Five Steps to Combat Business Email Compromise

Key Benefits

- Detect and stop BEC variants by addressing multiple attacker tactics
- Gain visibility into which users are most attacked and which third parties pose the highest risk of attack
- Receive notifications when suppliers you interact with have accounts that may be compromised
- Educate users to identify and report on email fraud
- Accelerate threat response and save time by automating remediation
- Improve security and operational effectiveness with an integrated, end-to-end solution

Business email compromise (BEC)) is a significant contributor to financial loss. According to the FBI's Internet Crime report, annual losses from BEC exceed $2.7 billion, or 80 times higher than that of ransomware.[1]

BEC attacks often impersonate senders with emails that try to fool recipients into thinking they are interacting with a trusted source. The attackers then use this trust to get the recipients to make, for example, a fraudulent bank transfer or other financial payment. Defending against such attacks is challenging, because they do not rely on malicious payloads to be effective. But some attackers go even further, using legitimate but compromised supplier accounts to launch their BEC attacks.

Protecting your organisation against BEC requires both technology and education. You need a more holistic approach to truly break the email compromise attack chain. Proofpoint can help.

We are the first and only vendor to provide a comprehensive, integrated threat protection platform that:

- Detects and stops BEC threats before they reach inboxes
- Enables users to spot and report on BEC
- Provides visibility into supplier risks and compromised third-party accounts
- Automates threat detection and response
- Protects your brand in email fraud attacks

This solution brief describes our approach in more detail.

1 *Internet Crime Report*, U.S. Federal Bureau of Investigation, 2022.

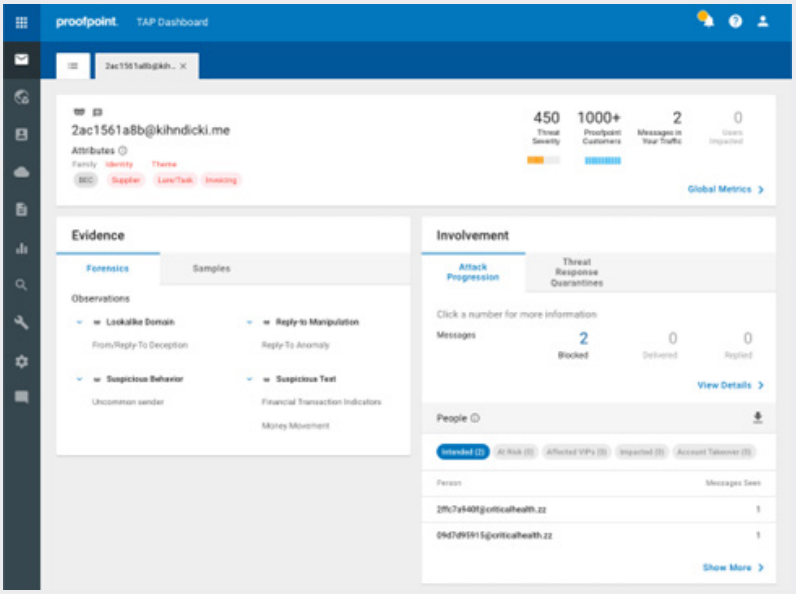

Figure 1: Proofpoint identifies users who are most attacked by BEC and provides granular visibility into BEC threat details, including themes, tactics used and more.

Detect and Block Impostor Threats Before They Enter

Our integrated platform uses Advanced BEC Defense, which is powered by our latest artificial intelligence (AI)-driven BEC detection engine, Supernova. This cutting-edge technology has resulted in an increase of 17 times more threats identified, expanding our detection to a wide variety of email fraud attacks.

Advanced BEC Defense conducts in-depth analysis on various message attributes, including:

- Message header data
- Sender's IP address
- Sender or recipient relationship
- Sender reputation

Advanced BEC Defense uses large-language module-based semantic analysis to analyse message bodies for sentiment and language. This helps to determine whether a message is a BEC threat. The behavioural machine learning engine tracks activity to extract behavioural tells, or signatures of threats, in order to understand patterns that it will then use to detect anomalies in real-time.

