Phishing Scheme Involving IRS Tax Forms

The Internal Revenue Service issued an alert warning of a phishing scheme in which fraudulent email requests copies of tax forms or claims to provide access to tax form information. Payroll and human resources professionals have been targeted in some campaigns.

The phishing email typically requests copies of employee W-2 forms or claims that electronic W-2s are available, encouraging unwitting victims to provide information and/or to click to log in and view/print their W-2s. In some versions of the scheme, links in the phishing email may point to a fraudulent website made to appear to be an organization’s human resources site. Those who fall victim to the phishing email may have their personal information compromised, including login, password, tax information, bank account information, personal contact information and benefit information.

Please continue to be vigilant and mindful of the following:

• DO NOT reply to email with any personal information or passwords. If you have reason to believe that the request is real, call the institution or company directly.
• DO NOT click a link in an unsolicited email message. If you have reason to believe the request is real, type the web address for the company or institution directly into your web browser.
• DO NOT use the same password for your work account, bank, Facebook, etc. In the event you do fall victim to a phishing attempt, perpetrators attempt to use your compromised password to access many online services.
• DO change ALL of your passwords if you suspect any account you have access to may be compromised.
• DO be particularly cautious when reading email on a mobile device. It may be easier to miss telltale signs of phishing attempts when reading email on a smaller screen.
• DO remember that official communications should not solicit personal information by email.

For additional information:

https://www.irs.gov/uac/Newsroom/IRS-Alerts-Payroll-and-HR-Professionals-to-Phishing-Scheme-Involving-W2s
https://www.us-cert.gov/ncas/tips/ST15-001

Issued: March 2016