URGENT ALERT FROM THE IRS REGARDING A FORM W-2 EMAIL PHISHING SCAM

On February 2, 2017 the United States Internal Revenue Service (IRS) issued an urgent alert to all employers that the Form W-2 email phishing scam is spreading beyond the corporate sector to other sectors including hospitals, school districts, tribal organizations and nonprofit groups. All employers, governmental or private, for-profit or nonprofit, should be cognizant of the risk the IRS described in its alert.

DETAILS OF THE ALERT

According to the IRS alert, "cybercriminals use various spoofing techniques to disguise an email to make it appear as if it is from an organization executive. The email is sent to an employee in the payroll or human resources departments, requesting a list of all employees and their Forms W-2. This scam is sometimes referred to as business email compromise (BEC) or business email spoofing (BES)."

The alert goes on to warn of a further scam where the cybercriminal follows up the W-2 request email with an "executive" email asking for a wire transfer to be made to a certain account. According to the alert, some companies have lost both employees' W-2s and thousands of dollars due to wire transfers.

The IRS, state tax agencies and the tax industry, working together as the Security Summit, have seen an upswing in reports of these scams in recent days.

ACTIONS TO TAKE

Employers should consider creating internal policies on the distribution of W-2 information and conducting wire transfers. Some employers have controls in place such as requiring a confirming telephone call to a known legitimate phone number for the party seeking the information or transfer. Others require two executives to sign-off on any wire transfer.

Employers receiving a W-2 scam email should forward it to phishing@irs.gov and write "W2 Scam" in the subject line. Organizations that receive the scams or fall victim to them should also report them to the Federal Bureau of Investigation (FBI) via the Internet Crime Complaint Center (IC3) website at https://www.ic3.gov.

For further information, please see the IRS alert at:

https://www.irs.gov/uac/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others

Please contact your Keenan HealthCare Account Manager for questions regarding this *Briefing*.