SOLUTION BRIEF

Seven Ways to Defend Against Business Email Compromise and Email Account Compromise with Proofpoint

KEY BENEFITS

- Detect and stop BEC/EAC attacks by addressing all attack tactics.
- Accelerate threat response and save time by automating detection and remediation.
- Reduce exposure by educating end users to identify deception tactics.
- Improve security and operational effectiveness with an integrated, end-to-end solution.
- Get visibility into the human attack surface, so you can deploy adaptive controls such as isolation and security awareness training.

Overview

Email fraud comprises two main threats:

- Business email compromise (BEC), in which attackers pretend to be you
- Email account compromise (EAC), in which attackers essentially **become** you

BEC and EAC are complex, multi-faceted problems. Attackers use a wide variety of tactics and channels to conduct these types of attacks. They target your employees' corporate and personal email, cloud apps and even your supply chain.

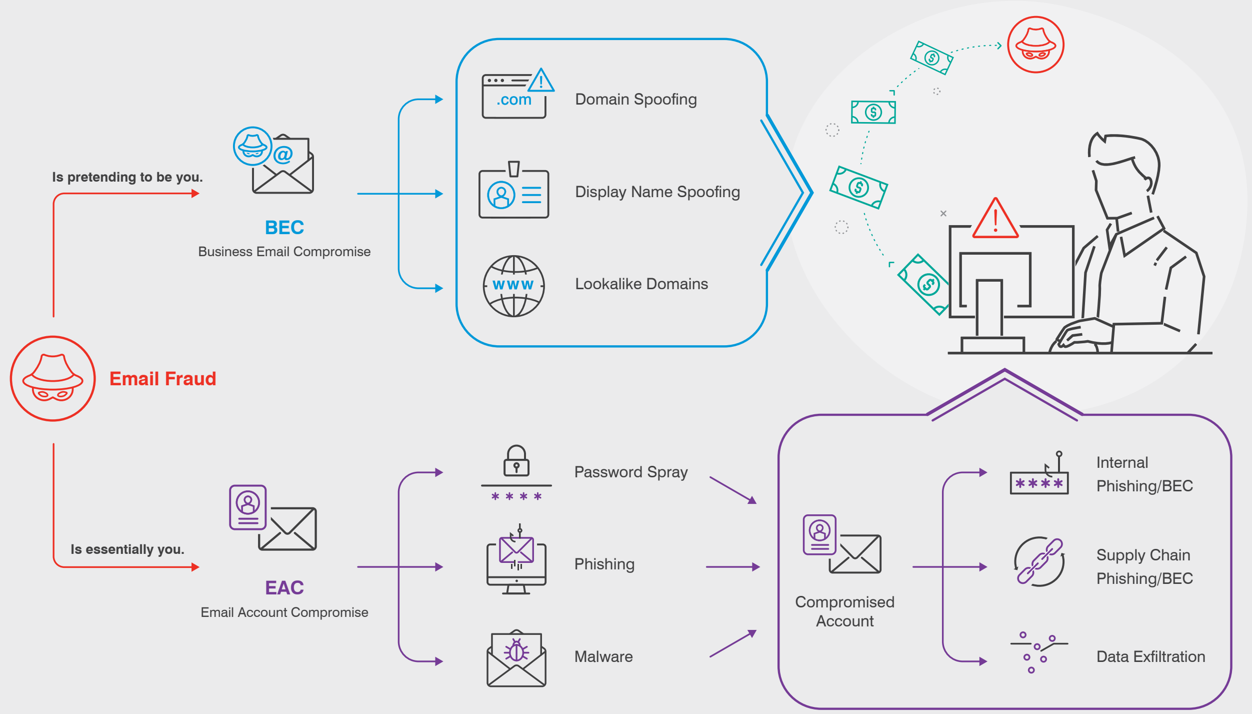
These scams have become the top concern of companies of all sizes. Nearly 90% of organizations have faced BEC and spear phishing attacks that could have led to account compromise in 2019[1]. The FBI reported that BEC and EAC scams have cost businesses more than $26B since 2016[2]. And financial losses associated with these scams continue to rise. In fact, Gartner predicts that through 2023, BEC attacks will continue to double each year to over $5 billion and lead to large financial losses for enterprises[3].

Because BEC and EAC are intertwined, you need to address them both at the same time. Only a comprehensive solution that addresses all attackers' tactics, automates detection and remediation, and provides visibility into your BEC/EAC risk will succeed. Here are seven ways Proofpoint can help defend against these new forms of email threats.

1. Block Impostor and Phishing Threats Before They Enter

BEC often starts with an email in which the attacker pretends to be someone the target trusts. Attackers use social engineering to trick or to threaten their victims into wiring money, sending sensitive data and more. It's hard to detect impostor threats because there is no malicious payload to find. Attackers forgo malware and malicious URLs in favor of a malware-free approach. While these attacks don't include malware, the intent—to steal money or data—is certainly criminal. Common BEC attack tactics include the use of domain spoofing, display name spoofing and lookalike domains.

