Smooth Criminals: Tax Scammers in the 21st Century

National Conference of State Legislatures   April, 2015

The emerging popularity of online tax filing websites has made tax preparation easier for millions of Americans. At the same time, however, eager and sophisticated scammers see these programs as opportunities in exploitation. With tax season in full force across the country, Americans are rushing to file their taxes to meet the April 15 deadline. To their surprise, some of them may find that their return has already been filed and their refund already cashed (and no, there is not a benevolent epidemic of anonymous tax preparation). As of the end of January, the IRS had received 290,000 complaints of fraud that has resulted in $14 million in payments to criminals who impersonated their unsuspecting victims. The problem is growing quickly with taxpayers currently filing between 9,000 and 12,000 related complaints a week, according to an anonymous spokesmen for the Treasury Inspector General for Tax Administration. This tax season, over 1,000,000 million Americans will be the victims of attempted tax fraud. This begs the question, what is happening?

The Scams

During tax season, the three most frequent methods of tax fraud involve identity theft.

1. The most common occurs when a hacker obtains a taxpayer's Social Security Number, logs on to their online tax preparation account, and then files a false return. The refund is then diverted to a prepaid debit card which is then sent to the destination of the hacker's choice.

2. In the "phone scam," taxpayers receive a phone call demanding personal information or money from someone pretending to represent the IRS (The IRS will not initiate contact through a phone call or email.[1]) After being threatened with arrest and legal action, the scammers often scare individuals into depositing money on pre-paid debit cards and then require that they relay the code numbers on the cards so that the money can be withdrawn. Unfortunately, this scam has already victimized thousands of Americans.

3. Of the three, the least common scam occurs after a taxpayer has filed a legitimate tax return. If the person is owed a refund, a hacker changes the taxpayer's banking information so that the refund is placed in their account.

[1] http://www.irs.gov/uac/Newsroom/IRS-Warns-of-Pervasive-Telephone-Scam

The Response

Federal agencies and online tax programs recognize the severity of this issue. Millions of online tax forms are flagged as suspicious so it is difficult to sift through what is actually fraudulent. For example, Intuit, the parent company of TurboTax, does not have the power to determine what's fraudulent, only the IRS, but the government agency has struggled to be responsive due to budget cuts that date back to 2010. In response to the complaints, TurboTax briefly stopped filing returns in March and now requires customers to submit state and federal returns together. Simultaneous filings of the returns increases the chances that either a state or federal agency will detect fraud. Intuit also installed a "multi-factor authentication" program, which requires customers to enter a code that is transmitted to their phones or e-mail addresses when they log in. This added layer of security aims to increase the difficulty for hackers to guess a user's log-in information.

How Indiana Fought Back

In 2012, the Indiana Department of Revenue began to take significant action to combat local tax fraud. According to Department's Commissioner Mike Alley, Indiana has realized greater than a 1000% return on investment based upon flagging fraudulent refunds compared to actual cost of the program. Their success was attributed to:

1. Making agreements with software companies to set higher standards on what constituted a legitimate return.
2. Creating a short identity quiz that was sent to people who filed suspicious returns.
3. Raising awareness of tax scams via social media, local news broadcasts, and public relations campaigns.
4. Creating a process that detected fraudulent returns and unusual activity prior to filing.

Other state and local governments, including the states of Utah and Oregon, have begun to create programs that could combat tax fraud. While it may take time and research to understand why and what programs are successful, it is important that officials realize the magnitude of this issue before too many taxpayers reach the point of "no return".

- *Joshua Bass, National Conference of State Legislatures (NCSL)*