IBM Security Shares Tips To Stay Safe This Tax Season

54M Americans Wait Until Last Minute to File Taxes; Cybercriminals Poised to Exploit Tax Deadline to Cash in on Refunds

CAMBRIDGE, Mass., April 5, 2017 /PRNewswire/ -- IBM (NYSE: IBM) Security today released a new report taking a closer look at the techniques and motivations of cybercriminals targeting taxpayers in the United States. Between December 2016 and February 2017, IBM X-Force researchers saw a 6,000 percent increase in tax-related spam emails. The researchers see this increase and other factors as evidence that cybercriminals are not slowing down their attacks in the days leading up to Tax Day 2017.

IBM's analysis found that historically one-third (54 million)[1] of Americans who file tax returns do so *after* April 1. This year's extended deadline of Tuesday, April 18, 2017 gives cybercriminals even more runway to execute their tax fraud schemes. IBM X-Force stresses that it's especially crucial for consumers to stay vigilant in protecting their online identities over the next month.

The new report, titled "Cybercrime Riding Tax Season Tides: Trending Spam and Dark Web Findings" outlines some of the top techniques used by cybercriminals including:

- **Seasonal Phishing**: Criminals use the topical time of tax season to entice consumers to open emails and files which have malware embedded in then which steals consumer's passwords and other financial information. The email might look like they are coming from the IRS but they are not it's the crooks posing as the IRS.
- **Who's The Boss?:** Crooks send a business's accounting staff an email that appears to have come from an executive asking for employee W-2 information. The emails look legitimate so unsuspecting employees open them, answer the questions and send sensitive information to the hackers.
- **Turbo Scammed:** Dozens of tax software companies are competing for consumer's business this time of year and send legitimate marketing emails to entice you to file with them. Cybercriminals have recreated the look and feel of those emails and are redirecting unsuspecting consumers to fraudulent websites where they steal log in details and ultimately enough info to file a return.

IBM X-Force has also mined the Dark Web and identified criminals selling W-2s for around $50 per document, thus enabling them to file false returns (and collecting the associated refunds) before an individual has had an opportunity to rightfully file. As a result, the longer a tax payer waits to file a tax return, the more they are potentially susceptible to this scam. In 2016, it was reported that the IRS paid out approximately $5.8 billion in fraudulent refunds.[2]

With this in mind, IBM X-Force has created the following tips to stay safe online this tax season and beyond.

Security Tips for Tax Season:

- **Don't delay, file right away:** Last year, 54 million Americans filed *after* April, waiting until the last minute to file. File your taxes as soon as you receive your W-2 from your employer. The longer you wait, the more opportunity a fraudster has to file on your behalf.
- **Sign up for a pin from the IRS:** The IRS IP PIN is a six-digit number assigned to eligible taxpayers to help prevent the misuse of their Social Security number on fraudulent tax returns.
- **Take advantage of free credit monitoring:** Most breached organizations now offer free credit monitoring services – consumers should plan to take advantage for the maximum time allotted.
- **Be vigilant with your inbox:** The IRS will never initiate contact with taxpayers by email, phone, text or social media to request personal or financial information. This includes requests for PIN numbers, passwords or similar access

information for credit cards, banks or other financial accounts.

- **Be aware of spoofing emails:** Scammers often send spoof emails from a target organizations' CEO, requesting all employee W-2 information from human resources and accounting departments. Don't fall for it, pick up the phone and call them to authenticate the request.
- **Avoid clicking on email links from tax vendors:** If you intend to self-file online, access your vendor's website directly to ensure you're accessing the trusted site.
- **Avoid password reuse:** Especially when filing your taxes online, make sure to avoid using a password you've used for other websites.
- **Report it:** If you suspect a phishing email, or a fake website purporting to be a tax authority's site, report it by sending it to phishing@irs.gov.

"Today's online fraudsters are savvy, scrappy, well-connected, and extremely motivated to go where the money is," said Limor Kessem, Executive Security Advisor, IBM Security. "It's inevitable for our researchers to observe spam campaign surges timed with topical events such as the Olympics, Cyber Monday or the Super Bowl. Consumers and businesses should be hyper vigilant during these key periods, and implement security best practices year round to successfully side step many of the tactics and traps regularly used by malicious hackers."

IBM Security's intelligence is gathered by hosting one of the world's largest URL databases with 25 billion+ web pages and images, collecting 1,000 financial malware samples daily, leveraging intelligence from 270M+ endpoints, and processing 1 trillion security events every month for more than 10,000 clients across 133 countries.

For additional insights into tactics and recommendations, download the "Cybercrime Riding Tax Season Tides: Trending Spam and Dark Web Findings" report http://ibm.co/2nTWvOG**.**

About IBM Security
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Contact:

Kelly Kane
IBM Security, External Relations
413-297-2668
kkane@us.ibm.com

[1] IRS: Filing Season Statistics

[2] United States Government Accountability Office Report: http://www.gao.gov/assets/670/667965.pdf

SOURCE IBM