[1] Proofpoint. "State of the Phish report." 2019.
[2] FBI. "Business Email Compromise: the $26 billion scam." September 2019.
[3] Gartner. "Protecting Against Business Email Compromise Phishing." 2020.



Stopping these new types of email threats requires a new approach. With our robust email gateway, you can detect and block these impostor threats before they get to your users.

Our email security solution uses unique machine-learning technology, impostor classifier, to protect you from these attacks. It can dynamically classify a wide range of email and detect threats, including phishing and impostor attacks, even if they don't involve malicious payloads. We assess the reputation of the sender by analyzing multiple message attributes across billions of messages, including:

- Headers
- Content
- IP addresses

Along with this information, we create a baseline by learning your organization's normal flow and aggregating information from other Proofpoint deployments. Having this baseline allows us to quickly identify email that falls outside of the norm.

Unlike other email security tools that rely on static rule matching and manual tuning, our impostor classifier learns in real time. This learning enables dynamic classification of "good" and "bad" emails. It reacts to changes in attack tactics, stopping non-malware threats more effectively. Our email security solution also lets you enforce email authentication policies, such as SPF, DKIM and DMARC, on inbound email at the gateway. This defense prevents domain-spoofed emails from entering your organization.

Our solution also blocks credential phishing and malicious emails that often lead to EAC. We use sandboxing for real-time detection by analyzing attachment-based threats in minutes. Plus, we provide predictive and click-time URL sandboxing to detect and block malicious URLs.

With detailed threat forensics on these attacks, you can understand exactly what is happening. Our deep analysis shows you everything from who was being attacked, to where the attack was coming from, and even what the attack looked like (with actual screenshots).

2. Authenticate Email with DMARC

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email authentication protocol. It's built on the backbone of two other important email authentication standards, Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM). DMARC verifies legitimate senders and prevents fraudulent or unverified emails from reaching your employee inboxes. It has proven to be the most effective way to protect against domain spoofing and to prevent fraudulent emails from being sent using your domain.

While DMARC authentication is highly recommended by industry analysts, the DMARC implementation process can be lengthy and complicated. It requires you to figure out all the ways your organization, as well as third-party senders like Salesforce, Marketo and Workday, are using all of your email domains. You also need to determine whether any of these domains have been hijacked in the past.

Deploying DMARC can be a long and arduous process. We make it easier with the visibility, tools and services to authorize legitimate email and block fraudulent messages before they reach the inbox. We help you enforce DMARC authentication quickly and confidently to block fraudulent emails at the Proofpoint gateway, that spoof trusted domains.

We also provide you with unmatched visibility and rich insights into all your email. This includes B2B email traffic—both to and from your organization. You can't get this level of detail from public data sources or other security tools. From a single portal, you can see all impostor threats, regardless of the tactic used or the person being targeted.

In addition, we automatically identify and flag lookalike domains registered by outside parties. This feature proactively prevents fraudulent lookalike domain email attacks before they strike. What's more, our managed service includes experienced consultants to guide you through every step of your rollout. We work with you to identify all your legitimate senders, including third-party senders, to ensure they authenticate properly.

With our proven implementation plan and world-class support, you can speed up the authentication process without blocking valid email.

3. Protect Cloud Applications

Cyber criminals use a variety tactics to get to your people. In the case of EAC, attackers gain access to a legitimate email account using a range of tactics.

One of the most common tactics is to use a brute-force attack. In this case, attackers use automated tools to try usernames and passwords repeatedly until they get into the account. Once they have access, they can start attacks inside and outside of your organization. For example, they can easily launch a payroll re-direct, a common type of BEC attack. That's why it's important to protect your cloud-based applications.

We help you defend against compromised accounts in Microsoft 365 (Office 365) and other platforms. We identify suspicious cloud account activities, such as failed logins, or excessive and unusual login attempts. These are considered early signs of account compromise.

At the same time, our cloud application protection capabilities allow you to detect, investigate and defend against cyber criminals accessing your sensitive data and trusted accounts. With advanced machine learning, we can create a user-behavior baseline by analyzing:

- User activity
- Email threat data
- Contextual data such as user location, device, network, and login time

We can then detect anomalies and any outbound or internal threats. Additionally, we combine rich threat intelligence with user-specific risk indicators. By conducting IP reputation checks using our global threat intelligence, we also detect logins from suspicious sources.

Most important, we correlate threat activities across email and cloud. We connect the dots between credential phishing email attacks and suspicious logins. We also help reduce alert fatigue by prioritizing alerts.

Sometimes attackers use a phishing attack to compromise an account. Sometimes they work the other way around, using a compromised account to launch a phishing attack within your organization. We give you visibility across these attack vectors so you can address them comprehensively. To respond quickly to suspicious cloud activity, you can set policies that automatically take action. For example, you can revoke a user's session, force a password reset or suspend a user when something goes wrong.

4. Isolate Web Access as Adaptive Control

Credential phishing is another common tactic that attackers use to compromise email accounts. They send an email with a URL that takes the victim to a fake website designed to steal their credentials. Most of these fake sites are so well crafted that they look real—even to careful users who take a second look. That's why isolating personal webmail and risky URLs is a critical control for securing email accounts.

