CYBERRISKS&LIABILITIES

Business Email Compromise

Cybercriminals continue to become more sophisticated, leveraging a wide range of tactics in order to attack their victims. One tactic that has increased in frequency, complexity and resulting losses over the past few years is the use of business email compromise (BEC) scams.

Put simply, a BEC scam entails a cybercriminal impersonating a seemingly legitimate source—such as a senior-level employee, supplier, vendor, business partner or other organization—via email. The cybercriminal uses these emails to gain the trust of their target, thus tricking the victim into believing they are communicating with a genuine sender. From there, the cybercriminal convinces their target to wire money, share sensitive information (e.g., customer and employee data, proprietary knowledge or trade secrets) or engage in other compromising activities.

BEC scams can lead to numerous consequences within your organization—including stolen data, financial hardship and potentially severe reputational damages. Nevertheless, these scams can be deterred through various cybersecurity techniques. Review this guidance to learn more about what BEC scams are and top measures that your organization can implement to prevent such scams.

BEC Scams Explained

Essentially, BEC scams consist of cybercriminals impersonating an individual or entity within their targets' trusted networks for malicious gains. These scams are categorized as a form of social engineering—which refers to a broader cyberattack method that preys on key human behaviors (e.g., trust of authority, fear of conflict and promise of rewards) to obtain unwarranted access to organizational systems, funds or data.

Cybercriminals who execute BEC scams often utilize these social engineering strategies:

- **Creating confusing variations**—In an attempt to convince their targets that they are a trusted source, cybercriminals may create email addresses that are nearly identical to the source they are impersonating, with the exception of a few characters (e.g., altering the email address "janedoe@samplecompany.com" to "janedoee@samplecompanyy.com").
- **Using spear-phishing techniques**—Cybercriminals may engage in spear phishing by conducting additional research on their targets and leveraging any extra details they discover to further motivate victims to believe their false identities. When spear phishing, cybercriminals often impersonate sources who are more directly connected to their targets (e.g., a close colleague or department leader).
- **Deploying malware**—When sending fraudulent emails in BEC scams, cybercriminals may encourage their targets to download harmful attachments or click on deceptive links in an effort to launch malicious software—also known as malware. Once activated, this software can help cybercriminals more easily gain access to their victims' systems, funds and data.

According to the FBI, there are several different types of BEC scams, including the following:

- **False invoice scheme**—In such a scheme, a cybercriminal impersonates an organizational supplier to trick their target into paying fraudulent invoices or transferring funds to a phony account.
- **CEO fraud**—This scam method entails a cybercriminal impersonating a senior-level employee or executive and requesting that their victim conduct a wire transfer to a fake account. The request is often demanding in nature, threatening the victim with work-related consequences or other punishments for failing to comply.

ATLAS INSURANCE AGENCY

- **Account compromise**—Within this scam tactic, a cybercriminal hacks into an employee or executive's actual email account and distributes messages to various contacts—attempting to fool these recipients into paying fraudulent invoices.
- **Attorney impersonation**—This scam technique refers to a cybercriminal impersonating a lawyer or other legal representative and requesting a payment be made to a phony account in order to handle an organizational matter deemed "sensitive" or "pressing."
- **Data theft**—In such a scam method, a cybercriminal impersonates an HR professional to trick their target into sharing personal information about employees or executives. The cybercriminal can then leverage this sensitive data during future attacks.

Preventing BEC Scams

Any employee can become the target of a BEC scam, putting the security and financial stability of your entire organization at risk. Be sure to implement the following cybersecurity measures to help deter BEC scams:

- **Educate your employees.** Minimizing losses from BEC scams starts with training your employees on how to detect and prevent such instances. Equip your staff with these best practices:
  - Refrain from sharing personal or work-related information on social media platforms, as cybercriminals could use those details to help launch a BEC scam.
  - Avoid opening or responding to emails from individuals or organizations you don't know. If an email claims to be from a trusted source, be sure to verify their identity by double-checking the address.
  - Be wary of emails that lack personalization, contain spelling and grammatical errors, request sensitive details or use threatening language. Don't divulge financial information over email.
  - Never click on suspicious links contained in emails. Similarly, avoid downloading email attachments or from unknown sources.
  - If you suspect a BEC scam, contact your manager or the IT department immediately for further guidance.
- **Implement effective payment protocols.** Having safe and secure payment procedures within your organization can help put a stop to BEC scams before any money is lost. As such, instruct employees who handle your organization's financial operations to carefully analyze invoices and fund transfer requests to ensure their validity. When possible, these requests should be discussed in person before moving forward—especially if they involve alternative payment procedures or changes in account numbers. Further, consider utilizing several verification methods to confirm payment requests.
- **Restrict access to sensitive data.** Only provide employees with access to sensitive organizational data if they are trusted, experienced and require such information to conduct their work tasks. Protect this data with access controls and multifactor authentication measures.
- **Utilize security features.** Make sure all organizational devices possess adequate security features to help deter BEC scams—including access to a virtual private network, antivirus and malware prevention programs, email spam filters, data encryption capabilities and a firewall. Update these security features as needed.
- **Have a plan**. Lastly, ensure that your organization has an effective cyber incident response plan in place. This plan should specifically address response protocols and mitigation measures for BEC scams. In particular, your organization should plan on contacting your financial institution as soon as a BEC scam occurs to determine whether funds have been stolen from your account. If money has been taken, the account should be temporarily frozen to prevent further theft. Apart from consulting your financial institution, your organization should also report BEC scams to your local FBI field office and log such scams with the Internet Crime Complaint Center.

For more risk management guidance, contact us today.