Top Strategies to Prevent Business Email Compromise (BEC)

Business Email Compromise (BEC) is a cyberattack where criminals trick employees into making unauthorized transactions or sharing sensitive data. It poses significant risks, including financial loss and damage to a company’s reputation. In this article, we’ll explain what BEC is, how it works, and how you can protect your business.

Understanding Business Email Compromise (BEC)

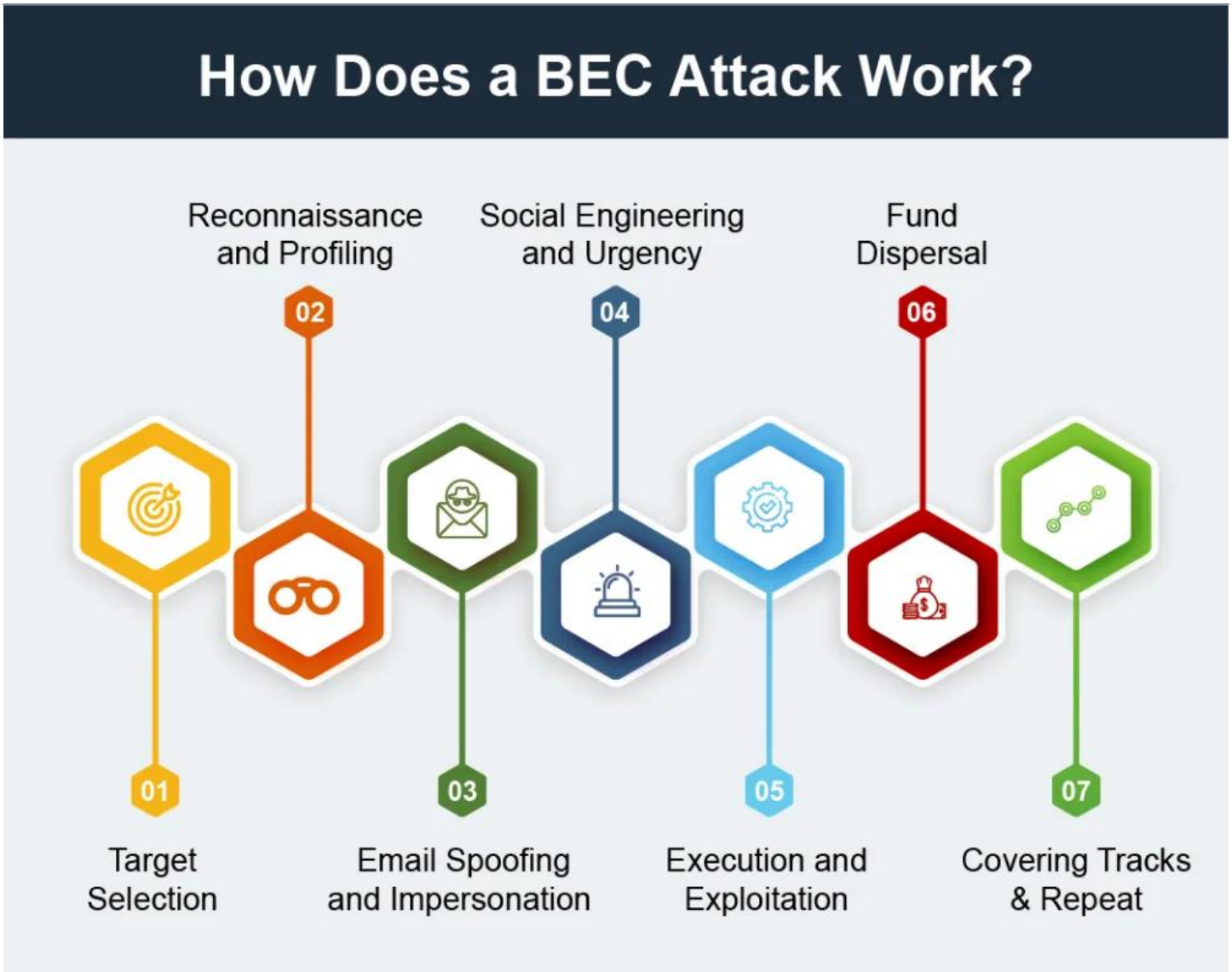
Business Email Compromise (BEC) is a targeted cyberattack where malicious actors deceive employees and executives into transferring funds or sensitive data to fraudulent accounts. Unlike mass phishing campaigns, BEC scams are highly targeted, leveraging detailed knowledge of business operations and human psychology to exploit trust and urgency. The primary goal of these attacks is to trick employees into making unauthorized financial transactions or revealing confidential information.

