How to Protect Organizations Against Business Email Compromise Phishing

28 March 2025 - ID G00788656 - 15 min read

By: Franz Hinner

Initiatives:Infrastructure Security; Build and Optimize Cybersecurity Programs

BEC attacks use targeted social engineering to succeed and maximize payout to attackers, making them a fast-growing threat to organizations. This research guides security and risk management leaders in upgrading their existing technologies and processes to protect against this threat.

Additional Perspectives

- Summary Translation: How to Protect Organizations Against Business Email Compromise Phishing (10 January 2024)

Overview

Key Findings

- Endpoint protection platform (EPP) and endpoint detection and response (EDR) solutions do not protect against business email compromise (BEC) attacks, as BEC emails usually do not contain any malware/malicious links and can't be filtered by basic anti-spam and anti-malware solutions.
- BEC phishing is commonly combined with account takeover (ATO) of the sender's account. As a result, the recipient or systems using only BEC protection solutions have no means to recognize that the email is not from a genuine user.
- BEC phishing emails resemble regular email content, and aim to exploit business process errors and immature practices involving funds/sensitive data transfer via email. This allows the attacker to change payment details and wiring instructions via email.
- Human errors account for approximately 74% of all security breaches. Social engineering attacks capitalize on these human errors, and they now comprise 50% of all security incidents.

Recommendations

Security and risk management (SRM) leaders responsible for infrastructure security should:

- Maximize protection against BEC by seeking out and implementing AI-based secure email gateway solutions that offer advanced BEC phishing protection, behavioral analysis, imposter detection and internal email protection.
- Supplement your existing email security solutions with additional controls to further reduce the risk of BEC attacks like ATO and domain abuse.
- Update processes around user and email authentication for financial/data transactions, and migrate high-risk ad hoc transactions to authenticated systems to bridge gaps in business process errors.
- Educate users and suppliers/partners on the different types of BEC phishing, and preventive measures for protection, by conducting user awareness training at regular intervals.

Introduction

BEC phishing attacks continue to pose a significant financial and data breach risk for organizations. A BEC attack impersonates or takes over a legitimate user email, and mostly targets high-ranking individuals, such as the CEO or others authorized to conduct fund transfers.

According to the 2023 Verizon Data Breach Investigations Report, more than 50% of social engineering attacks, such as pretexting, phishing and credential thefts, are related to BEC. The median amount stolen from these attacks has also increased over the last couple of years, from $40,000 to $50,000. [1] Sometimes, spoofing the sender's email address also tricks the receiver into sending money to the attacker. According to the FBI's Internet Crime Report 2022, around 22,000 complaints were registered for BEC attacks in 2022, and the total loss incurred was around $2.7 billion. [2]

Phishing protection is the only technical protection layer for BEC emails. And detecting BEC with traditional approaches such as EDR/EPP or security service edge fails because these attacks have simple execution techniques (as no malware or ransomware is involved), aiming to exploit gaps in business processes and human errors.

If the BEC protection filter fails to identify a threat, the attacker can take over the user's account (an ATO attack). The damage caused by these attacks reaches well beyond financial losses. If a supplier or customer falls for a BEC attack that purports to come from a known organization, it can harm the established trust in the existing relationship and the organization's reputation as well.

How can SRM leaders protect internal users from BEC attacks and also minimize risk to their suppliers and customers? This research examines types of BEC attacks and steps that leaders can take to prepare the organization to counter this simple yet destructive type of attack.

Analysis

There is no single technology solution to BEC; rather, it's a combination of technology upgrades, investment in additional controls, process improvements and user awareness.

Upgrade to an AI-Based Secure Email Solution, Including Internal Email Protection

A single email security solution might not always be the best choice for all organizations to protect against BEC attacks. However, consolidating different technologies can improve defense against BEC. SRM leaders should implement one of the following combinations of technologies to defend against BEC attacks. Table 1 outlines some of those combinations.

Table 1: Different Types of BEC Protection Solutions

Secure Email Gateway (SEG)	**Built-In Solution (Cloud Email Providers Such as Microsoft or Google Suite)**	*Integrated Cloud Email Security (ICES)*
SEG +	Built-in-solution +	ICES
SEG only		
SEG +		ICES
	Built-in solution +	ICES
SEG +	Built-in solution	

Source: Gartner (August 2023)

More details on each type of solution appear below.

