ADV 2018-47
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
DECEMBER 17, 2018

Tax professionals targeted by phishing emails

Scams involve payroll direct deposit and wire transfers, Security Summit says

PROVIDENCE, R.I. – The Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit warned today of an uptick in phishing emails that target tax professionals. The emails involve payroll direct deposit and wire transfer scams.

Overall, the scam is known as "business email compromise/business email spoofing" – or BEC/BES for short. As a general rule, BEC/BES tactics target all types of industries and employers. The Security Summit recently received a number of reports from tax preparers that they, too, are being targeted.

The Security Summit partners – including the IRS, the Rhode Island Division of Taxation, and tax community partners – are concerned that these scams, as well as a scam involving Form W-2 wage statements – could increase as the 2019 tax season approaches.

How the scams work

These emails generally impersonate a company employee, often an executive, and are sent to payroll or human resources personnel. The email from the "employee" asks the payroll or human resource staff to change his or her direct deposit for payroll purposes. The "employee" provides a new bank account and routing number, but the account is actually controlled by the thief. This scam is usually discovered pretty quickly, but not before the victim has lost one or two payroll deposits.

In another version of the BEC/BES scam, the emails impersonate a company executive and are sent to the company employee responsible for wire transfers. The email requests that a wire transfer be made to a specific account that is controlled by the thief. Companies that fall victim to this scam can lose tens of thousands of dollars.

A common theme in these and many other email scams is that they include grammatical and spelling mistakes.

All businesses should be alert to these BEC/BES scams that take many forms such as fake invoice payments, title escrow payments, wire transfers or other schemes that result in a quick payoff for the thief. Businesses should consider policy changes to guard against such losses.

One version that the IRS and Summit partners have highlighted in recent years is the W-2 scam. This scam involves an email from a criminal who is masquerading as an executive or person in authority. The email requests a list of the organization's Forms W-2 covering all of the firm's employees.

The purpose of this scam is to obtain information that would allow thieves to quickly file fraudulent tax returns for refunds. All employers, in both the public and private sectors, should be on guard against this and other dangerous scams. To learn more about W-2 and identity theft scams, click here.

BEC/BES email examples

Following are examples of emails that have been reported by tax professionals to the IRS in recent days. These emails have been edited by the IRS:

EXAMPLE # 1

From: [REMOVED]
Sent: Monday, December 10, 2018 [REMOVED]
To: [REMOVED]
Subject: (no subject)

Hello [REMOVED],

I changed my bank and I will like my paycheck DD details changed. Do you think this change be effective for the next pay date?

[REMOVED]

Sent from my iPhone

EXAMPLE # 2

------ Original message ------
From: [REMOVED]
Date: 12/10/18 [REMOVED]
To: [REMOVED]
Subject: ACH Payment Attention

[REMOVED],

Please confirm the receipt of my message, Authorized can you handle domestic transfer payment now?

Thanks you.

[REMOVED]

Sent from my iPhone

Where to send the BEC/BES emails

General non-tax related BEC/BES email scams should be forwarded to Internal Crime Complaint Center (IC3), which is monitored by the Federal Bureau of Investigation. To file a complaint about email scams or other internet-related scams: https://www.ic3.gov/default.aspx

Tax professionals and others should also report tax-related phishing emails to phishing@irs.gov. This account is monitored by IRS cybersecurity professionals. This reporting process also enables the IRS and Security Summit partners to identify trends and issue warnings.

Because of the dangers to tax administration posed by the Form W-2 scam, the IRS set up a reporting process for employers. Employers who fall victim to the W-2 scam should report it at dataloss@irs.gov. There is a process employers can follow – click here to learn more. Employers who receive the W-2 scam email but do not fall victim should forward the email to phishing@irs.gov.

About the Security Summit

The Security Summit consists of the IRS, state tax agencies, and the tax community -- including tax preparation firms, software developers, processors of payroll and tax financial products, tax professional organizations, and financial institutions.

Partners in the Security Summit work together to combat identity theft and fight other scams to protect the nation's taxpayers.

The Rhode Island Division of Taxation office is at One Capitol Hill in Providence, R.I., diagonally across from the Smith Street entrance of the State House. It is open to the public 8:30 a.m. to 3:30 p.m. business days. To learn more, see the Division's website: www.tax.ri.gov.