IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s

The Internal Revenue Service issued an alert to payroll and human resources professionals to beware of an emerging phishing email scheme that purports to be from company executives and requests personal information on employees. **Note that W-2 phishing campaigns have been recently targeting universities including CUNY.**

The email requests copies of employee W2 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.

The IRS has learned that this scheme - part of the surge in phishing emails seen this year - already has claimed several victims as payroll and human resources offices mistakenly email payroll data including Forms W-2 that contain Social Security numbers and other personally identifiable information to cybercriminals posing as company executives.

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 will attempt the compromised password in many places
- 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
Phishing Scheme Involving W-2s

easier to miss telltale signs of phishing attempts when reading email on a smaller screen

- Official communications from CUNY Finance, Payroll and OHRM departments should not use language similar to that used in "W-2" phishing emails

"This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments," said IRS Commissioner John Koskinen. "If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees."

If you receive such a phishing email please forward it "as an attachment" to security@cuny.edu. A sample phishing email received at CUNY is included below.

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

CUNY Phishing Advisory at http://security.cuny.edu (under "CUNY Issued Security Advisories")