BEC attacks often mimic routine workflows, making it easier for attackers to catch victims off guard. For instance, fraudsters may impersonate CEOs, CFOs, or other high-level executives, sending urgent requests for financial transfers or sensitive data. These emails are crafted to appear legitimate, often using free online tools and services to enhance their realism. The simplicity and reproducibility of these scams make them an attractive option for cybercriminals, leading to a rise in BEC incidents.

The consequences of a successful BEC attack can be devastating. Businesses of all sizes face significant financial losses, productivity disruptions, and reputational damage. Poor email protection directly correlates with these security breaches, emphasizing the need for robust defenses to prevent BEC threats.

Understanding the nature and impact of BEC is the first step in fortifying your organization against these insidious attacks.

How BEC Attacks Work



Step 1: Target Selection

Cybercriminals identify high-value targets based on their access to financial resources or sensitive information. They research companies and individuals, often using publicly available data from websites, social media, or previous breaches.

Step 2: Reconnaissance & Profiling

Attackers build detailed profiles of their targets, studying email habits, communication styles, and business relationships. This helps them craft highly convincing phishing emails that appear legitimate.

Step 3: Email Spoofing & Impersonation

Using tactics like domain spoofing, lookalike domains, or compromised accounts, attackers pose as trusted vendors, executives, or business partners. They send emails that mimic real communication patterns to avoid suspicion.

Step 4: Social Engineering & Urgency

To pressure the victim into acting quickly, attackers use psychological manipulation—urgent payment requests, CEO fraud (impersonating executives), or invoice scams. The goal is to bypass normal verification procedures.

Step 5: Execution & Exploitation

Victims may be tricked into:

- Initiating wire transfers to fraudulent accounts
- Updating payment details to attacker-controlled accounts
- Sharing sensitive financial or business information

Step 6: Fund Dispersal

Once the money is transferred, attackers rapidly move it across multiple accounts, often internationally, to evade detection and recovery efforts.

Step 7: Covering Tracks & Repeating the Attack

Cybercriminals may delete emails, set up auto-forwarding rules, or use compromised accounts for further attacks, ensuring persistence and maximizing financial gain.

9 out of 10 attacks are delivered by email, using phishing, macros and scripts, and social engineering.

- We can help you stay protected. Discover:
- All about Fidelis Network® Mail Sensor
- Data theft prevention
- Malware Detection Engine

Download Datasheet

Common Types of BEC Scams

The FBI has identified five major types of BEC scams, each exploiting different aspects of business operations. The most common type is CEO fraud, where attackers impersonate the CEO or other high-ranking executives to request urgent financial transfers from the finance team. These fraudulent emails often appear legitimate, leveraging the authority of the impersonated executive to compel quick action.

Another prevalent scam is the bogus invoice scheme, in which scammers masquerade as vendors and send altered invoices to redirect payments to fraudulent accounts.

Account compromise scams occur when hackers gain access to an employee’s email account and use it to request unauthorized invoice payments. These attacks are particularly effective because they originate from legitimate email addresses, making them more difficult to detect.

Other types of BEC scams include attorney impersonation and data theft. Attorney impersonation scams target less experienced employees with urgent legal requests, exploiting their lack of familiarity with legal procedures. Data theft attacks focus on obtaining personal information from HR or finance employees, which can then be sold or used for further malicious activities.

