Be Aware of New IRS Impersonation Scam

April 7, 2021

The Internal Revenue Services (IRS) and Social Security Administration (SSA) continue to warn consumers to guard against scam phone calls and emails from individuals who's intent is stealing money or identity. Criminals pose as the IRS or SSA to trick victims out of their money or personal information.

This week the IRS sent out another warning for university students about an IRS impersonation email scam. The suspect emails display the IRS logo and use various subject lines, such as *Tax Refund Payment* or *Recalculation of your tax refund payment*. It asks people to click a link and submit a form to claim their refund. The scam website requests taxpayers provide their:

- Social Security number
- First name
- Last name
- Date of birth
- Prior year annual gross income
- Driver's license number
- Current address
- City
- State/U.S. territory
- ZIP code/postal code
- Electronic filing PIN

Taxpayers who believe they have a pending refund can easily check on its status using the *Where's My Refund tool* [1] on IRS.gov [2].

Here are a few things people can do if they believe they are a target of the scam:
• **Report the scam**: People who receive this scam email should not click on the link in the email and report it to the IRS. For security reasons, they should save the email using save as and then send that attachment to phishing@irs.gov [3] or forward the email as an attachment to phishing@irs.gov [3].

• **Get an Identity Protection PIN:** Taxpayers who believe they may have provided identity thieves with their personal information should consider immediately obtaining an Identity Protection PIN [4]. This is a voluntary opt-in program. An IP PIN is a six-digit number that helps prevent identity thieves from filing fraudulent tax returns in the victim's name.

• **Report identity theft:** Taxpayers who attempt to e-file their tax return and find it rejected because a return with their SSN has been filed should file a Form 14039 [5], Identity Theft Affidavit to report themselves as a possible identity theft victim. See Identity Theft Central [6] to learn about the signs of identity theft and actions to take.

SSN Schemes

There have also been reports of identity theft and social security [7] schemes that target non-citizens who might be anxious about their immigration status. **There are a few steps you can take if the caller claims to be a U.S. government representative.**

1. Never give out any personal information.
2. Ask for a number to call them back.
3. Ask for their name, the agency they work for and their ID# (however, please be aware that some scams are citing “badge numbers” of law enforcement officers)
4. Search that phone number online. If it appears to be the number of a U.S. government agency, please contact your adviser at OISS [8] who can assist you in determining the next steps.
5. There are additional suggestions on this web page [9].

Source URL: https://oiss.yale.edu/news/be-aware-of-new-irs-impersonation-scam

Links:
[1] https://www.irs.gov/refunds
[2] http://www.irs.gov
[3] mailto:phishing@irs.gov
[4] https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin
[5] https://www.irs.gov/pub/irs-pdf/f14039.pdf
[6] https://www.irs.gov/identity-theft-central
[7] https://blog.ssa.gov/new-updates-to-our-warning-about-social-security-phone-scams/
[8] https://oiss.yale.edu/student-orientation-contact-oiss
[9] https://oiss.yale.edu/life-at-yale/safety/identity-theft