Office of Inspector General
Legal Services Corporation

The Fraud Corner

Payroll and Direct Deposit Phishing Schemes

The Office of Inspector General (OIG) for the Legal Services Corporation (LSC) is providing Grantee Executive Directors with the following information related to payroll fraud.

In recent weeks, two cybercrimes involving "phishing" emails targeting LSC program online payroll accounts were reported to the OIG; in these instances, the perpetrators were able to redirect direct deposits from employee payroll accounts to the perpetrator's account. Thieves continue to implement new tactics to trick accounting and human resource officials to update employee direct deposit information, which could lead to the theft of the employee's payroll check. Malicious actors may impersonate a trusted person or a person of authority to entice an employee to perform certain payroll related actions. Once the employee makes a direct deposit change based upon a fictitious email request, the thief has access to the employee's payroll disbursement. Employees who use a self-service portal to update their personal information, such as bank routing and account numbers, are particularly vulnerable to this type of scam.

The following information is based on an alert recently issued by the Federal Bureau of Investigation (FBI) to notify employers of a similar type of phishing payroll scheme. By becoming aware of potential phishing schemes and taking steps to prevent such schemes from being successful, grantees may be able to avoid falling victim to payroll related phishing scams.

The FBI warned that fictitious phishing emails are typically designed to update/change an employee's direct deposit information in order to capture the employee's login credentials. Once the phishing email is received, the employee is then directed to a false site impersonating the self-service portal for direct deposit. The thieves then use the stolen login credentials to change the direct deposit instructions to their own account which provides them access to the employee's payroll account.

The best defense is knowing what to look for to prevent such criminal acts from occurring in your program.

How to Detect Payroll Email Phishing Schemes

- Spelling and grammatical errors
- Urgent or unusual requests from a person of authority in the organization

- Unusual or questionable sender's email address especially public addresses such as yahoo.com or gmail.com
- Slight deviation of a site address that mimics the legitimate site – look for the https abbreviation and a lock symbol at the beginning of the site URL
- The email asks the employee to click a link, access a website, or answer a few questions
- An email requesting verification of employee paycheck direct deposit information
- An email requesting personal or sensitive information (login credentials)
- An embedded link that doesn't match the displayed link
- A misleading URL; to verify, hover your cursor over the URL hyperlink to see the web address to ensure its legitimately associated with the known company.

How to Prevent Payroll Email Phishing Schemes

- Alert your workforce to this scam
- Before clicking on any link, contact your network security, IT professional, or Human Resources Department to determine the validity of the email
- Never provide user IDs, login credentials or personal identifying information in response to an email
- Do not click on pop-up ads or links/attachments in a suspicious e-mail
- Separate payroll functions from human resources responsibilities
- Ensure payroll login credentials used for payroll purposes differ from those used for other purposes
- Employer self-service platforms should have a two-step authentication process requiring users to enter a second password
- Prior to making any change, independently contact the purported sender to obtain confirmation of the request – this separate verification step is a key prevention measure
- Ensure written payroll account change procedures exist and are followed
- Use security software to help defend against malware, viruses and known phishing sites – always make sure the security software is up to date with its definitions.

If you have any questions or would like additional information about this payroll phishing scheme, please contact Daniel O'Rourke, Assistant Inspector General for Investigations for the LSC OIG, at (202) 295-1651 or by email at dorourke@oig.lsc.gov.