Some of the elements that it tracks include:

- Whether a sender is sending an unusual number of emails
- Whether emails are coming from an unusual IP address
- Whether a sender has ever been seen by the users of the company

These signals strengthen the detection stack and enable new use cases. As a result, the detection engine now catches other advanced email threats, like ransomware, credential phishing and compromised third-party accounts.

Advanced BEC Defense detects display-name spoofing and lookalike domains. It even blocks the most sophisticated supplier fraud attacks by dynamically analysing messages for tactics associated with supplier invoicing fraud. It uses machine-learning to adjust and learn in real time and aims for low false-positive rates.

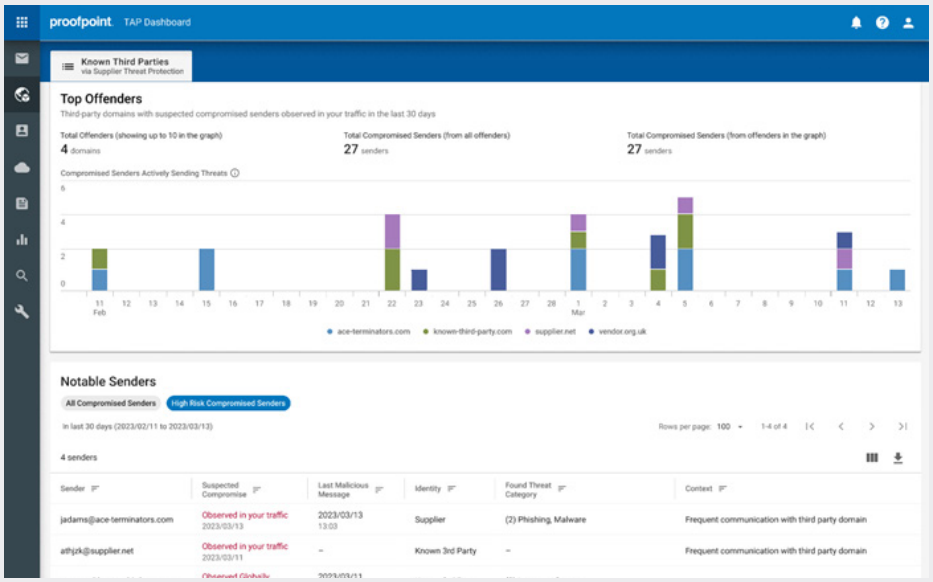

Figure 2: The Supplier Threat Protection add-on detects compromised third-party accounts that your organisation interacts with.

Get Visibility Into Your BEC Risks

To help you better understand, communicate and mitigate your BEC risks, we help you provide your management team with answers to the following questions:

- What are our BEC risks?
- Which users are most targeted?
- Which of our trusted third-parties have potentially compromised accounts?
- How can we quantify and mitigate risks?

Proofpoint can tell you which of your users are attacked most often and who is most likely to fall for impostor threats. We give you granular visibility into BEC threat details, revealing the themes to be wary of, such as gift carding, supplier invoicing fraud and payroll diversion (see Figure 1.) You can then apply adaptive security controls to targeted users and better communicate risk to your leadership.

Proofpoint extends your protection by providing visibility and insights into risky suppliers. We help you manage supplier risks and threats by:

- Proactively identifying potentially impersonated and compromised supplier accounts
- Providing a prioritised, supplier-centric view of BEC threats
- Identifying and preventing threats from supplier domains as well as malicious lookalikes of those domains

We assess and prioritise the risk level of these supplier domains and notify you about potentially compromised accounts. This allows your security teams to focus on suppliers who pose the highest risk to your organisation.

