Defending Against Identity Theft (2015)

This recent IRS tax season yielded many more reports of tax fraud on campus and across the country compared to previous years. The IRS has advised that approximately 1 out of every 100 taxpayers will be victims of tax fraud this year.

This past year roughly 130 UT Austin faculty and staff were affected by IRS tax scams in which attackers filed a forged return and received a fraudulent tax refund. Roughly 70% of the reported victims were faculty members.

The Information Security Office has worked directly with many of these affected parties and would like to share some potentially helpful information with you as well.

Please note that while there were no breaches associated with UT Austin information resources, attackers have employed a variety of tactics to carry out their fraud. Many taxpayers fell victim to highly targeted phishing scams, spoofed calls from the Travis County Sheriff's office and other law enforcement agencies, compromised tax preparation software credentials and services, and malware infections on their personal devices that logged keystrokes; reports also emerged of attackers stealing W2 forms from their victim's mailboxes.

For additional perspective, the UT Austin Information Security Office consulted with a number of other higher education institutions across the country and most of them reported similar activity. In one case, a smaller institution reported close to 200 cases. These reports further indicated that faculty members accounted for the majority of the victims.

In many cases, attackers have also created IRS transcript accounts for the victims.

What can you do?

- **Setup UT Austin Two Factor Authentication**
  If you have not yet setup the Toopher second factor option - which helps protect your W2 with an additional layer of authentication - we would encourage you to do so: [http://www.utexas.edu/eid/help/index.html#utdsf](http://www.utexas.edu/eid/help/index.html#utdsf)

- We would strongly urge you to set up a transcript account with the IRS if they haven't already ([http://www.irs.gov/Individuals/Get-Transcript](http://www.irs.gov/Individuals/Get-Transcript)) and do so before an attacker does.
  (NOTE: The IRS has recently disabled the online account setup option due to all of the attacks and misuse they were experiencing. Registering via physical mail is still an option).

- We also suggest that you create an account with the Social Security Administration before attackers do so on your behalf ([http://ssa.gov/myaccount/](http://ssa.gov/myaccount/)). Consider claiming accounts for your underage children as well.

- We also suggest you review these articles about the recent rash of IRS scams which offer practical resources for victims of tax fraud along with some insight into how the attackers are operating:
  - [Article: Creating an IRS transcript account before the attackers do](http://krebsonssecurity.com/2015/03/sign-up-at-irs-gov-before-crooks-do-it-for-you/)
  - [Article: Consider freezing your credit file](http://krebsonssecurity.com/2015/06/how-i-learned-to-stop-worrying-and-embrace-the-security-freeze/)
    (NOTE: Consider doing this for your underage children as attackers will often try to exploit credit of minors which is generally not being monitored by their parents)
  - [Article: IRS Identifies Five Easy Ways to Spot Suspicious Calls](http://www.irs.gov/uac/Newsroom/Scam-Phone-Calls-Continue;-IRS-Identifies-Five-Easy-Ways-to-Spot-Suspicious-Calls)

- There are a variety of services that can proactively monitor your credit activity for abuse or misuse. One such service that the university has had good luck with is AllClearID: [https://www.allclearid.com/plans/pro-plan](https://www.allclearid.com/plans/pro-plan)

- Lastly, here are a few related news articles that cover the various breach events associated with the IRS scams:
  - [Article: Seton reports a breach of ~40,000 customer records](http://kxan.com/2015/04/24/39000-affected-in-seton-phishing-attack-targeting-company-emails)
  - [Article: IRS reported at least 100,000 filers were breached via fraudulent access to tax transcripts](http://www.usatoday.com/story/tech/2015/05/26/irs-breach-100000-accounts-get-transcript/27980049)
  - [Article: IRS reported a local Austin employee was arrested in a tax return scheme](http://www.statesman.com/news/news/crime-law/austin-irs-employee-faces-federal-charges-in-false/nk4Ph)
  - [Article: IRS confirmed that roughly $40M was stolen by cyber thieves](http://www.usatoday.com/story/money/2015/06/02/irs-data-breach-senate-hearing/28353983)
The IRS has acknowledged that they need to strengthen authentication validation procedures they use and they have engaged private sector entities who are already using various forms of two-factor authentication.

If you have any questions or concerns or if you believe you have been a victim of such fraud please do not hesitate to contact the Information Security Office at security@utexas.edu.

Thanks for your vigilance!

UT Austin Information Security Office
http://security.utexas.edu
security@utexas.edu