Whitepaper

mimecast

Combating the Threat of Business Email Compromise

Overview

Business email compromise cost U.S. organizations more than $1.7 billion last year—and its impact is compounding faster than ever. Cybersecurity technology alone is not enough to combat the threat. Businesses can only succeed against the fast-growing threat of business email compromise through a combination of security awareness training, email security technology, and business process changes.

Key Challenges

- Business email compromise is the single biggest cause of cybersecurity-related financial losses—and it continues to grow rapidly.
- Because BEC phishing emails don't generally include malicious links or attachments, they cannot be detected using traditional email content scanning techniques.
- Attackers may also use BEC to scam your organization's customers or other members of your business ecosystem.

Introduction

Business email compromise (BEC) is a rapidly growing cyber threat that already causes greater financial losses than any other type of cybercrime. In 2019, BEC attacks cost U.S. businesses, governmental and other organizations at least $1.7 billion, according to the FBI's Internet crimes complaint center—more than three times as much as any other cybercrime.[1]

Each attack also results in much greater losses, on average, than other types of cybersecurity crime: victims reported average losses of nearly $75,000, according to the FBI. Some companies have lost tens of millions of dollars in BEC scams: in 2019, for example, a European subsidiary of one of the world's largest carmakers was the victim of a $37 million cybercrime based on a fraudulent invoice.[2] BEC has become the top cause of payment fraud attempts, overtaking other methods such as forged checks and stolen credit cards, according to the global Association for Financial Professionals.[3]

BEC attacks are expected to continue to skyrocket. Sixty percent of organizations have seen increases in impersonation/BEC attacks over the past year, according to research by Mimecast and Vanson Bourne. Gartner, Inc. forecasts that BEC phishing attacks will double every year, reaching more than $5 billion by 2023 and resulting in large financial losses for enterprises.

Recommendations

- Use a combination of security awareness training, advanced email security technology, and process changes to combat the threat of BEC.
- Effective security awareness training is key to reducing human error, which is a factor in all successful BEC attacks.
- Use an advanced email security solution to identify and prevent BEC attempts, including phishing emails that cannot be detected using traditional anti-malware tools.
- Use DMARC to prevent domain spoofing, protect your brand and stop attacks against your customers and business partners.
- Implement additional verification steps in payment-related processes such as requests for wire transfers or to change bank account information.

What is Business Email Compromise?

BEC attacks are email phishing scams that aim to trick people into making payments, or in some cases leaking sensitive information. These attacks typically use social engineering techniques to gain users' confidence. Attackers impersonate trusted people or entities—such as the company's CEO or one of its suppliers—and send phishing emails to individuals within the organization who have the authority to make payments. These attacks generally cannot be detected using traditional email scanning technology, because the phishing emails don't contain malware or malicious links.

Business email compromise attacks vary greatly in sophistication. Some attacks are carefully researched and targeted, and are extremely dangerous as a result. Others, such as gift card scams, are generally much more rudimentary—but still succeed far too often.

Attackers use a variety of techniques to create email messages look convincing. They may register internet domain names that closely resemble the names of their target organization or trusted suppliers, then send phishing emails from those domains. Another tactic is to create email accounts on widely used public email services like Gmail, and then use them to pose as executives sending emails from a personal address. Less sophisticated attacks may simply spoof the "sender" name in email messages to make them appear to have been sent from a trusted source.

For the most sophisticated BEC attacks, attackers carefully research their targets online, examining sources such as social media accounts and the organization's own web pages. This enables them to identify the individuals within the organization who have the authority to request and authorize payments, understand the relationships between them, and craft emails that incorporate the information needed to convince people that they're receiving a genuine payment request.

Business Email Compromise Attack Types

Most BEC attacks can be categorized into a few main types, although there are many variations.

1. Executive Impersonation

In this type of BEC exploit, an attacker posing as the CEO, CFO or another executive sends a payment request via email to someone with payment authority—an employee who works in purchasing or accounts payable, for example.