Understanding these common types of BEC scams can help organizations develop targeted defenses to prevent such attacks.

Key Characteristics of BEC Emails

BEC emails are crafted to appear legitimate and often include urgent requests for action, prompting immediate responses from the recipient. These emails typically lack the usual red flags like links, images, or attachments, allowing them to evade traditional **malware detection methods**. Instead, they rely on manipulation techniques to compel the recipient to take specific actions.

Attackers frequently spoof email addresses and impersonate trusted vendors to enhance the credibility of their messages. By referencing real events or relationships drawn from social media, they build a convincing narrative that deceives the recipient. Persuasive language is a common feature of BEC emails, designed to manipulate targets into complying with the request.

The sophisticated impersonation tactics used in BEC emails make them difficult to detect. These emails often request confidential information about employees, partners, or investors, revealing sensitive information that complicates detection efforts. The use of AI tools enables attackers to craft highly personalized and grammatically perfect emails, further challenging traditional detection methods.

Recognizing these key characteristics can help employees identify and respond to BEC threats more effectively.

Business Email Compromise vs Phishing

It’s easy to confuse a business email compromise attack with traditional phishing, but there are important differences. Phishing usually involves mass emails with malicious links or attachments, designed to steal credentials or deliver malware. On the other hand, BEC scams are highly targeted. Instead of relying on malicious files, they exploit trust and authority by impersonating executives, vendors, or partners to manipulate payments or sensitive information.

Put simply, phishing casts a wide net, while BEC attacks are precision strikes aimed at high-value financial fraud. Understanding this distinction is critical for implementing the right defenses, as stopping BEC requires both technical controls and strong internal processes.

Real-World Examples of BEC Incidents

Real-world examples of BEC incidents highlight the significant financial and reputational damage these attacks can cause. Between 2013 and 2015, a sophisticated BEC attack led to a financial loss of $121 million for Facebook and Google. In 2019, Toyota Boshoku Corporation suffered a $37 million loss due to a BEC scam. These incidents underscore the high stakes involved and the need for robust defenses.

FACC, an aerospace company, incurred a loss of €42 million ($47 million) in 2015 due to a BEC attack. The City of Lexington, Kentucky, lost $4 million in a BEC scam in 2022. These high-profile

cases demonstrate the sophistication of BEC threats and the severe financial implications for businesses.

These examples serve as a stark reminder of the importance of proactive measures to prevent BEC attacks. By understanding the potential impact and learning from these incidents, organizations can better **prepare their defenses** and avoid becoming the next victim of a successful BEC attack.

Evolving Trends in BEC Security

The nature of BEC phishing has evolved significantly over the past few years. Early scams focused almost entirely on wire transfer fraud. Today, attackers are also targeting payroll diversions, vendor payment fraud, and even requesting gift cards from unsuspecting employees.

A worrying trend is the rise of AI-generated content. Attackers are now using artificial intelligence to draft convincing emails or even voice deepfakes to impersonate executives. Some campaigns also combine BEC attacks with credential theft or malware to deepen access before initiating fraud.

These developments highlight why BEC security cannot rely solely on email filters or gateways. Organizations need to continuously adapt their defenses with layered controls, employee awareness, and verification processes to stay ahead of evolving tactics.

Strategies for Preventing BEC Attacks

Preventing BEC attacks requires a multifaceted approach that combines technical defenses and employee training. Employing **advanced email security solutions**, such as email authentication protocols and anomaly detection systems, is essential for protecting against BEC threats. These technical measures help detect phishing attempts and other malicious activities, reducing the risk of successful attacks.

Regular security training and awareness campaigns are equally important. Educating employees about the tactics used in BEC scams and conducting phishing simulations can significantly improve an organization’s defenses.

Continuous monitoring and security audits are also crucial for preventing future BEC incidents. By implementing these strategies, businesses can create a robust defense against BEC attacks.