SEG Solutions

Most modern (AI-based) secure email gateway (SEG) solutions are adequate to protect against legacy attacks, like phishing and malware-based emails. They also have advanced technologies for detecting BEC, including pattern detection based on machine learning (ML), and relationship graphs and mailbox-level behavior analysis to analyze previous email relationships and identify anomalies.

Internal Email Protection and ICES/API-Based Solutions

The existing built-in email solutions provide overall email security; however, as stand-alone products, they are insufficient to detect account takeover and vendor email compromise (VEC) attacks. Internal email protection should also be used to detect account takeover. Account takeover is harder to identify, so analysis of content with both rules and natural-language processing should be used. Integrated cloud email security (ICES) and SEG solutions with natural-language understanding, ML and social graph analysis improve protection against BEC. SRM leaders who choose to use an existing cloud email solution like Microsoft Office 365 should combine it with ICES solutions that provide specific capabilities focused on advanced phishing and BEC (see Market Guide for Email Security).

It's essential to be aware of false positives, which occur when an event is predicted to be positive but is actually negative. ML algorithms can generate false positives, but there are ways to avoid them. These strategies include using a large and representative dataset, tuning the model's parameters, and using a more conservative threshold. By implementing these strategies, false positives in ML models can be reduced, ultimately improving prediction accuracy. For more information, please refer to What Should I Know About Machine Learning?

Existing Built-In Solutions

Email security, especially for cloud solutions like Office 365, begins with implementing the critical controls and correct configurations. Navigate Microsoft's native security capabilities and third-party options, and establish a secure Microsoft 365 environment.

The best option to reduce BEC attacks would be to invest in a built-in solution (Microsoft or Google), along with a SEG and ICES solution. However, a customer's risk appetite and budget will determine which one (or more) of the solutions they choose to use. SRM leaders should choose a solution that uses AI and/or ML techniques to continuously adapt to organizational sending patterns, rather than a prebuilt model.

Gartner recommends using all of the existing tools/solutions to their full capabilities before adding new ones to the mix. Lastly, remember that properly configured tools protect better than many tools that are misconfigured.

Implement Additional Technology Controls

When chosen and configured correctly, email security solutions can protect against most of the inbound BEC attacks, but the risk can be further mitigated by using a variety of complementary security resources, such as:

- Domain-based message authentication and conformance (DMARC)
- Mail security orchestration automation and response (MSOAR)
- Identity and access management (IAM) tools
- Multifactor authentication (MFA)

Account takeovers may be detected by one or more of these nonemail security solutions, but they cannot be absolutely eliminated. Organizations can choose to implement one or more of these additional controls based on their risk appetite and current threat landscape (see Ignition Guide to Conducting an Enterprise Risk Assessment and How to Respond to the 2023 Cyberthreat Landscape).

Authenticate Email Domains and Reduce Domain Misuse With DMARC

Email is a fundamentally unauthenticated communication. The name displayed by an email client doesn't need to match the actual sender or return address. Various standards have been introduced to try to retrofit more security into SMTP with limited success: Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and DMARC.

The adoption of DMARC is quite high among global enterprises and government organizations. SRM leaders should implement DMARC in particular, as it will help to prevent exact domain name spoofing. Organizations should seek out vendors and suppliers with active DMARC policies. Also, existing vendors and suppliers should be encouraged to implement DMARC to protect against "internal spoofed email" and "external spoofed email to supplier/partner" attacks.

The deployment, configuration and maintenance of DMARC can be challenging, depending on the size and number of domains in an organization. SRM leaders may elect to use a third-party tool or service to implement, manage and monitor DMARC. This will enhance email security, as emails can be rejected if they fail DMARC.

Triage Emails and Automate Detection and Response With MSOAR

SRM leaders should implement a threat detection and response system like MSOAR for triaging suspect emails reported by end users, incident response, and investigation. These solutions help to reduce the response time and human fatigue associated with carrying out simpler tasks such as triaging alerts and user-reported phish emails on a daily basis by automating them. Several email security vendors offer a focused MSOAR product and/or service. Many SOAR vendors include email investigation workbooks (see Market Guide for Security Orchestration, Automation and Response Solutions).

Gain Location Intelligence and Identify Access Behaviors With IAM Solutions

SRM leaders should utilize IAM tools, as they are a critical add-on, and should be used to monitor and alert on unusual behavior, especially “impossible travel” logins. Often, this can be part of MFA or access management solutions (see Magic Quadrant for Access Management). Other techniques, like looking for atypical logins and forwarding rules, can also alert potential account takeovers. For example, Microsoft Azure Active Directory Identity Protection can alert when a user logs in from a different location.