These attacks often begin with a brief, relatively informal message designed to draw the victim into an email conversation. The attacker may inject a feeling of urgency in order to pressure the victim into responding without taking the time to check whether the communication is legitimate. For example: "I'm tied up in a meeting and I need help right now, can you quickly help me with something?" Or, if they're sending email from a fake personal account: "I'm traveling on vacation and can't access the corporate systems, can you help?" After engaging the victim, the attacker evolves the conversation into a request for a high-value payment, generally via a fast, irrevocable method such as a wire transfer.

These BEC attacks are often particularly convincing because they exploit the existing relationships and roles within the organization. By conducting online reconnaissance, the attacker already knows that the victim reports to the CFO, so they impersonate the CFO in their email request. They find personal information about the CFO or their victim on the corporate website or social media, so they can include a few details to make the email look more authentic. The victim is accustomed to receiving and executing payment requests from the CFO; in fact, it's their job to do so. Overall, the BEC attack simply appears to be a normal request that's part of everyday operations—and as a result, it's more likely to be successful.

2. Supplier impersonation

Many business email compromise attacks impersonate an organization's suppliers, using emails that include fake invoices or changes in banking information that divert payments into an account set up by the attacker. As with executive impersonations, these attacks often exploit existing relationships in order to look more convincing. For example, attackers may set up domains or create web pages that are similar to those of real suppliers, in addition to forging invoices or other business documents. In a scam perpetrated on Cabarrus County, N.C., an attacker emailed a fake invoice purporting to be from the construction firm managing the construction of a new high school. The attack defrauded the local government out of more than $2.5 million, most of which was never recovered.[4]

3. Payroll diversion

These attacks are usually directed at someone in human resources. They typically appear to be requests from an employee to change the employee's bank account details for direct deposit of wages. In reality, they channel the employee's wages into an account controlled by the attacker.

4. Gift card scam

These are often spam email campaigns that aim to get employees to buy gift cards and send the codes to the attacker. These attacks have become very common, perhaps partly because they require less work than other kinds of BEC attack. Many gift card scams are unsophisticated, with little attempt to create a convincing fake persona for the sender. Nevertheless, because these email campaigns are sent to very large number of people, even a low success rate can be financially rewarding for the attackers. In some cases, the same email template is used to mass-mail vast numbers of people; the template is translated into different languages for use worldwide.

5. Data theft

This variant of business email compromise attacks seeks to extract personal information or other sensitive data instead of requesting payments. Attackers email employees in human resources or payroll functions, requesting W2 or other personal information. The information may subsequently be used for identity theft, tax fraud or other financial scams.

6. Internal and outbound attacks

Attackers may take over internal email accounts using malware or phishing emails designed to steal credentials, then use these email accounts to send internal payment requests to people within the organization. They may also use these email accounts to target the organization's customers or business partners in BEC attacks. These attacks are particularly hard to detect because they originate from legitimate organizational email addresses. Other attacks on your organization's ecosystem may simply spoof your organization's identity without actually compromising your corporate email system: malicious actors impersonate your organization using fake email addresses or domains, and use them to launch BEC attacks on your customers or partners.

Detecting and Preventing BEC

Detecting and preventing BEC presents a complex challenge. BEC attacks generally can't be detected using traditional email scanning technology, because BEC phishing emails don't include malware or malicious links. Instead, organizations must use a combination of security awareness training, advanced email security technology capable of identifying impersonation attempts, and more rigorous payment authorization processes.

Security Awareness Training

All successful business email compromise attacks include an element of human error—an attack only succeeds if a user is deceived into making a payment. Cybersecurity awareness training can significantly reduce the likelihood of human error, and therefore plays an essential role in any strategy to prevent BEC.

Security awareness training should educate users about the specific techniques used in phishing attacks and BEC attempts. To make cybersecurity training stick, educational sessions must be frequent, engaging, brief, and continuously updated to evolve with cybercriminals' latest techniques.

Training should include phishing simulations that enable the organization to objectively measure employees' awareness and ability to spot attacks. A key message to communicate to employees is that email alone is not an adequate form of authentication—it must be supplemented with other methods, like verification phone calls to the vendor. For example, suppliers shouldn't be able to change their payment instructions with a simple email request, which is vulnerable to spoofing in BEC attempts.

