ultraviolet

THREAT ADVISORY

# Tax Season Social Engineering

**Services Performed By:**
UltraViolet Cyber TIDE Team
tide@uvcyber.com

**Published Date:**
March 24, 2026
TLP:GREEN

# Executive Snapshot

Tax-themed phishing campaigns continue to present a significant seasonal cyber risk because they exploit trust in familiar tax workflows, the urgency of filing deadlines, and the expectation that employees and taxpayers will receive official-looking forms and notices. Fake IRS forms are particularly effective because they provide a believable pretext for harvesting personally identifiable information, financial records, usernames, passwords, and multifactor authentication data, while also creating opportunities for malware delivery and unauthorized remote access. For organizations, this threat extends well beyond consumer fraud and should be treated as a business-risk issue that can affect payroll, finance, HR, tax operations, and any employee likely to interact with sensitive documents during filing season.

- Require employees to verify all IRS-related requests, forms, and notices through trusted internal processes and direct navigation to known government websites rather than links, attachments, or QR codes delivered through email or messaging platforms.

- Strengthen identity protections around finance, payroll, HR, and tax-related accounts by enforcing multifactor authentication, conditional access controls, and rapid alerting for suspicious login activity or abnormal access attempts tied to tax-season workflows.

- Monitor for tax-themed phishing, credential harvesting pages, and unauthorized remote access or file delivery tools, while providing targeted seasonal awareness training so users understand that fake IRS forms can be used to steal both personal data and enterprise credentials.

# TIDE Team Analysis

Tax season consistently creates a high-confidence attack window for cybercriminals because it combines urgency, financial anxiety, and a predictable flow of sensitive documents. Employees, taxpayers, payroll personnel, and tax professionals are all conditioned to expect forms, notices, corrections, and account-related communications during this period, which gives adversaries a trusted theme they can weaponize. Fake IRS forms are especially dangerous in this context because they do not need to rely on technical sophistication alone; they rely on familiarity, pressure, and the expectation that recipients will act quickly when tax matters appear to affect refunds, filings, or compliance.

These scams are no longer limited to low-quality spam or obvious fraud. Modern tax-themed phishing campaigns increasingly mimic official workflows, trusted cloud services, document portals, and government language to make malicious messages appear routine and credible. The result is a threat environment in which fake forms, transcript requests, filing alerts, and tax account prompts can be used to harvest personally identifiable information, business tax records, usernames, passwords, and multifactor authentication data. For organizations, this turns what might appear to be a seasonal event into a material identity, fraud, and intrusion risk.

Recent reporting shows that these campaigns are operating at significant scale and are reaching deeply into enterprise environments. Attackers are targeting thousands of organizations and tens of thousands of users with tax-themed messages designed to exploit the administrative and financial workflows that become more active during filing season. These campaigns are not narrowly focused on individual taxpayers. They also affect businesses, especially organizations in sectors such as financial services, technology, software, and retail, where employees frequently handle sensitive records, vendor payments, payroll data, and regulated financial information.

The primary danger is that fake IRS forms provide a highly believable pretext for victims to disclose sensitive data or authenticate into attacker-controlled credential harvesting systems. A recipient who believes they are reviewing a tax document, validating a return, or addressing an issue tied to a filing account may be far more likely to enter credentials, provide identifying information, or download a file without applying normal skepticism. Once that initial interaction occurs, adversaries can capture tax identifiers, employee information, financial records, corporate credentials, and authentication data that can be used for both immediate fraud and broader compromise.

In many cases, the threat does not end with phishing alone. Tax-themed lures can serve as the entry point for follow-on malware delivery, remote access enablement, and persistent footholds within enterprise systems. Attackers have increasingly paired fraudulent tax notifications with credential harvesting pages, packaged downloads, and software that provides remote control of the victim system. This expands the impact well beyond the loss of personal data and introduces the possibility of endpoint compromise, unauthorized remote administration, data theft, and downstream lateral movement.

One of the more troubling patterns is the use of messages that suggest a problem with tax filings, account activity, or transcript records, pushing the recipient to resolve the issue immediately. This form of coercion is effective because it exploits fear of financial loss, legal trouble, or administrative error. A fake IRS form or related notice does not need to appear perfect to succeed; it only needs to create enough urgency that the recipient bypasses normal verification steps. That is what makes these campaigns particularly effective against both individuals and business personnel during tax season.

The broader tax scam landscape further increases the risk by surrounding victims with multiple overlapping fraud narratives. Attackers are not relying on one technique alone. They are combining phishing emails, impersonation, fake online account activity, malicious attachments, fraudulent tax credits, social media deception, and phone-based scams to create a dense environment of confusion and urgency. Within that environment, fake IRS forms become one of several highly effective mechanisms for obtaining personal information, tax data, and enterprise credentials from people who believe they are responding to a legitimate government or tax-related request.

For security leadership, the central takeaway is that tax scams should be treated as a recurring identity and access threat with direct business impact. Organizations should prepare for this risk seasonally by hardening authentication controls, training employees to verify tax-related requests through known channels, monitoring for suspicious document lures and remote access tooling, and clearly defining how finance, payroll, HR, and tax functions should handle external requests involving IRS matters. Fake IRS forms are effective because they exploit trust in familiar processes, and reducing that trust gap through disciplined workflows, strong identity controls, and targeted user awareness is the most practical way to prevent PII theft, credential compromise, and follow-on intrusion.

# Why It Matters

This matters because tax-themed social engineering has repeatedly caused significant damage by exploiting trusted payroll and tax workflows rather than relying on technical exploits alone. During the 2016–2017 W-2 phishing wave, attackers commonly impersonated executives and sent urgent requests to HR or payroll staff for employee tax records, allowing them to obtain Social Security numbers, compensation data, home addresses, and other sensitive identifiers in a single exchange. Publicly reported victims from that period included Seagate Technology, Coupa Software, and Snapchat, illustrating that even well-known organizations were vulnerable when attackers embedded their requests inside normal business processes and timed them to coincide with filing season.

Further, the tradecraft behind these scams has evolved beyond tax fraud into a broader enterprise security issue. What began as executive-spoofing and W-2 theft has expanded into campaigns that also harvest credentials, capture multifactor authentication data, and in some cases deliver remote access tooling, increasing the likelihood of follow-on intrusion, fraud, and data theft. For executive leadership, the historical lesson is clear: tax-themed scams are not seasonal spam or a consumer-only problem. They are a recurring, high-trust social-engineering mechanism that can expose large populations of employees, compromise sensitive business data, and create downstream risk well beyond the initial theft of tax records.

# How to Respond

- Strictly adhere to cybersecurity Fundamentals and ensure all personnel undergo annual phishing and social engineering training. Speak with your UltraViolet Cyber TAM Representative to schedule a live phishing engagement.
- Ensure all users in your organization are aware of the threats surrounding tax season social engineering campaigns.
- Include additional ID and request verification by Accounting and HR personnel surrounding requests for tax documents.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a RedTeam or PurpleTeam engagement to gain insight into the vulnerabilities in your environment.

# What UltraViolet Cyber is Doing

- Collecting community sentiment and artifacts of new social engineering campaigns directed against customers industry verticals.
- Parsing available victim dump data for any social, financial, business, or technical relations to UltraViolet Cyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

---

---