SMALL BUSINESS EMAIL COMPROMISE & SPOOFING

Communication and validation are key to protection

When an accounts payable employee at a small manufacturing company received an urgent email from the firm's CEO to wire a significant amount of money immediately to an unfamiliar account, her urge to confirm the details was waylaid when informed in a follow-up email that the funds were needed for an acquisition that must be completed with haste or the opportunity would pass. After $250,000 was wired, it was discovered that the CEO was not the source of the request; his email account had been taken over by a fraudster who disappeared with the funds.

Business email compromise is a type of fraud perpetrated via email in which a business is tricked into transferring funds to accounts controlled by criminals or handing over sensitive data, such as employees' names, addresses and Social Security numbers. While scammers target businesses of all sizes, small businesses often lack the scale or the resources for a sophisticated cybersecurity program. However, small businesses are not defenseless. These basic precautions can help to prevent business email compromise.

How it works

Business email compromise, or BEC, occurs when someone falsifies a legitimate email address to authorize the disclosure of sensitive information or the transfer of funds to accounts managed by criminals. The scammer either hijacks or spoofs (impersonates) the email account of an executive who is authorized to instruct other employees to initiate payments, such as wire transfers or an automated clearing house (ACH) transfer.

Sometimes, fraudsters impersonate legitimate vendors and trick unsuspecting victims (businesses of all sizes) to reroute future payments to a different account, set up and controlled by fraudsters. Some reasons offered for the creation of new accounts include moving their business account to a different bank or because the account routinely used is undergoing an audit.

The employee believes the email instructions to be legitimate and completes the transfer of funds as requested, unknowingly depositing company funds into bank accounts controlled by the scammer.

Types of attack

The scammer needs some critical information in order to successfully impersonate the executive's or legitimate vendor's real email account to initiate the fraudulent transfer of funds or data:

Spoof an email account or website

Using slight variations of a legitimate address fools a victim into thinking fake accounts are authentic, such as replacing a lowercase "L" in the company name with the numeral one (1). The cybercriminal can use such a spoofed email to request that a vendor's bank account information be changed, for example.

Send spear-phishing emails

A spear-phishing attack is designed to trick employees into disclosing sensitive information or unknowingly providing access to a computer system by sending counterfeit messages that appear to be legitimate. A spear-phishing campaign targets a specific individual or groups, such as employees of a specific company. Attackers can use information available in social media profiles to gain knowledge about a business's workforce, organizational hierarchy, technology and communication channels, and target them with a phishing or social engineering campaign to acquire the sensitive information.

Use malware

Malicious software compromises company networks to access information about a business's billing and invoice processes, which will be exploited by the scammer, or to gain undetected access to a victim's data, including passwords and financial account information.

Vendor Impersonation

Many of the vendor impersonation schemes involve contracts that are publicly awarded. Typically, open source information is available regarding successful bidders that can easily be impersonated via slightly altered websites, often using legitimate images, logos, etc., taken from the victim's legitimate site. Email accounts often are also then set up using slight variations from the legitimate site/email. One such example might be a legitimate site using www.abctools.com versus a fraudster site set up using www.abctoolsinc.com.

Email Account Compromise

Criminals acquire valid credentials for a legitimate company email account. They subsequently email a customer of the company, often with new payment information. Any changes to payment information should be verified by another communication channel that is trusted and used prior to receiving this new payment email. The best defense against email accounts being compromised is to have multifactor authentication enabled.

Warning Signs

- An employee receives an email from a higher-up executive/ manager ordering them to quickly process an invoice, change the recipient of a payment or provide sensitive data.
- The message is urgent and presses the employee to bypass standard policies and procedures.
- The email comes from the executive's/manager's personal account rather than their company account.
- The email address of the sender is a variation of the real company's email addresses.

Report the fraud

All business email compromise cases should be reported, no matter how small or large, to alert authorities to the activity. Report any online fraud or BEC activity to the Federal Bureau of Investigation's Internet Crime Complaint Center (https://www.ic3.gov). While a specific case may not be fully remediated, authorities gain more insight about patterns and attackers from multiple reports.

Also, if a fraudulent transfer is discovered, contact your financial institution to explore the potential for recalling the funds.

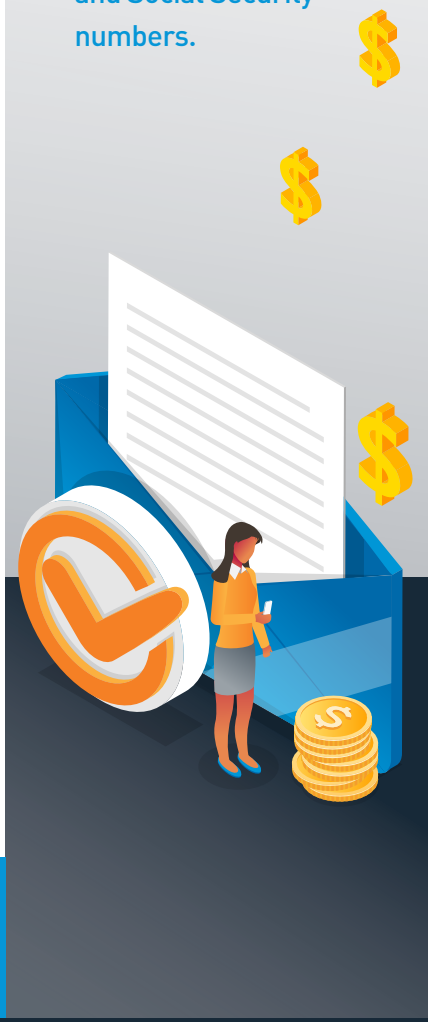
Tips for Employers

- Create a culture that encourages employees to verify instructions directly with those executives who are authorized to approve payments prior to releasing funds.
- Establish basic security practices and policies for employees, such as requiring strong passwords and multifactor authentication for employees to access areas of the network with sensitive information.
- Train staff on business email compromise and how to spot spoofed and spear-phishing emails.
- Have a separation of duty — the same employee should not be able to initiate and approve money movement.
- Educate staff about what to do or who to contact if they suspect they clicked on malicious content.
- If possible, configure an email gateway/system to flag external emails as "External," alerting employees to spoofing of internal personnel and to be extra careful about clicking links or opening attachments.
- Visit the Security & Privacy Center on pnc.com (www.pnc.com/ securitytips) for more tip sheets on strong passwords and social engineering.

Tips for Employees

- Call the appropriate executive/ manager to request validation or clarification of unusual payment requests prior to authorizing transactions or disclosing sensitive data, such as personnel records. Use a known phone number.
- Verbally confirm emailed instructions from a vendor or supplier to change payment methods or bank information. Call them on a known contact number.
- Do not deviate from established policies and procedures regarding payments, the transfer of funds or disclosure of sensitive data.
- Carefully check the email address of any individual requesting a transfer of funds or sensitive data; scammers may slightly vary a genuine address, adding a letter or changing punctuation to make it appear legitimate.
- Be cautious about sharing specific information about your job on social media sites. Attackers can use your profile information to gain knowledge about your company, your role and technology used, and target you with phishing or social engineering campaigns to execute this type of fraud.

Business email compromise is a type of fraud perpetrated via email in which a business is tricked into transferring funds to accounts controlled by criminals or handing over sensitive data, such as employees' names, addresses and Social Security numbers.



For more information regarding small business cybersecurity, visit the Federal Trade Commission website.

PNC BANK

CON PDF 0321-0107