Inc.	9

Overview

Tax software and Internet access have made the process of electronic filing a mainstay of tax systems around the world.

In the United States, the number of Americans who file their returns electronically rose from just under 12 million in 1995 to over 61.5 million in 2004.¹ In Canada, 3.9 million returns were filed electronically in 1995. That rose to 11.1 million in 2004.² Almost a third of all tax returns filed in North America this year will be filed electronically.

At the same time, the incidence of identity theft has increased almost as dramatically, with a particular focus on tax fraud. The problem has become so widespread in the United States that the Federal Bureau of Investigation has created a web site (available at www.ic3.gov) specifically for reporting identity theft.

In 1995, the biggest story regarding electronic tax fraud in the United States involved the conviction of 3 people in Houston for filing 800 falsified returns using stolen identities. By 2003, one in every 933 returns filed in the U.S. was fraudulent.³ In the United Kingdom, Her Majesty's Revenue and Customs (HMRC) was forced to close down the tax credits website at the start of December of 2005, after it was learned that fraudulent claims using stolen identities had amounted to losses in excess of £2.7 million.⁴ The perpetrators had stolen 8,800 identities and used 6,500 of them in the illegal tax scheme before the illegal activity was spotted.

The practice of identity theft related to tax records has spread around the world. In April of 2005, the deputy commissioner of the Tax Office of Australia reported at a conference in Canberra that, "identities were being harvested from the Internet," after discovering 3,500 fraudulent tax returns that had been filed electronically.

¹ 2004 IRS Data Book

² Canada Customs and Revenue Agency, May Tax Year 2004-May 2005

³ The Office of Refund Crimes of the Internal Revenue Service

⁴ Statement to Parliament by Dawn Primarolo, Paymaster-General, HMRC

Obstacles to Securing Electronic Tax Preparation

While many people using tax software and electronic filing systems have some familiarity with the Internet and its inherent risks, it appears very few use security tools in conjunction with their tax preparation activities. Security software statistics point to a lack of awareness about phishing and spyware.

A recent study by Forrester Research, an independent research firm, states that a clear majority of North American computer users – 60% – fail to scan for spyware at least once a month. Furthermore, 45% of users don't even know what spyware is, much less how to protect against it.

Unfortunately, spyware – software that installs without the user's knowledge that may capture keystrokes, personal information, and marketing data and then report your information to a third party – is far more likely to intercept information that could steal your identity than viruses. While viruses and other malware caught by anti-virus software are usually intended to replicate and “take over” computers for use by the virus writer, spyware and keystroke loggers (typically called “keyloggers”) operate silently in the background, reporting the information to a third party.

Tax preparation software and electronic filings are high-profile targets for spyware and keylogger developers. The personal information you enter into your tax filing is exactly the type of information that identity thieves seek.

Information Type	Found in tax filing	Required for credit card application	Involved in typical identity theft
Full name	√	√	√
Home address	√	√	√
Social Security Number (SSN)	√	√	√
Statement of income	√	Sometimes	Rarely
Name of employer	√	Sometimes	Rarely

Figure 1 – Correlation of information found in tax filings, required for credit card applications, and typically involved in identity theft

The most popular individual tax filing software programs in the market do not include embedded security features that prevent keystroke logging. Nor does that appear to be a consideration by consumers or tax professionals in selecting the software they use. For example, the annual survey of the Certified Public Accountants of the State of New York rates tax software by cost, ease of use, customer support, available features, timely updates, availability of state tax software, company reliability, and user familiarity. Internet security features are not included in the list of primary qualities assessed by the 500 New York CPAs who were asked to participate in the survey.⁵

About Keyloggers

Keyloggers present one of the largest risks to your identity when using financial software or interacting with Internet sites that require personal information. They are as much a threat to customers using installed tax software, as to those using online tax services.

Keyloggers are applications that monitor a user's keystrokes and then send the information via the Internet to a malicious source. They will typically generate a log file or even screen shots of what is on the user's desktop, and email or download this information to a server somewhere on the Internet. These logs or screen shots can then be used to harvest personal information including details of financial relationships from the unsuspecting user.

Keyloggers have existed in some form for many years. The growth of spyware in this decade has resulted in a mass propagation of the technology. In an article on the spread of spyware infections via the Internet, the respected Internet research firm Gartner Group reported, "At mid-2004, Gartner customers are seeing a surge in manifestations of 'spyware,' invasive methods to steal user privacy that disrupt users and their workstations at home and at work. Customers report that the cleanup effort may take a few hours, but that in no time at all, the same systems are infected again."⁶

⁵The CPA Journal, July 2005

⁶ Gartner, "A Field Guide to Spyware Variations," John Girard, July 2004

In an article published in April, 2004, Information Week reported, “Microsoft estimates that spyware is responsible for 50% of all PC crashes,” and, “Dell reports 20% of its technical support calls involve spyware.”

