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

BEC Schemes Targeting Grantee Financial Institutions

2/18/2022

The Office of Inspector General (OIG) for the Legal Services Corporation (LSC) is issuing this advisory to alert grantees of a recent Business Email Compromise (BEC) scheme that targeted a grantee's financial institutions.

The FBI defines BEC schemes as scams that target businesses that regularly perform wire transfers by compromising official email accounts in an attempt to conduct unauthorized fund transfers. **This recent BEC scheme is the first reported scheme that has identified and targeted an LSC grantee's financial institutions in order to gain unauthorized access to their accounts (including both banking and investment accounts).** Prior BEC schemes against LSC and LSC grantees have targeted grant remittances, payroll, and gift card purchases.

The perpetrator of this most recent scheme impersonated the grantee executive director and attempted to gain signatory authority and administrative access rights to the grantee's financial accounts. Fortunately, the targeted financial institutions flagged the emails as suspicious and contacted the program to verify their authenticity.

How was the scheme perpetrated?

- The scheme included two separate emails to two financial institutions used by the grantee.
- The perpetrator used a spoofed email domain that appeared to match the executive director's actual email address, except the spoofed email domain was one letter off from the grantee's actual email domain; (for example, spoofing the email address janedoe@lscorp.com by removing one letter in the spoofed email address janedoe@lscor.com).
- The perpetrator's emails created a sense of urgency (a common red flag) by stating that the executive director was sick with COVID-19.
- The emails claimed a legitimate business need, stating that a new president had been named to the grantee's Board of Directors who required access to the grantee account. The perpetrator provided the bank with a fictitious name and an email address for the purported new Board president.

How to prevent perpetrators from identifying your financial institutions.

- Make sure staff (especially fiscal staff) are aware of social engineering techniques used to deceive employees into disclosing sensitive business information.
- Ensure your program's information technology (IT) security can promptly detect network breaches, such as compromised staff email accounts.
- Do not name your financial institutions in public documents, such as annual reports or online financial statements.
- Conduct periodic checks with your financial institution for any recent unauthorized changes to the account administrator or signatory authority.
- Contact your financial institutions to make them aware of this type of scheme.
- Discuss with your financial institutions security measures such as two-part identity verification when changes to your accounts are requested.
- Make sure fiscal staff monitor fiscal accounts for unauthorized fund transfers.
- Ensure the receipt and storage of all electronic banking notices and documents are secure and checked periodically for intrusion.

Additional preventative suggestions for BEC schemes and email scams.

- Be alert to emails with hyperlinks that may contain misspellings or changes to the actual domain name.
- Add spoofed email domains to your organization's blocked domain list.
- Prohibit international IP addresses from accessing your systems, and block emails from high-risk domains and international origin.
- Disable automatic forwarding and deleting email rules, especially related to external addresses.
- Consider withholding the names of fiscal staff from the grantee website.
- Require two-part identity verification for all payment and purchase requests or bank account routing changes. For instance, LSC requires a video virtual meeting with the employee before changing a direct deposit account.
- Require a second level of approval for all requests to change bank account and routing numbers related to payments and purchases.
- Enable automated notifications, if available, for changes to bank accounts, contact name, email address, phone number, physical address, etc.
- Employ multi-factor authentication on grantee accounts when available.
- Beware of URL spoofing.
- Adopt an incident response plan.
- Consider purchasing cyber-insurance.

IT security and cyber threat prevention measures for grantees to consider with their IT departments and IT contractors.

- Help prevent email-based fraud schemes by configuring email systems with SPF, DKIM, and DMARC records that authenticate inbound and outbound emails and email systems.
- For grantees that use Microsoft 365 cloud, consider enabling Microsoft 365 Defender and utilizing the Microsoft Digital Crimes unit.

For additional information on identifying and preventing BEC schemes and email scams, please review the following LSC-OIG alerts related to scams that targeted LSC grantees during the COVID-19 pandemic:

Email Scams Targeting LSC and LSC Grantees

LSC Business Email Compromise Fraud Scheme

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