Prevent Account Takeover With Multifactor Authentication

Legacy out-of-band methods (for example, those using SMS) are deprecated. MFA, in particular, is critical to reducing ATO attacks when passwords have been compromised. SRM leaders should leverage the use of different types of tokens, such as mobile push methods, one-time password hardware tokens and Fast Identity Online v2 (FIDO2) security keys to ensure better security against ATO attacks (see Innovation Insight for Many Flavors of Authentication Token).

In many implementations, conditional access rules can be used to bypass MFA for access from a trusted enterprise network or a trusted endpoint device, to improve user experience (UX) when ATO risk is low.

UX can be further improved in remote access situations by “remembering” MFA from a known endpoint device for a configurable period (typically seven days). Richer analytics approaches (for example, Azure AD Identity Protection) can dynamically modify MFA behavior to address variable risks, and thus permit longer periods between fixed MFA prompts.

Upgrade SOPs for Transfer of Funds and Sensitive Data via Email

Revise Your Vendor Risk Management Strategy

Your vendor risk management (VRM) strategy should include BEC awareness when formally reviewing the candidate’s processes and practices. SRM leaders should ensure that policies are in place to convey to external parties that changes to payment destinations will not be requested at the time of payment. Also, ensure that any such change is confirmed by an appropriate second channel where company officials are confident in the identity of the requestor. Adding this policy to an automatic disclaimer at the end of each external email can be used to reiterate the message. A specific email address or contact should be provided for reporting suspicious requests.

Investigate All Ad Hoc Requests for Bank Account Updates

Internal financial controls should include steps to independently verify any changes to payment details, especially when transactions are sourced from email and represent a material risk (i.e., large transactions and sensitive data requests). These transactions could include changes in payroll payments or the purchase of gift cards (another common BEC technique). To add a verification control, move ad hoc processes, such as bank account change and wiring instructions, to more authenticated systems such as Workday or accounts payable portals (see Magic Quadrant for Procure-to-Pay Suites).

Create a Playbook for Reporting and Recovering From BEC Attacks

If a user falls victim to a BEC attack, it's important that they report it to their financial organization as quickly as possible, to increase the possibility of recovering lost funds. The Recovery Asset Team of the FBI helps the victims to respond to reported events.

Depending on the nature of the fraud, it can take some time before the victim realizes it has occurred. However, it is still important to report it as soon as it's identified. As part of the security awareness training, users need a clear reporting mechanism that is actively monitored.

Educate Users and Suppliers on BEC Phishing

Enforce End-User Education and Security Awareness Trainings

BEC attacks typically compromise the user through social engineering and end users easily fall prey, as they are sent from legitimate email systems. [3] As such, SRM leaders should ensure user education at regular intervals to protect against BEC attacks.

There are a variety of security awareness training solutions available that focus on basic training, testing (e.g., phishing simulations, surveys) and reporting (e.g., click rates, report rates, complete rates). Security behavior and culture programs capabilities help to improve human risk management, as they focus on risk reduction via tangible employee behavior management (see Innovation Insight on Security Behavior and Culture Program Capabilities).

Adopt Additional Methods to Enhance Security Awareness

Other methods that increase awareness about BEC attacks include internal email campaigns, intranet messages and even posters in the office. In particular, users responsible for payments, such as payroll, and with privileged access, such as executive assistants, should have specific, targeted training.

Contextual banners also enforce user awareness training in real time, based on the message content.

The main message of such campaigns is that email alone is not a valid form of authentication and should not be used to authorize high-risk transactions without additional steps to validate the sender's actual identity.

SRM leaders should include suppliers, customers and clients in BEC awareness education. To learn more about the different types of BEC attacks, refer to Note 1.

Evidence

[1] See pages 31-32 of Verizon's 2023 Data Breach Investigations Report (registration required).

[2] Internet Crime Report 2022, U.S. Federal Bureau of Investigation.

[3] See page 8 of Verizon's 2023 Data Breach Investigations Report (registration required).

Note 1: Types of BEC Attacks

Table 2 below summarizes the different types of BEC attacks and which technologies help reduce the risk of their occurrence. Security awareness training covers all types of attacks.