Organizations should identify higher-risk employees and provide them with additional or individualized training. These employees may be identified by their roles: users who are responsible for payments or have privileged access for other reasons may be particularly likely to be targeted. Some email security solutions can also identify which internal users are most heavily targeted in phishing campaigns. The organization can then offer individualized training to those users.

As part of security awareness training, it's important to provide users with a clear mechanism for reporting BEC attempts as soon as they are detected.

Organizations should also consider extending training to other key members of their business ecosystem, including customers, suppliers, and partners. This helps to protect the security of the entire ecosystem. Among other benefits, it helps to prevent attackers from exploiting the brand by impersonating the organization in attacks on other ecosystem members.

Advanced Email Security Services

No single technology can stop all BEC attacks. However, advanced email security services can identify and prevent many BEC attempts. These cloud-based security email gateway services can work with enterprise email systems such as Office 365, analyzing incoming and outgoing email to detect and prevent threats. To be effective, security technologies must protect users across all the devices they use, including desktop, mobile and personal devices.

Impersonation phishing attacks can be hard to spot. Malicious actors can use a variety of methods to disguise their attacks as genuine emails; there's no single indicator that can be used to reliably identify an incoming email as a BEC phishing attempt. Therefore, an email security solution must search for a variety of warning signs to determine the probability that an incoming email is an impersonation attempt.

When attempting to create convincing phishing emails, malicious actors can only manipulate a limited number of message characteristics. Essentially, they can create fake sender information, craft persuasive text in the body or subject of the message, and attach files. An advanced email security solution can examine all these characteristics to determine the probability that inbound email is malicious. If enough indicators are found, the service will reject or flag the message.

Typical warning signs include:

- Sender display names that don't match the real sending domain, and therefore may indicate a spoofing attempt. For example, an attacker may create emails that appear to come from users within your organization but are actually sent from an external domain.
- Emails sent from domain names that are similar to your organization's domain name, or to those of well-known brands or trusted third parties.
- Emails from recently registered domains, which indicate that the domain may have been registered for malicious purposes.
- Keywords in the body of the message. All BEC attempts eventually make a request, typically for a payment or sensitive data. To make that request, an email must include specific terms, such as "wire transfer." An advanced email security solution can search the message text to detect a wide variety of these keywords.

DMARC
DMARC is an email validation standard that protects against domain spoofing. It can help your organization prevent malicious actors from exploiting your brand in BEC attacks on your customers or other organizations. It also enables email providers to filter out many incoming BEC attacks before they reach your organization.

To use DMARC to protect your brand, you first need to identify all the domains associated with your organization. Then you set policies for what email systems should do if they receive emails that are spoofing those domains. Email systems check incoming emails against your DMARC policies and determine whether to accept, reject or quarantine mail as a result. Most major email platforms apply DMARC checks to the email they receive. Your organization receives reports from these providers that help you track and prevent brand exploitation attempts. Because DMARC can be complex to configure and the reports difficult to read, it's advisable to use a commercial tool to manage and analyze your DMARC implementation.

Process Changes
Changes to payment processes can also help to prevent BEC scams, according to Gartner Inc. For example, similar to a multi-factor authentication process, the organization can stipulate that any email requests from vendors to change bank account information must be verified using other methods, such as phone calls. In addition, processes such as changing bank account information can be moved to financial systems such as accounts payable portals that require additional authentication steps.

Conclusion:

Combatting the fast-growing threat of business email compromise is not easy—but it is possible. Preventing business email compromise attacks requires a coherent strategy that encompasses security awareness training, email security technology, and changes to internal processes. An effective strategy will not only help to protect your organization against thefts of money and sensitive data; it can also help to protect your customers, your business partners, and your reputation.

---

1. 2019 Internet Crime Report, FBI Internet Crime Complaint Center | 2. Toyota Parts Supplier Hit By $37 Million Email Scam, Forbes | 3. 2020 AFP Payments Fraud and Control Survey, Association for Financial Professionals | 4. Cabarrus County Government targeted in social engineering scam, Cabarrus County