FORTRA™

WHITE PAPER (EMAIL SECURITY)

Effective Strategies for Protecting Against BEC

While security tools have become more adept at detecting payloads in emails, attacks that lack known indicators and rely instead on impersonation/social engineering tactics are successfully bypassing these traditional controls and reaching inboxes.

Why Is It So Difficult for Organizations to Stop BEC?

BEC attacks reach user email inboxes because they evade traditional methods of email security that primarily depend on technical threat indicators typically observed in email messages. If an organization's email security controls are not effective against email impersonation and social engineering, they are at high risk of experiencing a successful BEC attack.

BEC threats are not overly sophisticated and, in fact, they're rather basic in nature. However, it's that simple style and impersonation that make them so much more difficult to detect. The following are common reasons you're seeing BEC threats and what you can do to stop them.

They Are Research-Based

Cybercriminals create target lists using databases, LinkedIn profiles, company websites, and more to identify key individuals and understand their relationships. It's important for them to understand some basic information like who the executive team is, their email addresses, and other employees who work for the organization. While easy, it proves invaluable to cybercriminals looking to create BEC attacks.

They Lack Technical Indicators

BEC threats lack indicators such as payloads, blacklisted URLs, etc., that traditional email security would typically detect. Oftentimes, BEC enters the organization as a simple text-based email increasing its chances of successfully making it into employees' inboxes.

They Impersonate Trusted Entities

Impersonation is key to BEC attacks. Executives, administrators, vendors, customers – cybercriminals will pose as any trusted entity. Often, they go as far as spoofing the sending domain or register a lookalike domain to make it even harder for the recipient to spot the ploy.

They Are Persuasive

Targeted social engineering content can be quite convincing to users. They create scenarios that play on authority, urgency, fear, and other motivators leading victims to let down their guard. The more knowledge and research cybercriminals do, the more authentic an attack can look to employees.

They Abuse Legitimate Infrastructure

To avoid blocklists and ensure deliverability, cybercriminals will often abuse legitimate email services that organizations are reluctant to block outright. Additionally, they may compromise legitimate email accounts such as those from suppliers or from within the target organization. Using these accounts, they can easily evade security filters and pose as trusted individuals.

What Is Needed to Combat BEC?

While BEC is incredibly simple and effective, it is not unstoppable. However, organizations need to go beyond traditional email security measures to detect, block, and prevent email impersonations. Here are the ways in which organizations should think about advanced email security solutions to stop this growing threat.

Model Email Patterns

Solely depending on signature-based email security controls will only stop recognizable payloads such as viruses, Trojans, and malware. Instead, organizations can use a solution with a collection of machine learning models that evaluate relationships and behavioral patterns between individuals, brands, vendors, and domains using hundreds of characteristics to detect malicious emails. Capabilities like these could also allow you to detect when internal email accounts start behaving abnormally, like the CFO requesting financial data at 2 a.m.

Prevent Spoofing of Your Legitimate Email Domains

Building a good reputation can take years as trusted relationships take time. However, a cybercriminal can destroy that reputation in a matter of minutes through email impersonation. Preventing the delivery of emails that directly spoof your email domain is paramount in the protection of your brand.

DMARC is an essential email authentication protocol that enables administrators to prevent hackers from hijacking your domains for email spoofing, executive impersonation, and spear phishing attacks. Without DMARC, organizations are risking years' worth of hard work by their email administrators and SOC teams.

Detect and Suspend Lookalike Domains

Threat intel on reported suspicious emails by users is important in building a threat intelligence database. However, managing such a task would prove nearly impossible for most organizations. That's why it's important to invest in an advanced email security solution that collects and analyzes intel on threats happening not only in your organization, but from a host of global enterprises compromised of millions of users. Having a large, crowdsourced intel feed will aid in the detection of email impersonations.

The solution also needs to proactively monitor for lookalike domain registrations created with the intent to prey on user inboxes. The domain intel, curated by experts, can eliminate false positives and gather the necessary evidence to suspend malicious domains. It should also be done quickly. Which is why having a solution with an extensive network of registrar partners can automate killswitches to remove these threats quickly.

