REN-ISAC

To: IT Executives and Business Officers Date: 02/06/2015
RE: Tax Fraud Advisory

As the 2015 tax filing season begins, taxpayers should prepare for heightened risks and be vigilant to tax fraud.

Attack Details

Phishing: Scam artists pose as legitimate entities—such as the Internal Revenue Service (IRS), other government agencies, and financial institutions—in an attempt to defraud taxpayers. They use phishing emails to lure users to open malicious email attachments or visit malicious sites to gain access to passwords and sensitive information.

Phone Fraud: The Treasury Inspector General for Tax Administration has received reports of roughly 290,000 contacts and has become aware of nearly 3,000 victims who have collectively paid over $14 million as a result of a phone scam, in which scammers make unsolicited calls to taxpayers fraudulently claiming to be IRS officials and demanding that they send them cash via prepaid debit cards.[1]

Fraudulent filings: There is a reported increase in attempts by scammers who attempt to use victims' personal information to file fraudulent tax returns, then claim resulting refunds.[2] [3] Taxpayer victims generally have no idea that anything is wrong until they attempt to submit their own returns. In many cases, it is extremely difficult to determine how the perpetrators were able to get the victims' filing information.

Recommended Actions

- Remind individuals to be beware of contact purportedly from the IRS by phone, email, text, or social media:
  - The IRS will never contact taxpayers by email to request personal or financial information or demand immediate payment via phone.
  - Call the IRS and states directly at 800-829-1040 to confirm legitimate communications from them.
  - Report suspicious activity to phishing@irs.gov or file a report with the Treasury Inspector General for Tax Payer Administration (TIGTA)[1], the Federal Trade Commission, and the police.
- Remind individuals to protect personally identifiable information
  - File tax returns early to thwart identity thieves.
  - Do not open email attachments or click on links from unknown or questionable sources.
  - Do not provide social security numbers and financial account information to anyone unless required.
  - If you think you are a victim of identity fraud, contact the IRS Identity Protection Specialized Unit, 1-800-908-4490 and the states where you file taxes to ensure steps are taken to secure your information.
- Protect organizational credentials through two-factor authentication.
- Redact and reduce personally identifiable information provided in online systems.
- Be cautious about sending emails to individuals that link them directly to login pages, which could unintentionally train users to be susceptible to phishing.
- Refer to US CERT[4] and the IRS[5] for additional recommendations.

Additional protection and response information is shared within the REN-ISAC information sharing community.

Points of Contact

Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)[6]

REN-ISAC's mission is to aid and promote cybersecurity operational protection and response within the research and higher education (R&E) communities.

[1] http://www.treasury.gov/tigta/press/press_tigta-2014-03.htm
[2] http://www.usatoday.com/story/money/personalfinance/2015/02/06/turbotax-state-filings-halted/22979519/?csp=breakingnews
[3] http://krebsonsecurity.com/2014/04/states-spike-in-tax-fraud-against-doctors/comment-page-1/
[4] https://www.us-cert.gov/ncas/tips/ST15-001
[5] http://www.irs.gov/uac/Tax-Fraud-Alerts
[6] http://www.ren-isac.net