Keyloggers found on the Internet are created in one of two forms. The developer may create a piece of software using a ‘hooking’ mechanism involving the Microsoft Windows operating system. This type of logging is accomplished by using the Windows function SetWindowsHookEx() that monitors all keystrokes. The spyware will be delivered in the form of an executable file that calls the hook function, plus a DLL file to handle the logging functions. An application that calls SetWindowsHookEx() is also capable of capturing ‘autocomplete’ passwords provided as a service to Windows users.

Kernel based keyloggers operate at the kernel level of the operating system and receive data directly from an input device, which is typically the keyboard. This form of keylogger can be almost undetectable because it launches when the user’s computer boots into the operating system before any security applications or other programs are loaded and active.

Steps to Securing Electronic Tax Preparation

Despite the potentially dire consequences of preparing your tax returns on an unsecured computer, there are simple and low-cost safety measures you can apply to protect your identity. Install and use a high quality anti-spyware program to complement your electronic tax preparation tools and online filing of your return. Make sure your operating system is up to date and has the latest patches and security features installed. Use a hardware router or software firewall to avoid detection and infection. Personal diligence is the most effective method for avoiding identity theft and fraud.

Mitigating Vulnerabilities at Tax Time

1. Install, run, and regularly update anti-spyware software

There are many security programs available for download and trial on the Internet. ParetoLogic Inc. publishes and sells a leading-edge anti-spyware solution, XoftSpySE (available at www.paretologic.com/products) which includes state-of-the-art detection and removal of known keyloggers and spyware aimed at identity theft. A free scan is available to determine if a user's computer has any threats or infections. An annual license includes the fully functional program which offers removal tools and customer support to remove any identified threats. Regular use of XoftSpySE will provide ongoing protection against spyware, keyloggers and other forms of malware.

2. Ensure that your operating system is up-to-date

Due to security challenges faced by the most popular operating systems, the major software companies that create and license them offer continual patches and updates to ensure the integrity of your operating system remains intact. Updates are typically automatically downloaded to your computer, but you are responsible for installing them. If you run Microsoft Windows, you can visit Windows Update at www.windowsupdate.com.

3. Increase your knowledge of prevention techniques

The following resources are available to assist you in determining if you are at risk, and to respond to threats if you believe your personal information has been obtained by an unauthorized source:

<http://www.spywaredaily.com/>

Internet blog about Spyware, Adware and other Internet threats

<http://www.paretologic.com/products/>

Free anti-spyware scanner available by download

<http://www.ic3.gov/>

Internet Crime Complaint Center provided in the U.S. by the FBI

<http://www.usdoj.gov/criminal/fraud/idtheft.html>

Identity Theft and Fraud web site of the U.S. Department of Justice

<http://www.consumer.gov/idtheft/>

U.S. Federal Trade Commission web site on identity theft

<http://www.fraud.org/>

National Fraud Information Center

<http://www.justice.gc.ca/en/ps/ec/index.html>

Department of Justice, Government of Canada

Conclusion

Computers are an embedded tax reporting and filing tool in today's society. Tens of millions of returns are prepared and filed each year by users seeking convenience and time and cost savings. However, this activity carries an inherent risk which should be addressed to ensure protection of your confidential personal information. Taking the three simple steps outlined in this white paper will decrease your likelihood of suffering identity theft or the loss of personal and confidential information.



About [XoftSpySE](#)

XoftSpySE is an industry leader in advanced spyware detection and removal

Spyware can install on your computer without your knowledge and can be used to steal your confidential information resulting in identity theft and credit card fraud. Anyone who surfs the internet or shares files with other individuals is at risk.

Key Features:

- ✓ Complete PC scanning, including running processes, registry entries, files and folders
- ✓ Detects and removes: Adware, Spyware, Browser Hijackers, Trojans, Pop-Up Generators, Keyloggers, and Malware
- ✓ One of the largest spyware definitiondatabases in the industry
- ✓ Automatic definition and program feature updates
- ✓ Fast, powerful, and easy to use
- ✓ Comprehensive customer technical support
- ✓ Protects your privacy and your confidential information

Powerful protection to secure your privacy and your PC

About [ParetoLogic Inc.](#)

ParetoLogic is an international software development company headquartered in Victoria, British Columbia, Canada. A member of SIIA, we specialize in providing advanced security applications for enterprise, business and personal computer users. These include custom software solutions for business and government.

All information contained in this document is the proprietary information of ParetoLogic, Inc. and is protected by international copyright treaties. This document contains information that is privileged and confidential. Any disclosure, distribution or copying of this document without the prior written consent of ParetoLogic is strictly prohibited under applicable law. ParetoLogic, and Zheng, are registered trademarks or trademarks of ParetoLogic, Inc. in Canada and in other countries. All other trademarks are the property of their respective owners.

Copyright © 2005 ParetoLogic, Inc. All rights reserved.