Practical Business Email Compromise Prevention Checklist

Beyond technical safeguards, organizations need practical policies to minimize the success of BEC scams. Some essential steps include:

- **Dual Approval on Payments:** Require more than one approver for large transactions or vendor account changes.
- **Out-of-Band Verification:** Always verify bank account or payment changes with a second communication channel such as a phone call.
- **Vendor Management Controls:** Maintain updated vendor records and revalidate account details for unusual or high-value requests.
- **Mandatory MFA:** Enforce multi-factor authentication across all email accounts to prevent unauthorized access.
- **Monitor Forwarding Rules:** Attackers often set hidden mailbox rules to intercept or

forward emails; monitoring these can expose compromise early.
- **Targeted Awareness Training:** Train finance, HR, and executive staff to recognize red flags like urgent payment requests or unusual language.

This blend of policies and awareness training creates a strong foundation for business email compromise prevention.

Use Advanced Email Security Solutions

Investing in advanced email security solutions is vital for defending against BEC, phishing, and malware attacks. These solutions can detect anomalies and threats in emails, providing real-time threat remediation capabilities. Features like **anomaly detection** and malware and anti-spam solutions enhance overall email security against BEC threats.

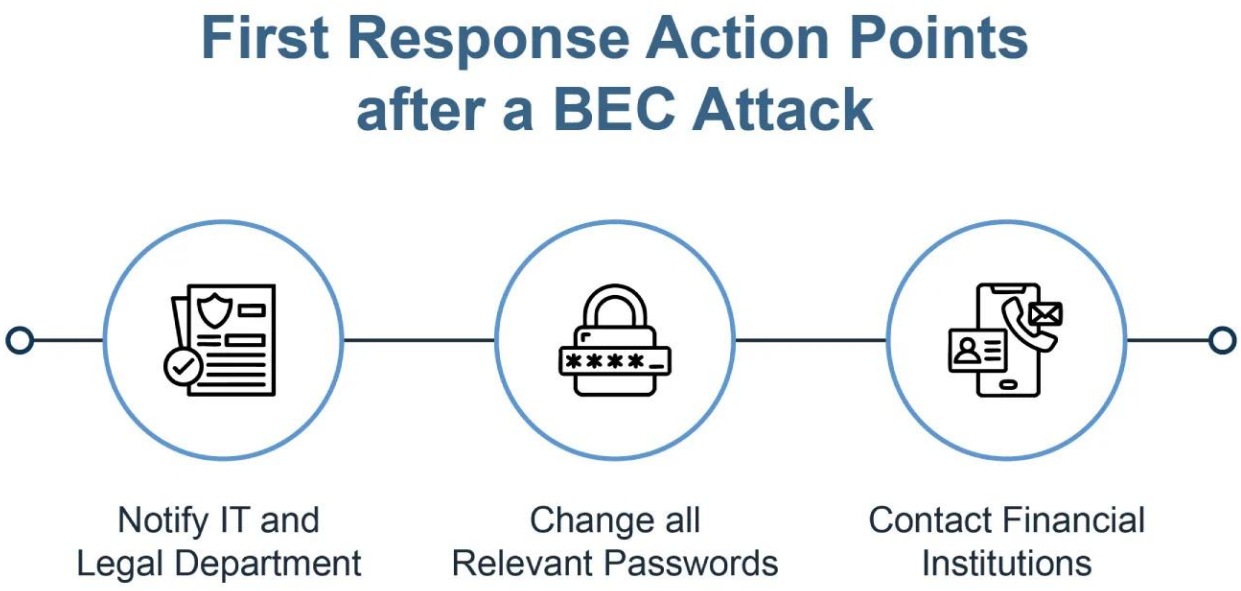
Email authentication protocols, such as DMARC, play a crucial role in enhancing email security. DMARC allows domain owners to set policies on how to handle emails that fail authentication checks, improving overall email security. By ensuring emails have authenticated matches in SPF, these protocols prevent unauthorized emails from reaching employee inboxes.

Implementing advanced email security solutions is a critical step in mitigating BEC risks.

