Privacy Technical Assistance Center
U.S. Department of Education
(855) 249 3072
privacyTA@ed.gov
ptac.ed.gov

W 2 Phishing Scam Now Targeting Schools

Especially during the tax season, everyone should be aware of the threat that phishing attacks pose to personal data. But did you know that the threat also extends to entire organizations, where highly targeted phishing emails have caused the loss of large amounts of employee private information and resulted in the theft of significant amounts of money? The Internal Revenue Service (IRS) released guidance this month warning of a new and particularly virulent phishing threat ***currently targeting education organizations like schools and districts.*** The scam is two-fold:

Phase 1

The first component typically consists of an email purporting to be from a highly placed executive like the Superintendent, and sent to an employee responsible for payroll or human resources. This message may ask for listings of employees, or even copies of forms that contain sensitive information like W-2 forms. If the employee is unsuspecting, they may respond to the attacker thinking it is an actual request and provide the attacker with information that could be used for identity theft like filing and submitting fraudulent tax returns.

Phase 2

A second component of this attack includes an email from an executive targeting an individual responsible for payroll or comptroller functions, instructing them to provide a payment via wire transfer to an attacker-controlled account. The IRS warns that this second portion of the attack may not necessarily reference anything tax related.

What to Do?

Schools and school districts should be aware of this immediate threat, and take steps to ensure that employees are trained to recognize and report suspicious emails to the appropriate authorities through their organizational security incident reporting process. In the interim, schools and districts should reiterate their policies on the use of email to transmit personally identifiable information (PII) across their organizations, and take this opportunity to remind employees in the payroll and human resources functions that they are being specifically targeted for these types of phishing attacks.

If your school or district has been targeted or is a victim of this type of attack, feel free to contact the Privacy Technical Assistance Center (PTAC) at the U.S. Department of Education for assistance in responding and reporting the incident at privacyta@ed.gov.

The IRS requests that anyone receiving one of these emails also forward the email to the IRS at phishing@irs.gov with the subject of "W2 Scam," and consider reporting the incident to the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3). For more information on this guidance from the IRS, please refer to the original IRS guidance at https://www.irs.gov/uac/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others.