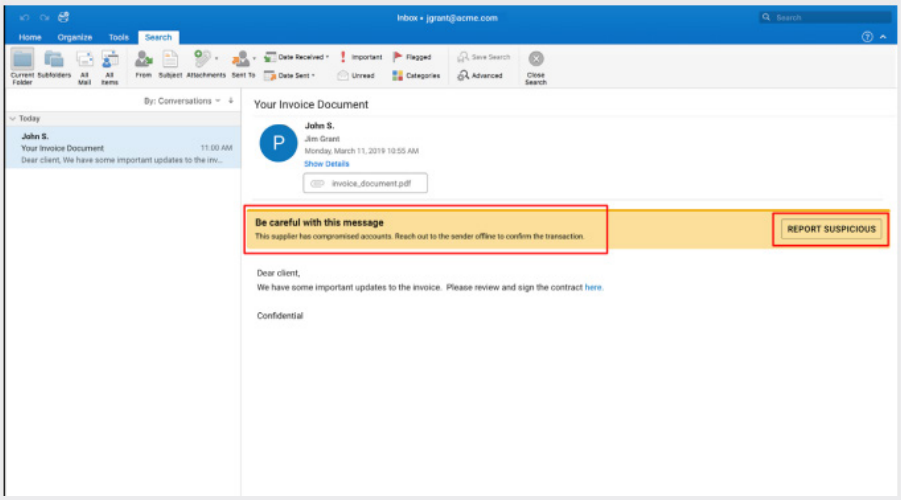

Figure 3: Email Warning Tag alerts your users and enables them to make more informed decisions on uncertain emails.

Make Users Resilient Against BEC

BEC attacks target people, relying on them to carry out malicious actions unwittingly. Because these impostor attacks rely on social engineering and identity deception, your users are often the last line of defence. This is why mitigating BEC risks requires both technology and training.

With our Proofpoint PhishAlarm report button, you can empower your users with the right knowledge and tools to identify and report on suspicious impostor emails. Our Email Warning Tags also alert users to uncertain email so they can make more informed decisions. You can train users on the latest attack tactics used in trending BEC attack tactics and assign targeted education to your most attacked users. This can ensure that they are resilient against BEC.

Automate Threat Response

Many organisations struggle with staffing shortages in their IT security departments. Finding, investigating and mitigating BEC threats across an organisation is difficult. We bring automation to the forefront of threat detection and remediation processes. With our Threat Response Auto-Pull (TRAP), you can quickly quarantine or remove any suspicious or unwanted email with just one click. The automation extends to messages forwarded to or received by other users, as well as to messages received by other Proofpoint customers. This means everyone benefits from the additional intelligence.

We also streamline abuse mailbox management. User-reported emails are automatically analysed, and those found to be malicious can be quarantined or remediated. This allows you to accelerate threat response and reduce manual work.

Protect Your Brand in Email Fraud Attacks

In the case of brand spoofing, attackers will turn you against your customers and business partners by using your company's name and brand to steal money from them. Proofpoint protects your brand from being abused in BEC attacks by preventing fraudulent emails from being sent using your trusted domains. We authenticate all emails delivered to and sent from your organisation. And by streamlining DMARC implementation with guided workflow and managed services, we help you secure your domains from being spoofed and we block all attempts to send unauthorised emails from your trusted domains.

We also give you visibility into all the emails that are sent using your domain, including from trusted third-party senders. We identify lookalikes of your domains. We dynamically detect newly registered domains that pose as your brand in email attacks. And with our Virtual Takedown service, you can take quick action to get these sites taken down.

Summary

Email fraud accounts for the largest financial losses. As fraudsters become more sophisticated, the BEC schemes have also evolved to include complex supplier fraud attacks. Proofpoint is the first and the only vendor who provides an integrated, end-to-end solution to effectively defend against these emerging threats.

Our BEC solution:

- Detects and stops various types of BEC attacks
- Provides visibility into human attack surface and granular BEC threat details
- Identifies the suppliers who pose risk and may have compromised accounts
- Trains users to become more resilient to BEC
- Automates incident investigation and response
- Protects your brand in email fraud attacks

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

LEARN MORE

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