A Security Center Update

Tax Phishing Scams

Tax Phishing Scams

The IRS has issued an urgent warning concerning a phishing scam that seeks to steal Electronic Filing Identification Numbers. This scam focuses on tax preparers. It emerged right before tax filing season has begun – Feb 12th. It involves emails that impersonate the IRS with a subject line "verifying your EFIN before e-filing" The text of the email asks tax preparers to email copies of the EFIN verification and driver's license with a fake warning that if they do not comply, their ability to file tax documents electronically will be disabled[1].

If a person falls for the scam, the information obtained can be used to illegally file tax returns for refund by impersonating the victim. If you receive one of these scam emails, you should save it as a file and then send it as an attachment to phishing@irs.gov. They should also visit the Treasury Inspector General for Tax Administration website at www.tiga.gov to report the scam.

Like all other scams, this one attempts to get the receiver to open a link or attachment. These links or attachments may be designed to collect information or download malware to the receiver's PC. Although the focus on many of these scams are tax professionals, consumers are still at risk. COVID-19 has provided scammers with a perfect backdrop for their phishing campaigns.

You can protect yourself by:

- Slow down. The most common reason given for falling for a scam was that the receiver was in a hurry and not paying attention.
- Think before you click. Does your email have links? A link could either be an email address or to a web site. If so, hover your mouse over the link but do not click the link. A pop-up box should appear showing you were the link will send you. Does it match the text of the link? Practice using these safe samples. The bad link samples are examples only. They will not send you anywhere:
  - Safe samples: www.PenFed.org PenFed.org the IRS website
  - Bad links: www.PenFed.org PenFed.org the IRS Website
  - Bad email links: marvin@mars.gov jane@penfed.org
- Read the FROM address carefully. Many scammers will "one off" or misspell a name. For example:
  - johnjones@annazom.com Did you catch the two n's instead of the 'm' in amazon?
  - George.washinton@us.gov Did you catch the misspelling in Washington?
- Does the email ask for personal details? Most businesses will **never** ask you for this kind of information over email.
- Look for out of ordinary things, such as images that are crooked, or of poor quality. Missing signature blocks. Typos. Bad grammar or word choices or phrases that just "sound off".
- Verify the sender – If you know the sender, call them from a phone number you have. Don't use a number provided in the questionable email, it may be fraudulent. If you don't, use the internet to find a number to call. In either case, verify that the person or organization sent you the email **before** you click any items or provide any information.

Understand that cybersecurity is ultimately YOUR responsibility. Think before you clink. Don't just be smart, be cybersmart!

Remember, Security is Everyone's Responsibility

[1] "IRS, Summit partners issue urgent EFIN scam alert to tax professionals", https://www.irs.gov/newsroom/irs-summit-partners-issue-urgent-efin-scam-alert-to-tax-professionals

Questions or Issues

If you have questions or need assistance, please contact Information Security Risk & Compliance about the policy or Access Control to provision access.