JS|HELD

PERSPECTIVES

How to Defend Against Identity Theft This Tax Season

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

In recent years, identity theft cases have surged, especially during tax season. According to the Internal Revenue Service (IRS), in 2022, the federal agency identified and prevented USD 5.7 billion in tax-related fraud, and much of that can be linked to identity theft, highlighting how significant the problem has become.

Cybercriminals are more sophisticated than ever. They are using phishing attacks, malicious websites, and many forms of fraud to steal taxpayers' identities. To make matters worse, there has been a recent increase in the number of data breaches resulting in the leakage of personally identifiable information, specifically the leaking of social security numbers (SSNs). The flood of stolen SSNs combined with a steady increase in the number of online tax filings has resulted in a greatly increased opportunity to the fraudsters, and increased risk for all taxpayers.

In this article, we examine the many tactics modern fraudsters have at their disposal and what taxpayers can do to protect themselves from these attacks. These days, threat actors can impersonate the IRS or tax preparation companies, create fraudulent websites, or send phishing emails designed to steal SSNs and financial information. They also may simply obtain lists of stolen and leaked identity information from which to initiate their fraudulent tax claims.

One reason cyberattacks spike around tax season is that cybercriminals are well aware of how the US tax filing workflow operates and the anxiety taxpayers face while filing. These attacks really started to pick up back in the 2016 tax season when crafty fraudsters started developing websites and phishing campaigns designed to exploit the inherent trust between taxpayers and the IRS. Since then, we have seen a consistent increase in identity theft driven tax fraud as new vectors of attack have come to light, such as the shift from paper returns to online returns that was prompted by the Covid-19 pandemic.

Recent years have also seen a rise in the emergence of synthetic identity theft, where fraudsters create entirely new identities by combining real and fake information. This trend allows criminals to open new accounts, obtain credit, and file false tax returns, all under a completely fabricated identity. This is especially troubling when considering the leak of 270 million social security numbers and other personally identifiable information in early 2024 from National Public Data – a data service company that provided background checks for institutional clients. For those taxpayers whose information was leaked, the damage is likely to continue. It is possible that threat actors will use that event along with the power of artificial intelligence to design novel tax fraud threats at scale. Buckle up, this is going to be a long tax season.

CONCLUSION

This all just points to the need for heightened diligence on the part of the average person. Below is a list of proactive steps that will help protect your personal and financial information:

- Use secure tax software: Ensure that any tax preparation software or platform is legitimate and encrypted.
- Beware of phishing scams: Don't click on unsolicited emails or links that claim to be from the IRS or tax-related companies. The IRS will never initiate contact with taxpayers by email, text, or social media to request personal or financial information.
- Also be aware of phishing scams over the phone: The IRS will never call taxpayers with threats of lawsuits or arrests, or to ask for sensitive information such as your IRS PIN.
- Enable multi-factor authentication (MFA): Whenever possible, secure your accounts with MFA to add an extra layer of protection.
- Monitor your accounts: Regularly check your bank and credit accounts for suspicious activity, especially during tax season.

- File your return as soon as possible: It is “first come, first serve” at the IRS. If you beat the fraudsters to the game, they won’t be able to successfully file a return under your SSN.

- Apply for an IRS Identity Protection PIN: This PIN is a unique identify feature that once issued, is required to file your return. It is tied to your SSN, and if the fraudsters don’t have it, it gives you a great leg up on them.

Cybercriminals are adapting, and taxpayers must do the same to protect their identities in an increasingly digital world.

ABOUT THE AUTHOR

Denis Calderone is a Senior Managing Director who leads Cyber Security Services within the Digital Investigations and Discovery group in J.S. Held’s Global Investigations practice. He joined the company in October 2022 following J.S. Held’s acquisition of TBG Security. Denis brings nearly three decades of experience in the information technology field, with more than 20 years dedicated to information security. He holds multiple security certifications, including the CISSP and CISA certifications. His key technical expertise is in network and application penetration testing as well as Vulnerability Assessments, Security Policy, Development, Regulatory and Standards Compliance Testing. Denis also plays a CISO / CSO on-demand role for numerous consulting customers. Previously, he led the technical consulting arm of TBG Security and performed the role of CSO. Prior to TBG Security, Denis worked for Exodus Communications as part of their Northeast Security Practice, and for Lycos as their information security engineer.

Denis can be reached at denis.calderone@jsheld.com or +1 516 621 2900.