The Fraud Corner

Email Scams Targeting LSC and LSC Grantees (1/25/2021)

The Office of Inspector General (OIG) has confirmed that the Legal Services Corporation (LSC) and at least two LSC grantees have recently been the target of business email compromise (BEC) scams. These scams resulted in the successful diversion of grant funds and gift cards to cyber-criminals. This threat is ongoing, and we have reason to believe that the cyber-criminals may be targeting additional LSC grantees. We therefore strongly encourage you to take immediate preventative steps, described in more detail below. The preventive steps include training your employees on BEC schemes and enhancing your internal controls and data security. Please share this fraud advisory with all employees to prevent the success of future scams in our community.

In each of the schemes described below, emails purport to originate from known sources (such as an LSC employee, a grantee executive director or a senior grantee employee) and appear to contain legitimate requests related to a payment or a purchase. The cyber-criminals used social engineering techniques, and potentially systems breaches, to elicit sensitive business information from the unsuspecting grantee or LSC employee. By these fraudulent contacts, the cyber-criminals attempt to convince employees that requests to change information or make fraudulent purchases are legitimate. In these instances, the unsuspecting employees' actions in response to the scams resulted in the success or near success of the cyber-criminal's scheme.

Business Email Compromise Schemes

Three BEC schemes have been perpetrated against LSC and its grantees in the last month. The schemes aim to trick employees into changing payment information to the cyber-criminal's bank account or to make purchases for the cyber-criminal.

Scheme One

In order to gain access to sensitive LSC and grantee information, the cyber-criminal created spoofed email domains for LSC and an LSC grantee. The spoofed email domains closely resembled LSC and the grantee's actual domains but for the addition of a dash or extra letters (e.g., @lscgov.com vs. @lsc.gov). Using the spoofed email domains, the cyber-criminal impersonated LSC and grantee fiscal employees. The cyber-criminal then sent emails requesting an LSC bank account change for the grantee. Overlooking potential indicators of fraud in the cyber-criminal's emails, LSC and grantee employees supplied the requested information. The cyber-criminal then used the information to successfully request that LSC update the grantee's banking information of record to the cyber-criminal's banking information. As a result, the grantee's monthly LSC grant payment was diverted to the cyber-criminal's bank account.

Scheme Two

The cyber-criminal gained access to an LSC grantee's Chief Financial Officer's (CFO) email account using stolen credentials. It is unknown how the CFO's email credentials were obtained. Cyber-criminals often use phishing schemes to trick employees into providing passwords and other sensitive data. Once inside the CFO's email account, the cyber-criminal enabled Microsoft Office 365's auto-forwarding function so that all emails from LSC's email domain (@lsc.gov) would be automatically forwarded to the CFO's junk folder, where the cyber-criminal could view and respond to LSC's emails undetected. The cyber-criminal then emailed LSC's fiscal department from the CFO's legitimate email account, requesting bank-change forms. Although the cyber-criminal did not complete and return the form to LSC, the attempt was to divert the grantee's monthly LSC grant payment to the cyber-criminal's account through a bank account change scheme.

Scheme Three

The cyber-criminal, posing as the grantee Executive Director, contacted a newly hired administrative employee by email. The cyber-criminal requested that the employee purchase gift cards as a surprise for staff. The cyber-criminal asked the employee to keep the request confidential and to respond by email with photos of the gift card codes once the purchase was complete. The employee requested and received a corporate credit card from their manager, purchased the cards, and sent the cyber-criminal the card codes. The scheme was discovered when the employee notified the Executive Director in person that the task was complete

Important Preventative Suggestions

- **Add the spoofed email domain @lscgovt.com to your organization's blocked domain list**.
  The spoofed email domain created for LSC in Scheme 1 was @lscgovt.com. Although it has been disabled, it could be recreated with a different domain host company. Thus, we suggest adding it to your blocked list.

- **Verify all emails that appear to be from LSC are legitimate.**
  LSC's email domain name is @lsc.gov.
  Emails from LSC will **always** end in .gov, **never** .com, .org, etc.
  Beware of emails that contain a sense of unnecessary urgency, request for confidentiality, spelling and grammatical errors, and deviations in names or titles.

- **Disable automatic forwarding and deleting email rules, especially related to external addresses.**
  According to the FBI, attackers are able to conceal their activity through auto-forwarding rules implemented on victims' web-based email clients, but which often do not sync with the desktop client, thus hiding the malicious rules from security

administrators. Using social engineering and stolen credentials, the attackers gain access to victim email accounts. The scammers prevent the victim from identifying any fraudulent communications by setting up auto forwarding rules to ensure the success of their malicious activity. If web and desktop mail clients are not actively synced, administrators may not have visibility into the fraudulent activity.

- **Prohibit international IP addresses from accessing your systems, especially email systems**.
  Because BEC schemes typically originate outside of the United States, blocking international IP addresses can be an additional preventive measure.

- **Ensure that staff, especially finance staff, is aware of these BEC scams and other types of cyber-threats.**
  Require cyber-threat training and make staff aware of various types of social engineering techniques (the use of deception to manipulate individuals to provide confidential information for fraudulent purposes). Instruct staff to be wary of requests for information for items that should be common knowledge to the person requesting the information. If you haven't already procured a cyber-security training program (cyber-training expenses are chargeable to your Basic Field grant), some training, such as The Department of Defense's Phishing Awareness Training Course is available free of charge.

- **Require at least a two-part identity verification for all payment and purchase requests or changes to existing payments or purchases.**
  Two-step verification typically involves an email and telephonic or in-person verification of information. Changes that require two-part identity verification for payments or purchases should include changes to bank accounts, contact name, email address, phone number, physical address, etc. So, for example, when receiving an email request that appears legitimate, follow up with a phone call to a previously confirmed number to verify that the email and request are legitimate.

- **Enable automated notifications, if available, for changes to bank accounts, contact name, email address, phone number, physical address, etc.**
  Some software, such as payroll, typically have settings that allow for automated notifications for these types of changes. These notifications can act as an extra step to verify the legitimacy of requested changes.

- **Require at least a second level of approval for any requests related to payments and purchases or changes to payments or purchases.**
  Similarly, changes that require second level approval for payments or purchases should include changes to bank accounts, contact name, email address, phone number, physical address, etc. This additional control would require review of the actual request and approval by more than one employee.

- **Employ multi-factor authentication on grantee accounts when available.**
  A user would be required to present one or more verification factors in addition to his/her login credentials in order to gain access to the account or system. This additional measure helps prevent system access when credentials are stolen.

- **Beware of URL spoofing.**
  When a fraudulent link, including links to email addresses, is masked to look like a legitimate and/or familiar source.

- **Adopt an incident response plan.**
  An incident response plan outlines how an organization will respond to breaches, notify the appropriate authorities, and take appropriate corrective measures. Having a plan in place can increase an organization's response time and potentially mitigate any loss or liability.

- **Consider purchasing cyber-insurance.**
  Cyber-insurance policies may limit an organization's financial and legal exposure if a cyber-fraud does occur.

For additional ways to prevent and detect email scams, including BEC schemes, the OIG urges LSC and grantee staff to review the advisories and alerts provided in the links below. LSC grantee staff must remain vigilant to identify suspicious emails and beware of the schemes identified in this Fraud Corner article.

Additional OIG Cyber-Threat Resources

Special Fraud Advisory - Business Email Compromise (BEC) Scheme

Fraud Corners

Fraud Alerts

Results of Information Technology Vulnerability Assessments

COVID-19 Fraud Scams

If you have any questions or would like additional information about this Fraud Corner 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.