2-Krebs on Security-IRS

IRS Suspends Insecure ‘Get IP PIN’ Feature

March 7, 2016

70 Comments

Citing ongoing security concerns, the Internal Revenue Service (IRS) has suspended a service offered via its Web site that allowed taxpayers to retrieve so-called IP Protection PINs (IP PINs), codes that the IRS has mailed to some 2.7 million taxpayers to help prevent those individuals from becoming victims of tax refund fraud two years in a row. The move comes just days after KrebsOnSecurity first exposed how ID thieves were abusing the service to revisit tax refund on innocent taxpayers two years running.

Last week, this blog told the story of Becky Wittrock , a certified public accountant (CPA) from Sioux Falls, S.D., who received an IP PIN in 2014 after crooks tried to impersonate her to the IRS. Wittrock said she found out her IP PIN had been compromised by thieves this year after she tried to file her tax return on Feb. 25, 2016. Turns out, the crooks beat her to the punch by more than three weeks, filing a large refund request with the IRS on Feb. 2, 2016.

The problem, as Wittrock’s case made clear, is that IRS allows IP PIN recipients to retrieve their PIN via the agency’s Web site, after supplying the answers to four easy-to-guess questions from consumer credit bureau Equifax *[]*. These so-called knowledge-based authentication (KBA) or “out-of-wallet” questions focus on things such as previous address, loan amounts and dates and can be successfully enumerated with random guessing. In many cases, the answers can be found by consulting free online services, such as Zillow and Facebook.

In a statement issued Monday evening, the IRS said that as part of its ongoing security review, the agency was temporarily suspending the

Identity Protection PIN tool on IRS.gov.

"The IRS is conducting a further review of the application that allows taxpayers to retrieve their IP PINs online and is looking at further strengthening the security features on the tool," the agency said. *[Rebuild]*

According to the IRS, of the 2.7 million IP PINs sent to taxpayers by mail for the current filing season, about 5 percent of those – approximately 130,000 – used the online tool to try retrieving a lost or forgotten IP PIN. The agency said that through the end of February 2016, the IRS had confirmed and stopped 800 fraudulent returns using an IP PIN.

"For taxpayers retrieving a lost IP PIN, the IRS emphasizes it has put strengthened processes and filters in place for this tax season to review these tax returns," *[Rebuild]* the statement continued. "These strengthened review procedures – which are invisible to taxpayers – have helped detect potential identity theft and stopped refund fraud *[Rebuild]*. Taxpayers who have been issued an IP PIN should continue to file their tax returns as they normally would. The online tool is primarily used by taxpayers who have lost their IP PINs and need to retrieve their numbers. Most taxpayers receive their IP PIN via mail and never use the online tool." *[Rebuild]*

Eight hundred taxpayers may not seem like a lot of folks impacted by this security weakness, but then again the IRS doesn't release stats on fraud it may have missed. Also, the agency has a history of significantly revising the victim numbers upwards in incidents like these. *[Worry]*

For example, the very same weakness caused the IRS last year to disable online access to its "Get Transcript" feature (the IRS disabled access to the Get Transcript tool in May 2015). The IRS originally said a little over 100,000 people were impacted by the Get Transcript weakness, a number it later revised to 340,000 and last month more than doubled again to more than 700,000 taxpayers . *[Diminish, Disappointment]*

This entry was posted on Monday 7th of March 2016 11:02 PM