Issued 2/3/17

IRS: Scam Blends CEO Fraud, W-2 Phishing

The IRS said phishers are off to a much earlier start this year than in tax years past, trying to siphon W-2 data that can be used to file fraudulent refund requests on behalf of taxpayers. The agency warned that thieves also appear to be targeting a wider range of organizations in these W-2 phishing schemes, including school districts, healthcare organizations, chain restaurants, temporary staffing agencies, tribal organizations and nonprofits.

“This is one of the most dangerous email phishing scams we’ve seen in a long time,” IRS Commissioner John Koskinen said. “Although not tax related, the wire transfer scam is being coupled with the W-2 scam email, and some companies have lost both employees’ W-2s and thousands of dollars.”

The IRS says organizations receiving a W-2 scam email should forward it to phishing@irs.gov and place “W2 Scam” in the subject line. Organizations that receive the scams or fall victim to them should file a complaint with the Internet Crime Complaint Center (IC3,) operated by the FBI.

Employees whose Forms W-2 have been stolen should review the recommended actions by the Federal Trade Commission at www.identitytheft.gov or the IRS at www.irs.gov/identitytheft. Employees

should file a Form 14039 (PDF) Identity Theft Affidavit, if the employee's own tax return rejects because of a duplicate Social Security number or if instructed to do so by the IRS.