Rhode Island Department of Revenue
Division of Taxation

ADV 2017-21
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
JULY 11, 2017

Security Summit warns about spear-phishing emails

Example shows cybercriminal impersonating prospective client to snare tax professional

PROVIDENCE, R.I. – The Rhode Island Division of Taxation, tax agencies in other states, the Internal Revenue Service, and the tax industry today warned tax professionals to beware of spear-phishing emails, which are commonly used by cybercriminals to target practitioners.

Spear-phishing emails, often tailored to individual practitioners, result in stolen taxpayer data and fraudulent tax returns filed in the names of individual and business clients.

Information about spear phishing kicks off a new "Don't Take the Bait" awareness campaign aimed at tax professionals.

This is the first of a special 10-part series developed by the IRS, the Rhode Island Division of Taxation, tax agencies from other states, and the tax industry, who are are working together as the Security Summit. They are focused on fighting refund fraud and tax-related identity theft.

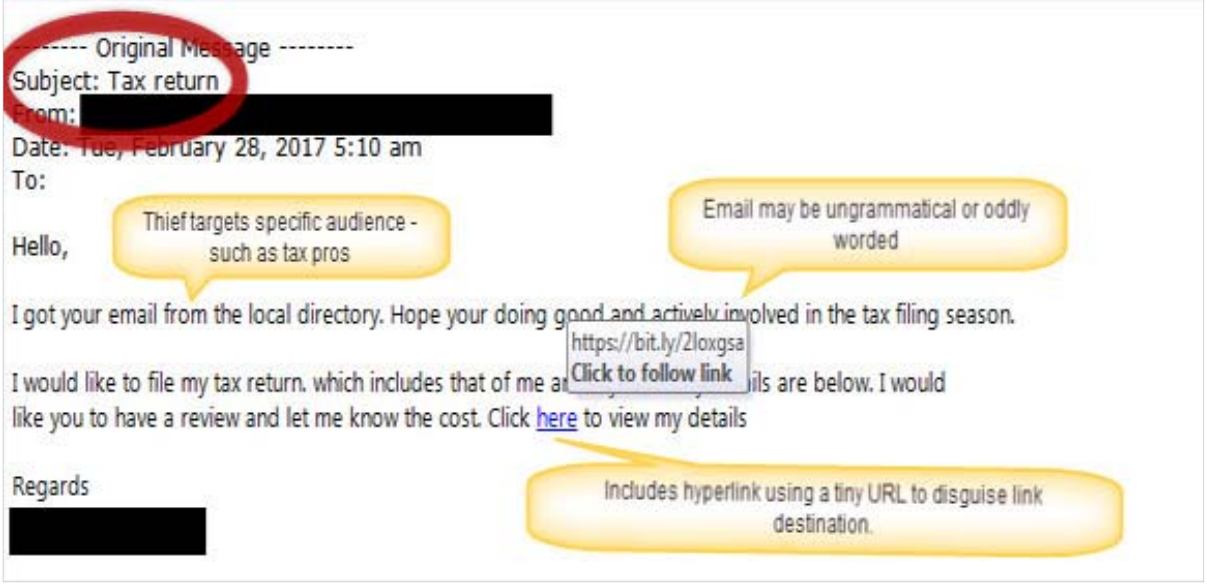
"We are seeing repeated instances of cybercriminals targeting tax professionals and obtaining sensitive client information that can be used to file fraudulent tax returns. Spear-phishing emails are a common way to target tax professionals," said IRS Commissioner John Koskinen. "We urge practitioners to review this information and take steps to protect themselves and their clients."

Trying to catch a few victims

Phishing emails target a broad group of users in hopes of catching a few victims. Spear-phishing emails pose as familiar entities, and the cybercriminals have done extensive research and homework in order to target a specific audience. Tax professionals and taxpayers are among the groups that regularly receive phishing emails.