Conduct Regular Employee Training

Regular training sessions are essential to educate employees about scamming techniques and help them recognize BEC threats effectively. Phishing simulations are an effective method for training employees to identify and respond to BEC attacks. These simulations help employees experience realistic scenarios and learn to spot red flags in email communications.

Ongoing communications about BEC threats are crucial to keeping employees informed and vigilant. Employees should be encouraged to verify suspicious emails by calling the sender or sending a separate email instead of replying directly. By fostering a culture of awareness and vigilance, organizations can significantly reduce the risk of falling victim to BEC scams.



Technical Measures to Mitigate BEC Risks

Employing technical methods like DKIM, SPF, and DMARC is essential to bolster defenses against BEC threats. These protocols help verify the authenticity of email senders and prevent email spoofing, enhancing overall email security. Fidelis Security's advanced solutions provide extensive visibility into network traffic and communications, allowing for the detection of BEC threats.

By implementing these technical measures, organizations can create a robust defense against BEC attacks. These protocols not only help prevent unauthorized access but also ensure that legitimate emails are correctly authenticated, reducing the risk of successful BEC attempts.

Domain Keys Identified Mail (DKIM)

DKIM, or DomainKeys Identified Mail, is a protocol designed to validate the authenticity of outgoing emails. It works by preventing email spoofing through the verification of email signatures against the domain's public keys. This verification process ensures that emails are genuinely from the claimed sender, reducing the risk of fraudulent emails reaching recipients.

Implementing DKIM helps protect against email spoofing and enhances overall email security. By ensuring that only legitimate emails are delivered, DKIM plays a crucial role in mitigating BEC risks and protecting sensitive information from unauthorized access.

Sender Policy Framework (SPF)

The Sender Policy Framework (SPF) verifies email sender authenticity against approved domains. It helps prevent email spoofing by defining which mail servers are allowed to send emails on behalf of a domain. Domain owners can create a list of authorized mail servers, enhance the legitimacy of emails and reduce the risk of fraud.

Domain-Based Message Authentication, Reporting & Conformance (DMARC)

DMARC, or Domain-Based Message Authentication, Reporting & Conformance, allows domain owners to publish email authentication requirements, enhancing the overall security of digital communications. By aligning with protocols like DKIM and SPF, DMARC ensures that emails are properly authenticated, reducing the risk of email spoofing and other malicious activities. This alignment is crucial in identifying and mitigating potential BEC threats, as it provides a comprehensive framework for email authentication.

Additionally, DMARC enables domain owners to analyze email content for malicious intent, going beyond just validating the sender's authenticity. This dual approach of authentication and content analysis makes DMARC a powerful tool in the fight against BEC, providing an extra layer of security to protect sensitive information and prevent unauthorized access.

Developing a Response Plan for BEC Incidents

Developing a robust response plan for BEC incidents is crucial for minimizing damage and ensuring a swift recovery. The first step in any response plan is to isolate the incident, preventing further unauthorized access or fraudulent activity. This involves immediate containment measures, such as disconnecting compromised systems from the network and securing affected email accounts.

Once the incident is contained, a thorough investigation should be conducted to assess the extent of the damage and identify the root cause of the attack. This includes analyzing email logs, reviewing financial transactions, and gathering evidence to support any legal actions. It's also important to alert internal cybersecurity teams and notify banks if financial transactions are involved.

Establishing strong policies to validate and authorize financial transactions can significantly reduce BEC risks, while clear protocols for verifying unexpected payment requests further help mitigate BEC attacks.

Post-incident, it's crucial to evaluate the response and update the incident response plan to improve future readiness. Incorporating legal counsel in the response process ensures adherence to regulatory requirements and effective communication with affected parties. A focused strategy specifically targeting BEC attacks is essential since these threats often lack dedicated security controls.

By following these steps, organizations can effectively manage BEC incidents and enhance their overall security posture.

