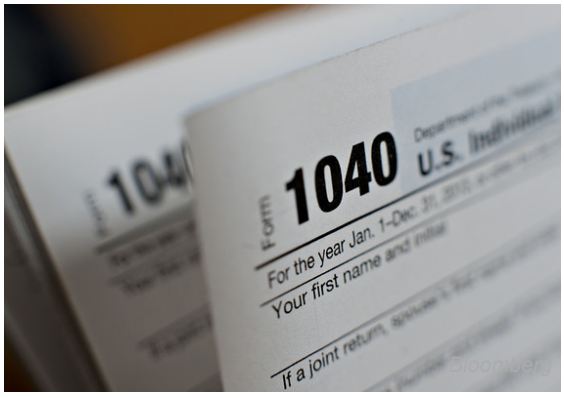
MarketWatch

IRS data theft: 5 things you need to know

By Priya Anand
Published: May 30, 2015 8:36 a.m. ET

Be wary of unsolicited email and phone calls related to the breach



As you may have heard, criminals used the Internal Revenue Service's own website to steal taxpayer information for about 100,000 U.S. households, the agency said Tuesday, showing how vulnerable it remains as fraud proliferates.

By using data stolen elsewhere, including Social Security numbers, birth dates and street addresses, thieves cleared past verification questions and gained access to old tax transcripts through the IRS website from February to Mid-May — information that can be used to file fraudulent refunds.

The IRS says it has shut down the "get transcript" feature and plans to add more security features before reviving it . The breach doesn't involve the agency's main computer system, which "remains secure," it says.

For years, the IRS has been struggling to keep tax refunds out of the hands of crooks, especially as online tax filing became common. It gave criminals who filed fraudulent refunds an estimated $5.8 billion in 2013, according to the U.S. Government Accountability Office. Earlier this month, the IRS set up a new cybercrime unit to fend off hackers. And after inadvertently giving out millions of dollars to prisoners who sent in fake filings while behind bars , the agency in 2013 began sharing more information with federal and state prisons to better match records.

This scenario, unlike the typical breach of a website or hack into a database, shows how criminals can harvest information from the growing market for stolen personal data and leverage it for financial gain in other contexts.

Here's what taxpayers should know:

1. The IRS will send you a letter if your records were at risk.

The criminals attempted to crack 200,000 accounts and made it into about half of them. The IRS will send you a letter if your account was among those 200,000, regardless of whether or not it was hacked. The agency will not call, email or send letters that ask for your personal information in response, but scammers might. Cyber thieves often take advantage of incidents like this by calling people and posing as taxmen , or emailing taxpayers malicious links.

Nasty links could infect your computer with malware in an attempt to steal your personal information, or lock up the machine until you pay a ransom — a tactic hackers began using this year while sending fake refund receipts to taxpayers, according to KnowBe4, a Clearwater, Fla.-based security company.

Cyberthieves hack into IRS system, grab personal data

(1:57)
Personal data from thousands of taxpayers were stolen when cyberthieves broke into IRS computers, posing as consumers and collecting millions in refunds.

2. The IRS will offer you free credit monitoring, but that is in no way a catch-all

If you are among the 100,000 or so taxpayers whose accounts were accessed by criminals, the IRS says it will offer you free credit monitoring. That's nice, given that your information is already with hackers and at least these services will notify you if someone attempts to open a new line of credit in your name.

That said, these services are not preventative. Credit monitoring cannot stop a criminal from opening new accounts in your name; it can merely notify you after the fact that someone has done so and you need to clean up the mess. Given that the thieves already had Social Security numbers for the accounts they cracked, victims of the hack are in for a lifetime of looking over their shoulders. Theft of this kind of information — coupled with the data from past years' tax returns — means people are likely to feel the impact for much longer than they do when credit card numbers are stolen, as banks swiftly replace those cards.

Also see: What to do if your Social Security number was stolen

3. The IRS already knew it needed to do a better job at securing taxpayer data.

Watchdogs have repeatedly warned that the IRS has a lot of work to do when it comes to security because otherwise, "its financial and taxpayer data will remain unnecessarily vulnerable to inappropriate and undetected use, modification or disclosure," according to a GAO report released in March.

In fact, the last three years' worth of GAO reports on IRS information security have called out "significant" and "serious" weaknesses that could affect the "confidentiality, integrity and availability of financial and sensitive taxpayer data." Some of these reports call out network vulnerabilities, like failure to install security updates on all servers and databases. That's in addition to the fact that criminals snuck past the authentication process to access prior tax returns.

But the IRS also had warning that identity thieves can find the necessary information to breeze through security controls via public records or other sources, the GAO said in a January report.

Also see: How the IRS could get better at stopping fraud

4. Personal identity-verification questions are a poor security practice.

In this case, crooks made it past "several personal verification questions that typically are only known by the taxpayer." Clearly, the answers to those questions were not only known to those taxpayers.

Google researchers recently released a white paper reaching that conclusion as well. They studied hundreds of millions of secret answers and account recovery claims and found that while secret questions seem like a great idea, in practice, they fail. People choose questions with obvious answers, or the questions are so difficult that the user doesn't recall the response at all.

"Many personal knowledge questions have common answers shared by many in the user population which an adversary might successfully guess," the paper says. For 16% of questions, the answers were listed in social networking profiles. Others were easily found in public records, and some questions had few plausible answers in the first place.

5. Your information isn't much safer with the government.

The number of security incidents involving personally identifiable information that federal agencies reported to the Department of Homeland Security's cyber unit increased from 10,481 in 2009 to 27,624 in 2014, according to the GAO's

2015 list of the highest risks. Inspectors general at 22 of the 24 major federal agencies called information security a major management challenge.

But you may have already figured that out: Only 6% of U.S. adults are “very confident” that government agencies can keep their records private and secure,” according to a Pew Research Center report released last week. About 25% of respondents said they are “somewhat confident” in government agencies, and 54% said they’re either “not too confident” or have no faith at all.