The security software firm Trend Micro reports that 91 percent of all cyberattacks and resulting data breaches begin with a spear-phishing email. The email, disguised as being from a trusted source, may seek to have victims voluntarily disclose sensitive information such as passwords. Or, it may encourage people to open a link or attachment that actually downloads malware onto the computer.

Following is an example of a spear-phishing email that targeted a tax professional during the 2017 filing season. Note the use of "Tax return" in the subject line to bait the tax preparer as the sender impersonates a prospective client:



Note that the sender has done research, obtaining the name and email address of the tax pro. And, the email is conversational but ungrammatical and oddly constructed: "hope your (sic) doing good (sic) and actively involved in the tax filing season." This is potentially a sign that English is a second language. Finally, note the hyperlink using a "tiny" URL is used to mask the true destination – this is another red flag.

Attachment has malware

There are several other versions of spear-phishing emails in which the criminal poses as a potential client. In one version, the prospective "client" directs the tax professional to open an attachment to see the 2016 tax information needed to prepare a return. However, the attachment in reality downloads malware that tracks each keystroke made by the tax professional so that the criminal can steal passwords and sensitive data.

Most spear-phishing emails have a "call to action" as part of their tactics, an effort to encourage the receiver into opening a link or attachment. The example above asks the preparer to review their tax information and provide a cost estimate.

Other spear-phishing emails impersonate the IRS, such as the IRS e-Services tools for tax professionals, or in some instances a private-sector tax software provider. In those examples, preparers are warned that they must immediately update their account information or suffer some consequence. The link may go to a website that has been disguised by the thieves to look like the login pages for IRS e-Services or a tax software provider.

Cybercriminals are endlessly creative. This year, some identity thieves hacked individuals' email accounts. Noticing that the individuals had been in email contact with tax preparers, the criminals used the individual's email address to send a note to their preparer asking that the direct deposit refund account number be changed. The scam prompted an IRS alert to preparers about last-minute refund changes.

Protecting clients and your business from spear phishing

There is no one action to protect your clients or your business from spear phishing. It requires a series of defensive steps. Tax professionals should consider these basic steps:

1. Educate all employees about phishing in general and spear phishing in particular.
2. Use strong, unique passwords. Better yet, use a phrase instead of a word. Use different passwords for each account. Use a mix of letters, numbers and special characters.
3. Never take an email from a familiar source at face value; example: an email from "IRS e-Services." If it asks you to open a link or attachment, or includes a threat to close your account, think twice. Visit the e-Services website for confirmation.
4. If an email contains a link, hover your cursor over the link to see the web address (URL) destination. If it's not a URL you recognize or if it's an abbreviated URL, don't open it.
5. Consider a verbal confirmation by phone if you receive an email from a new client sending you tax information or a client requesting last-minute changes to their refund destination.
6. Use security software to help defend against malware, viruses and known phishing sites and update the software automatically.
7. Use the security options that come with your tax preparation software.
8. Send suspicious tax-related phishing emails to phishing@irs.gov.

For more information:
https://www.irs.gov/individuals/protect-your-clients-protect-yourself
https://www.irs.gov/individuals/taxes-security-together

CONTACT INFORMATION

The Division of Taxation is located on the first floor of the Powers Building, at One Capitol Hill in Providence, diagonally across from the Smith Street entrance of the State House. The Division is typically open to the public from 8:30 a.m. to 3:30 p.m. business days. The main phone number is (401) 574-8829. (For questions about personal income tax, choose option # 3.) To see a list of phone numbers and email addresses to various sections within the agency, use the following link: http://www.tax.ri.gov/contact/. For refund status, see: https://www.ri.gov/taxation/refund/. (The Division of Taxation cannot directly respond to taxpayer inquiries via social media, such as Twitter and Facebook, because of State statutes protecting taxpayer confidentiality. For the same reason, individual taxpayer inquiries cannot be directly addressed when made through traditional media, such as TV stations and talk-show programs.)