Our web isolation capabilities let your users access websites, personal webmail and corporate email safely by isolating browser sessions in a secure container.

We allow users to interact with the website in a secure environment but disable uploads and downloads and restrict data input while the website is being analyzed. (This usually takes no more than a few minutes.) Our proprietary real-time anti-phishing scan runs as soon as the page is opened. If the page is identified as malicious, it automatically blocks any further interaction. This technology helps prevent credential theft and protects your users against malware and malicious content, especially for phishing emails that contain URLs that become unsafe after they're delivered.

Other vendors provide a one-size-fits-all approach to web isolation. Our solution instead lets you apply adaptive isolation controls to select users based on their risk profiles. This people-centric approach enables you to set custom isolation policies for targeted users, effectively lowering your risk.

Our browser isolation capabilities protect your people from high-risk URLs that include unknown URLs, social networks and online cloud applications. We also provide you with real-time phishing detection and URL re-write for your Very Attacked People™, allowing you to deploy adaptive security controls and better manage risk for your organization.

5. Get Visibility into Your BEC and EAC Risks

BEC and EAC are inherently focused on people, rather than on vulnerabilities in your critical infrastructure. Unless you understand what your BEC and EAC risks are, you can't effectively explain or mitigate them. We help you give your management team answers to the following questions:

- What are our BEC and EAC risks?
- Which people are the most vulnerable?
- What should we do to mitigate the risks?

Proofpoint gives you people-centric visibility so you can identify your Very Attacked People within your organization. We tell you who is being attacked with phishing and impostor emails, who is mostly likely to fall for these types of threats, and whose cloud email account has been compromised.

In addition, we give you visibility into all the emails being sent using your domain, including trusted third-party senders. You can even get insights into lookalike domain registrations. With visibility across all these areas, you can better understand and communicate BEC and EAC risks to your management. You can prioritize risk mitigation. And you can deploy adaptive security control for risky users.

6. Automate Threat Remediation

Most organizations struggle with IT security staffing shortfalls. Security teams are overwhelmed by the need to manage so many security vendors and products that usually don't talk to each other. As a result, quickly finding, investigating and cleaning up BEC and EAC threats across the organization is difficult. And the longer it takes, the longer the organization is exposed.

When a compromised account is detected, you need to take action before damage is done. Our solution lets you set policies for fast response. You can automatically force password resets, suspend compromised accounts, revoke a user's session, or enforce risk-based authentication. With our threat-response auto-pull capability, you can also remove phishing emails containing URLs poisoned post-delivery, as well as unwanted email from internal accounts that are compromised. This takes just one click, or can be automated, even if it was forwarded or received by other end users.

Proofpoint also helps streamline end user reporting and security response to impostor and phishing attacks, allowing you to automatically neutralize an active threat in minutes and reduce IT overhead. Your end users can easily report phishing emails and suspicious impostor messages with a single click, using the PhishAlarm® email reporting add-in.

If the message is found to be malicious, the reported message and any other copies (including those forwarded) can be automatically quarantined. You do not need to manually manage and investigate each incident. To complete the cycle, end users will receive a customized email letting them know the message was malicious. This reinforces behavior and encourages them to report similar messages in the future. Automating these functions helps you quickly contain the spread of BEC and EAC threats. You get accelerated threat response while doing less manual work.

7. Train End Users to Identify Identity Deception Tactics

BEC and EAC both target people and rely on them to unwittingly carry out the attacks, usually some form of wire or financial fraud. Because these impostor attacks are designed to bypass traditional security layers, your users are often left as the last line of defense. That's why mitigating BEC and EAC risks requires both technology and training. You need to train your end users so they can become more resilient to BEC and EAC attacks.

Our security awareness training capabilities help you train your users to spot credential phishing and common BEC tactics, such as display-name spoofing and lookalike domains. We give your users the knowledge and skills they need to protect your organization against these human-activated threats.

First, you can identify which users are vulnerable to BEC and EAC threats. Then, safely assess how they would engage with impostors in their day-to-day environment by simulating real-world BEC and phishing attacks.

Those who fall for attacks are automatically presented with just-in-time guidance that lets them know what they did wrong. It also offers tips to help them avoid future impostor and phishing threats. Plus, you can auto-enroll users for a training assignment to complete at a later date.

Training materials are fully customizable to improve relevance and reiterate your organization's internal processes. For example, you can teach your users to report a potential impostor threat to an abuse mailbox and verify financial requests using your organization's specific process.

Conclusion

Because BEC and EAC are intertwined, you need to address them both comprehensively. Proofpoint is the only vendor that provides an integrated, end-to-end solution to effectively stop BEC and EAC attacks.

Our BEC and EAC solution:

- Addresses all attackers' tactics
- Automates detection and remediation
- Provides visibility into your human attack surface
- Trains your end-users to become more resilient to BEC/EAC attacks

With Proofpoint, you can defend against BEC and EAC more quickly, easily and effectively.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.