Morgan L. Burkett is an associate in Neal & Harwell's transactional group. She is also a Certified Public Accountant. Morgan earned her J.D. from The University of Tennessee College of Law and her undergraduate degree from The University of Florida.
Contact: mburkett@nealharwell.com

TAX-RELATED PHISHING SCAMS

by Morgan L. Burkett

Everyone knows that April 15th is Tax Day (okay, okay, it's actually April 18, or April 19 if you live in Maine or Massachusetts[1])! However, many people are unaware of the numerous "phishing scams" associated with tax season. Tax-related phishing scams are so prevalent that the Internal Revenue Service (IRS) has dedicated an entire webpage on its website to warn taxpayers of these scams as well as how to avoid them.[2] Phishing is defined as "the practice of tricking Internet users (as through the use of deceptive email messages or websites) into revealing personal or confidential information which can then be used illicitly."[3] According to the IRS, "[p]hishing emails or SMS/texts (known as "smishing") attempt to trick the person receiving the message into disclosing personal information such as passwords, bank account numbers, credit card numbers or Social Security numbers."[4]

Tax professionals, those who prepare clients' tax returns, are a common target during tax season. Tax professionals, "especially those who engage in remote transactions, have been vulnerable this year to identity thieves posing as potential clients . . . [by tricking] practitioners into opening email links or attachments that infect computer systems."[5] More specifically, scammers will pose as potential clients, exchange numerous emails with a tax professional regarding their tax return, and will follow up with an attachment that they claim contains their personal tax information.[6] When the tax professional clicks on the attachment, malware infects their computer, which can lead to myriad problems for the tax professional.[7] This scam was widespread during the COVID-19 pandemic when tax professionals' correspondence with their clients was done via email versus in-person contact. The IRS has identified certain traits of these email phishing scams to watch out for, to include:

- "They appear to come from a known or trusted source, such as a colleague, bank, credit card company, cloud storage provider, tax software provider or even the IRS.
- They tell a story, often with an urgent tone, to trick the receiver into opening a link or attachment."[8]

Another common scam during tax season involves phone calls from individuals who claim to be IRS employees.[9] These scammers will use fake names and fake IRS identification badge numbers to trick the taxpayer into providing personal and financial information. The IRS lists "telltale signs" of these kinds of tax scams, to include:

- "Call to demand immediate payment using a specific payment method such as prepaid debt card, gift card or wire transfer. Generally, the IRS will first mail a bill to any taxpayer who owes taxes.
- Threaten to immediately bring in local police or other law enforcement groups to have the taxpayer arrested for not paying.
- Demand that taxes be paid without giving taxpayers the opportunity to question or appeal the amount owed.
- Call unexpectedly about a tax refund."[10]

A recent variation that has occurred with these phone scams involves "criminals' fake calls from the Taxpayer Advocate Service (TAS), an independent organization

[1] *2022 tax filing season begins Jan. 24; IRS outlines refund timing and what to expect in advance of April 18 tax deadline*, INTERNAL REVENUE SERV., https://www.irs.gov/newsroom/2022-tax-filing-season-begins-jan-24-irs-outlines-refund-timing-and-what-to-expect-in-advance-of-april-18-tax-deadline (last updated January 10, 2022).
[2] *Tax Scams/Consumer Alerts*, INTERNAL REVENUE SERV., https://www.irs.gov/newsroom/tax-scams-consumer-alerts (last updated Mar. 12, 2022).
[3] *Phishing*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/phishing (last updated Mar. 3, 2022).
[4] *Security Summit Warns Tax Pros To Be Wary of Pandemic-Related Email Schemes*, INTERNAL REVENUE SERV. (Aug. 10, 2021), https://www.irs.gov/newsroom/security-summit-warns-tax-pros-to-be-wary-of-pandemic-related-email-schemes.
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Taxpayers Beware: Tax Season is Prime Time for Phone Scams*, INTERNAL REVENUE SERV. (Jan. 27, 2022), https://www.irs.gov/newsroom/taxpayers-beware-tax-season-is-prime-time-for-phone-scams.
[10] *Id.*

within the IRS."[11] The TAS helps taxpayers if there is an "IRS problem, if [the taxpayer's] problem is causing financial difficulty, or if [the taxpayer] believe[s] an IRS system or procedure isn't working as it should."[12] The TAS would not initiate contact to a taxpayer "out of the blue."[13]

The IRS has created a list of ways for people to determine whether is the person calling is an authentic IRS employee or an impersonator contacting the taxpayer. Most IRS contact and correspondence is done through regular mail delivered by the United States Postal Service (USPS).[14] However, the IRS notes that there are special circumstances in which the IRS will call or come to a home or business in person "such as when a taxpayer has an overdue tax bill, to secure a delinquent tax return or a delinquent employment tax payment, or to tour a business as part of an audit or during criminal investigations."[15] If an IRS employee visits a taxpayer in person, they will always provide "two forms of official credentials called a pocket commission and a HSPD-12 card. HSPD-12 is a government-wide standard for secure and reliable forms of identification for federal employees and contractors."[16]

If you determine you have been targeted by a phishing scam, the IRS encourages you to report it. To report a phishing scam, some steps to take include the following:

- **If a taxpayer receives an unsolicited email claiming to be from the IRS or an IRS-related function, or that contains a request for "personal information, taxes associated with a large investment, inheritance or lottery[,]" forward the email as-is to phishing@irs.gov[17]**
- **If a taxpayer receives a suspicious telephone call:**

1. **If the phone call is IRS-related, report the call to the Treasury Inspector General for Tax Administration via their online complaint form at https://www.treasury.gov/tigta/reportcrime_misconduct.shtml.[18]**
2. **If the phone call is Treasury-related, report the call to the Office of the Treasury Inspector General via email at OIGCounsel@oig.treas.gov.[19]**
3. **In addition, report any IRS- or Treasury-related fraudulent calls to phishing@irs.gov with the subject "IRS Phone Scam."[20]**

As a taxpayer, if you find yourself unsure if it is the IRS contacting you or a potential phishing scam, refer to the IRS website for additional guidance on how to differentiate legitimate IRS contact from phishing scams.

[11] *IRS Warns of New Phone Scam Using Taxpayer Advocate Service Numbers*, INTERNAL REVENUE SERV. (Mar. 15, 2019), https://www.irs.gov/newsroom/irs-warns-of-new-phone-scam-using-taxpayer-advocate-service-numbers.
[12] *Id.*
[13] *Id.*
[14] *How to Know It's Really the IRS Calling or Knocking on Your Door*, INTERNAL REVENUE SERV. (Apr. 19, 2017), https://www.irs.gov/newsroom/how-to-know-its-really-the-irs-calling-or-knocking-on-your-door.
[15] *Id.*
[16] *Id.*
[17] *Report Phishing and Online Scams*, INTERNAL REVENUE SERV., https://www.irs.gov/privacy-disclosure/report-phishing.
[18] *Id.; Report a Crime or IRS Employee Misconduct*, INTERNAL REVENUE SERV., https://www.treasury.gov/tigta/reportcrime_misconduct.shtml (last updated Sept. 30, 2021).
[19] *Id.*
[20] *Id.*