BEC Attack Response Checklist (First 72 Hours)

A quick, structured response can make the difference between containing a BEC attack and suffering large-scale financial or reputational damage. Organizations should follow a clear timeline:

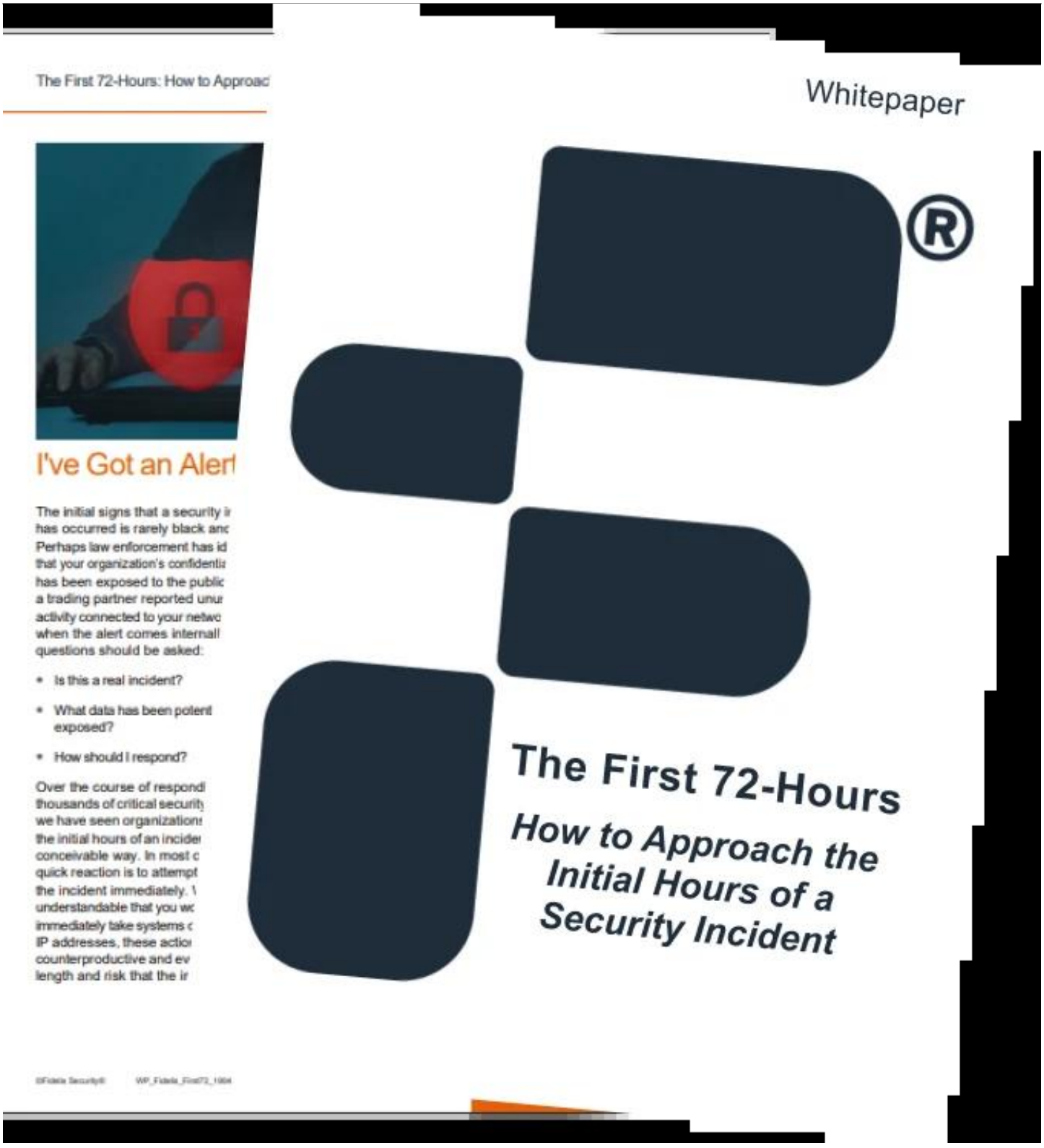
- **First 24 Hours:**
  - Notify your bank's fraud department to attempt recovery of funds.
  - Lock and reset any compromised email accounts.
  - Alert internal security and legal teams.
- **Within 48 Hours:**
  - File a report with the FBI IC3 (or relevant local cybercrime authority).
  - Begin forensic investigation to determine how the email compromise occurred.
  - Contact affected vendors or partners if their details were used.
- **Within 72 Hours:**
  - Patch process gaps (e.g., payment verification or weak approval workflows).
  - Update staff training with lessons from the incident.
  - Document the case to improve future response readiness.