Table 2: BEC Attack Types

(Enlarged table in Appendix)

Type of Attack	Description	How to Defend
External spoofed email	Here, the display name in the email is modified to appear as an individual within an organization. The return address is actually that of the attacker. The email format allows for a "display name" that doesn't have to be related to the actual sender's email address, so it is easy to fraudulently use the name of a trusted individual.	▪ DMARC ▪ SPF ▪ DKIM ▪ SEG/ICES
External spoofed email to supplier/partner	A variation on the first example; here, the attacker spoofs a user from company A to target a supplier or vendor (company B). However, unlike account takeover attacks, it's easier for security teams to determine that it did not come from the real user by examining the email headers.	▪ Outbound email scanning (for internal emails) ▪ MFA ▪ Anomaly detection (impossible travel) ▪ SEG/ICES
Account takeover (ATO)	This is a more sophisticated BEC attack, where a legitimate user's email account is used. The sender ID and return address displayed are legitimate, but the attacker now has control over the inbox and the account is compromised. Attackers sometimes set up forwarding rules, so they can monitor a victim's email conversations following the initial message. They can then step in at an appropriate time with urgent messages that appear authentic, making the attack even more convincing.	▪ Outbound email scanning (for internal emails) ▪ MFA ▪ Anomaly detection (impossible travel)
Vendor email compromise (VEC; also known as account takeover with external victim)	This is a variation of an ATO attack that targets an external supplier or vendor instead of an internal user. The sender ID is that of a legit external supplier or vendor with a correct return address, which makes it difficult to identify this attack with traditional email security technologies. As in an account takeover attack, forwarding rules are used to track conversations and attackers have full access to any email-accessible documents to generate forged invoices. The attacker can then modify the payment details to their own.	▪ DMARC ▪ SPF ▪ DKIM ▪ Supply chain fraud detection feature (SEG/ICES)

Source: Gartner (August 2023)

Document Revision History

Protecting Against Business Email Compromise Phishing - 19 March 2020

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Innovation Insight for Many Flavors of Authentication Token

4 Tenets to Address Advanced Email Security Threats

Magic Quadrant for Email Security Platforms

Table 1: Different Types of BEC Protection Solutions

Secure Email Gateway (SEG) ↓	Built-In Solution (Cloud Email Providers Such as Microsoft or Google Suite) ↓	*Integrated Cloud Email Security (ICES)* ↓
SEG +	Built-in-solution +	ICES
SEG only		
SEG +		ICES
	Built-in solution +	ICES
SEG +	Built-in solution	

Source: Gartner (August 2023)

Table 2: BEC Attack Types

Type of Attack	Description	How to Defend
External spoofed email	Here, the display name in the email is modified to appear as an individual within an organization. The return address is actually that of the attacker. The email format allows for a “display name” that doesn’t have to be related to the actual sender’s email address, so it is easy to fraudulently use the name of a trusted individual.	■ DMARC ■ SPF ■ DKIM ■ SEG/ICES
External spoofed email to supplier/partner	A variation on the first example; here, the attacker spoofs a user from company A to target a supplier or vendor (company B). However, unlike account takeover attacks, it’s easier for security teams to determine that it did not come from the real user by examining the email headers.	■ Outbound email scanning (for internal emails) ■ MFA ■ Anomaly detection (impossible travel) ■ SEG/ICES

Type of Attack	Description	How to Defend
Account takeover (ATO)	This is a more sophisticated BEC attack, where a legitimate user's email account is used. The sender ID and return address displayed are legitimate, but the attacker now has control over the inbox and the account is compromised. Attackers sometimes set up forwarding rules, so they can monitor a victim's email conversations following the initial message. They can then step in at an appropriate time with urgent messages that appear authentic, making the attack even more convincing.	■ Outbound email scanning (for internal emails) ■ MFA ■ Anomaly detection (impossible travel)
Vendor email compromise (VEC; also known as account takeover with external victim)	This is a variation of an ATO attack that targets an external supplier or vendor instead of an internal user. The sender ID is that of a legit external supplier or vendor with a correct return address, which makes it difficult to identify this attack with traditional email security technologies. As in an account takeover attack, forwarding rules are used to track conversations and attackers have full access to any email-accessible documents to generate forged invoices. The attacker can then modify the payment details to their own.	■ DMARC ■ SPF ■ DKIM ■ Supply chain fraud detection feature (SEG/ICES)

Source: Gartner (August 2023)