NCFTA®

The National Cyber-Forensics and Training Alliance

ONE TEAM, ONE GOAL. COMPANIES, GOVERNMENT, AND ACADEMIA WORKING TOGETHER TO NEUTRALIZE CYBER CRIME.

Business Email Compromise (BEC) Mitigation Guide

This guide is to supplement the NCFTA BEC white paper and serve as a blueprint for mitigating BEC using a joint business and information technology approach. Both are essential for protecting against BEC, but at minimum there should be a business response to prevent further victimization. BEC remains a fairly "low tech" type of cybercrime and can often be effectively stymied by instituting a portion or all of the following recommended business and IT practices. NCFTA intelligence analysts sourced these practices from independent research as well as contributions from our industry and law enforcement partners.

BUSINESS PRACTICES

Establish protocols that require identity verification after any change to payment instructions. Although this may add significant friction, including provisions in future agreements stating that any payment changes will result in processing delays should help manage party expectations.

Plan your organization's response to BEC incidents, phishing, or other unusual activity. Report any suspicious activity to your IT department, financial institution, and the Internet Crime Complaint Center (IC3). If your organization fell victim to a BEC scam and sent funds to a fraudulent account, contact your bank immediately to begin the recall process and file a complaint at www.IC3.gov. For the best chance of recovering funds, include as much detail as possible, including victim and recipient account information.

Regularly train and test employees to detect, identify, and report phishing and other unusual activity. Develop and implement a training program, either internally or from a third party, to address social engineering, phishing, credential security, and financial transaction handling. Train employees to identify and report abnormal emails (e.g. beneficiary name different from that of the business, use of non-corporate email addresses, odd language, spoofed domains, etc.) or activity.

Limit access to corporate financial information to specific employees. Create a defined "Limit of Authority" policy that outlines a person's access to sensitive corporate information and signing authority. Limitations should follow the principle of least privilege (i.e. role, function, organizational hierarchy, etc.).

Maintain awareness of new methods of communication and payment. Bad actors use alternative forms of communication and payment, often in an attempt to circumvent fraud controls, and may capitalize on emerging platforms to impersonate targets and divert funds. For example, BEC fraudsters often request victims purchase gift cards, which are then converted to bitcoin or other cryptocurrency.

Employ proactive countermeasures. These may include monitoring for domain registrations attempting to impersonate your organization and pursuing means to remove them, limiting public disclosure of personal information of employees, and challenging scammers to produce specific details.

INFORMATION TECHNOLOGY PRACTICES

IT PRACTICES

- Use Managed Email Gateway
- Develop Incident Response Procedures
- Monitor Spoofed Domains
- Review Email Content
- Leverage DMARC
- Deploy MFA
- Protect Cloud-Hosted Servers
- Keep Systems Current
- Add Encryption
- Avoid Executive Exemptions

Use a managed email gateway solution and disable certain email settings for all users, such as mail-forwarding and the ability to delete their own email inbox. The use of email filtering and quarantining to prevent impersonating/fraudulent emails is an efficient way of scanning the senders and content of incoming emails. Once a criminal has obtained access to a business email account, they will often use the mail-forwarding feature to maintain access and monitor future emails.

Develop and implement incident response procedures to address BEC, phishing, and other unusual activity. It is recommended companies document formal incident response procedures ready for action in the event of a compromise. The proper documentation and implementation of such procedures can be the difference between successful recovery and loss of funds. For example, in the event of a BEC incident, the organization's bank POC, as well as local FBI and/or Secret Service POCs, should be clearly documented and readily available.

Monitor spoofed domains to mitigate BEC. It is important to leverage tools and available resources to identify spoofed domains. Domain age can be useful in alerting on potentially spoofed domains; it is advisable to quarantine domains less than 90 days old. Maintain documentation to include appropriate tools or vendors used for monitoring and designate who is responsible for the monitoring efforts, and declare takedown processes.

Review email content. Phishing attempts share common features, such as a sense of urgency, the threat of an impending charge, and use of awkward grammar, including misspellings, extra dashes or periods, or unnatural wording. The rate of success and the ability to increase the volume of phishing emails leads to the frequent reuse of templates. Examine URLs within all emails before clicking or following any link. Quarantine, or mark with a content warning, all emails containing embedded hyperlinks, emanating from outside your domain. Train employees to review headers of suspicious emails for authenticity and potentially malicious indicators.

Authenticate email via Domain Message Authentication Reporting and Conformance (DMARC). Leveraging DMARC allows for the use of existing authentication tactics to verify that the sender of an email is as claimed, as well as allowing for reporting. With DMARC, a domain owner is notified when an email is sent on its behalf.

Deploy multi-factor authentication (MFA). Threat actors regularly attempt to use breached credentials and brute force login attacks against company email servers or gateways. MFA enables companies to add an extra layer of protection against potentially compromised credentials. It is recommended that companies develop a credential compromise awareness capability and enforce strict password-replacement policies in the event of a compromised account.

Protect cloud-hosted servers. Maintain proper documentation to establish clear responsibilities between CSPs and customers, making it clear who is responsible for ensuring secure and proper configuration of servers. Use of least privilege access is advisable to protect against user errors. Use key-based cloud encryption to prevent unauthorized users from gaining access to data files saved to cloud storage devices.

Keep systems current with security patches & updates and automate threat detection and remediation. This must extend to updating legacy systems as they near end of life to avoid compromise by known exploits and vulnerabilities. Threat actors often leverage default device credentials and vulnerabilities with known remediation steps as initial infection vectors.

Add encryption on employees' machines. Particularly when employees are working from home or using personal or mobile devices for business purposes. Adding encryption to these devices allows for another layer of security in the event of loss or theft.

Resist making executive exemptions to security protocols. Senior level employees will continue to be targeted and often unintentionally become the weak link in the security chain.