Office of Inspector General
Legal Services Corporation

3333 K Street, NW, 3rd Floor
Washington, DC 20007-3558
202.295.1660 (p) 202.337.6616 (f)
www.oig.lsc.gov

LSC-OIG HOTLINE ADVISORY

Recent Ransomware and Phishing Attacks
7/13/2021

The Legal Services Corporation (LSC) Office of Inspector General (OIG) is issuing this advisory to remind grantees of the threat posed by phishing schemes and ransomware attacks, and to alert you to recent schemes targeting LSC grantees.

One recent phishing scheme involved an email that was sent to a grantee employee containing a link embedded with malware. The phished employee clicked the link, which allowed the perpetrator to gain access to the system and encrypt all the program's data. The grantee eventually regained access to their system's data through the aid of a cyber security firm and did not need to pay the ransom. The grantee had acquired cyber insurance prior to the phishing scheme, which should allow them to recover any losses related to the attack, including any loss of productivity.

In another recent phishing scheme, an email was sent to all grantee employees requesting that employees purchase gift cards using personal funds, which would then be reimbursed. As in other similar schemes, a recently hired employee followed the directions, replied with her personal cellphone number, and purchased eight Apple Gift cards at $100 each for a total purchase of $800. As instructed by the perpetrator via a follow up text, the employee provided all gift card authorization numbers, allowing the perpetrator to redeem the gift cards and complete the theft. Cellphones make it much harder to identify the red flags associated with a phishing scheme; unlike with laptops and desktops, there is no ability to hover over the link to preview the URL before clicking the link.

The OIG suggests each grantee share this advisory with all employees. It is also recommended that as part of the onboarding and orientation provided new employees, the grantee inform employees that no one from the program will ever send an urgent text or email to employees to purchase gift cards or direct them to send money through email or text. Employees should also be informed that requested changes to direct deposit information for the program or payroll must be verified by direct (telephone or in-person) contact with a known requester. Additionally, employees should be reminded that it only takes one ill-advised click of the mouse to become a victim of cyber fraud.

The OIG suggests all Executive Directors and staff review the previously provided OIG advisories on phishing and ransomware prevention, as well as the social engineering red flags associated with email messages linked here, created by KnowBe4, an expert in security awareness related to cyber threats. Links to the previously released alerts can be found below. Finally, the OIG recommends scheduling cyber security training for staff on a regular and ongoing basis to prevent the grantee and/or its employees from becoming a victim of these types of scams.

LSC Business Email Compromise Fraud Scheme

Fraud Corner Email Schemes FINAL

Ransomware_Attacks_FA_10-02-20_Final.pdf (lsc.gov)

Hotline_Advisory_Grantee_Mitigates_Ransomware_5-06-21_Final.pdf (lsc.gov)

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