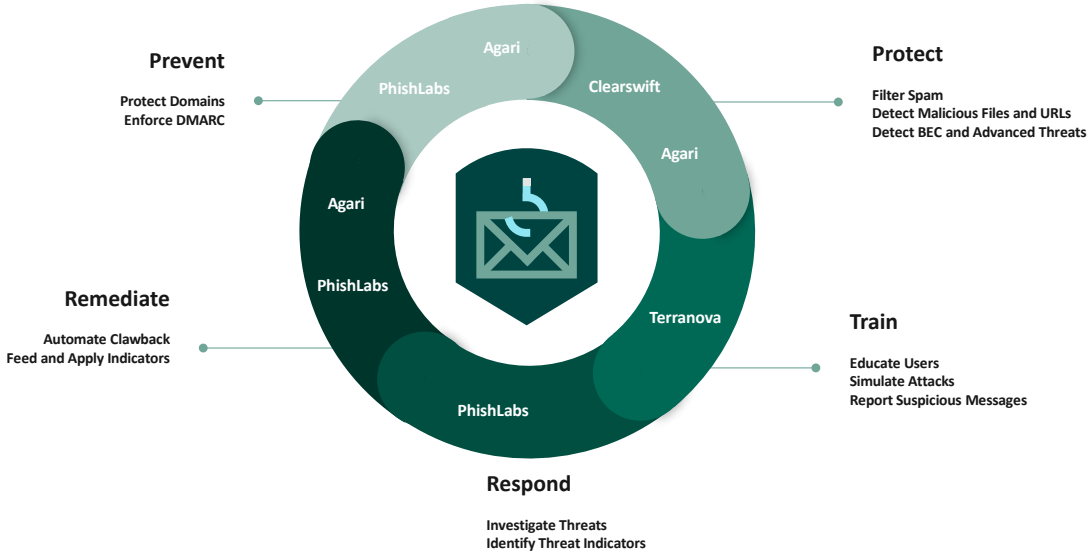
Turn Your Users from Liabilities to Assets

Email users who lack understanding of email threats can lead to financial damages, downtime, and data breaches – all of which can severely harm a brand's image. Effective, scalable email training can promote safe email behaviors and inform users of risks thereby helping to prevent cybercriminals from succeeding.

Proper training can also lead to stronger threat reports. If email users can identify threats lurking in their inboxes, they can relay intel to their organizations. Better reports lead to further strengthening of digital risk protections.

Fortra Advanced Email Security

Email impersonation can come from many different entry points. Organizations need to be ready with a solution that covers all areas discussed. However, finding a solution that fits the bill can be a daunting task. Fortunately, Fortra's Advanced Email Security is the most comprehensive email security architecture that detects, defends against, and deters advanced identity-based email attacks.



Fortra's Advanced Email Security includes:

Agari Phishing Defense: prevents threats from reaching employee inboxes by scoring every message flowing into and within the organization to defend against low-volume, highly targeted identity deception-based attacks.

Agari DMARC Protection works on the DNS level to prevent attacks from hijacking, spoofing, or impersonating your domain. While DMARC reporting and analytics tools simplifies DMARC management at every level to help your organization protect customers and partners from email attacks.

Clearswift Secure Email Gateway review external threats for ransomware, spyware, and malware so that you only see legitimate emails. With zero-hour active code detection, malicious content embedded within items such as documents, images, and even PDFs are removed.

PhishLabs Domain Monitoring continuously mines DNS zone files from more than 2,000 top-level domains, passive DNS data, and SSL certificate logs, and active DNS sourcing to proactively find potential look-alike domains. These are curated by our experts, eliminating false positives and gathering evidence necessary to suspend malicious domains. We then leverage our extensive network of registrar partners and automated killswitches to remove these threats.

PhishLabs Suspicious Email Analysis collects email threat intel to strengthen security architecture. Through automated and expert analysis, threats that pass traditional email security stacks are mitigated and email-borne payload threats are eliminated.

Terranova Security Awareness Training delivers the industry's highest quality training that enables you to easily manage content, evaluate knowledge retention, and report participation and progress on learning outcomes.

Learn how Fortra reduced impersonation attacks for a global company.

See How

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.