Following this BEC phishing response checklist ensures that financial losses are minimized, and future resilience is strengthened.

Critical Incident Response: Key Steps for the First 72 Hours

- What data has been potentially exposed?
- Incursion detection and Persistence detection
- How should I respond?

Download the Whitepaper



The Role of Fidelis Security in BEC Prevention

Fidelis Security plays a pivotal role in BEC prevention by providing advanced solutions that offer full visibility, deep insights, and rapid response capabilities. These solutions help security teams worldwide protect, detect, respond to, and neutralize advanced cyber adversaries, including those involved in BEC attacks. **Fidelis Security platforms** enhance email protection through comprehensive visibility into email threats, allowing organizations to understand potential BEC threats and their origins.

Fidelis's **rapid response capabilities** enable organizations to quickly detect and address BEC threats before they escalate. By providing solutions for email security, Fidelis aims to significantly reduce the risks associated with sophisticated email attacks, including BEC.

Fidelis Network® Mail Sensor, for instance, enhances encrypted email protection, providing an extra layer of security for sensitive communications. With Fidelis Security, organizations can stay one step ahead of cybercriminals and safeguard their digital communications against BEC threats.

Conclusion

Concluding, it can be said that Business Email Compromise (BEC) represents a significant threat to organizations, exploiting human trust and routine business operations to cause devastating financial and reputational damage. Understanding the mechanics of BEC attacks, recognizing the common types of scams, and identifying the key characteristics of BEC emails are crucial steps in fortifying defenses against these threats. Real-world examples of BEC incidents highlight the high stakes involved and the need for robust prevention strategies.

Implementing advanced email security solutions, conducting regular employee training, and employing technical measures such as DKIM, SPF, and DMARC are essential for mitigating BEC risks. Developing a comprehensive response plan ensures that organizations can effectively manage BEC incidents and minimize damage. Fidelis Security's advanced solutions provide the necessary tools and insights to protect against BEC threats, enabling organizations to stay ahead of cybercriminals. By taking proactive measures, businesses can safeguard their digital communications and ensure a secure operational environment against BEC attacks.

Frequently Ask Questions

What is Business Email Compromise (BEC)?

Business Email Compromise (BEC) involves targeted cyberattacks where attackers deceive employees or executives into transferring funds or sensitive information to fraudulent accounts by impersonating trusted sources. It is crucial for organizations to implement robust security measures to mitigate this risk.

How do BEC attacks typically work?

BEC attacks typically work by targeting individuals, developing detailed profiles, spoofing email addresses, and employing social engineering tactics to coerce victims into transferring funds or divulging sensitive information.

What are some common types of BEC scams?

Common types of BEC scams include CEO fraud, bogus invoice schemes, account compromise, attorney impersonation, and data theft, each targeting different vulnerabilities within business operations.

How can organizations prevent BEC attacks?

To effectively prevent BEC attacks, organizations should implement advanced email security measures, conduct regular employee training, utilize DKIM, SPF, and DMARC protocols, and establish a robust response plan. These steps collectively enhance security and mitigate risks associated with business email compromise.

What role does Fidelis Security play in BEC prevention?

Fidelis Security plays a crucial role in BEC prevention by providing advanced solutions that ensure full visibility and rapid response capabilities, enabling organizations to effectively protect against, detect, and neutralize BEC threats.