proofpoint.

SOLUTION BRIEF

Five Steps to Combat Business Email Compromise (BEC)

- Detect and stop BEC variants by addressing multiple attacker tactics
- Gain visibility into which users are most attacked and which suppliers pose the highest risk
- 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

Email fraud accounted for the largest financial losses in 2020, according to the FBI.[1] It has cost businesses nearly $2 billion, representing 44% of all reported losses. Also, Gartner predicts that through 2023, business email compromise (BEC) attacks will continue to double each year. It is expected to cost over $5 billion and lead to large financial losses for enterprises.[2]

BEC often starts with an email in which the attacker poses as someone the target trusts or "actually becomes" that person by compromising their account. Attackers use social engineering to trick or to threaten their victims into wiring money, sending sensitive data and more. Because there is no malicious payload, BEC attacks are hard for legacy gateways that only rely on reputation and malware sandboxing to detect.

As fraudsters become more sophisticated, we're seeing more BEC variants. Such as gift card scams, payroll diversion and supplier invoicing fraud. To combat the ever-evolving email fraud threats, you need a holistic solution that addresses all BEC actors' tactics by encompassing multiple security controls and user awareness.

How Proofpoint stops BEC attacks

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

- Detects and stops BEC threats before they enter
- Provides visibility into BEC risks
- Enables users to spot and report on BEC
- Automates threat detection and response
- Protects your brand in email fraud attacks

This solution brief explains how we address common BEC attacks.

1 Internet Crime Report, The FBI, 2021.
2 Protecting against Business Email Compromise, Gartner, 2020.

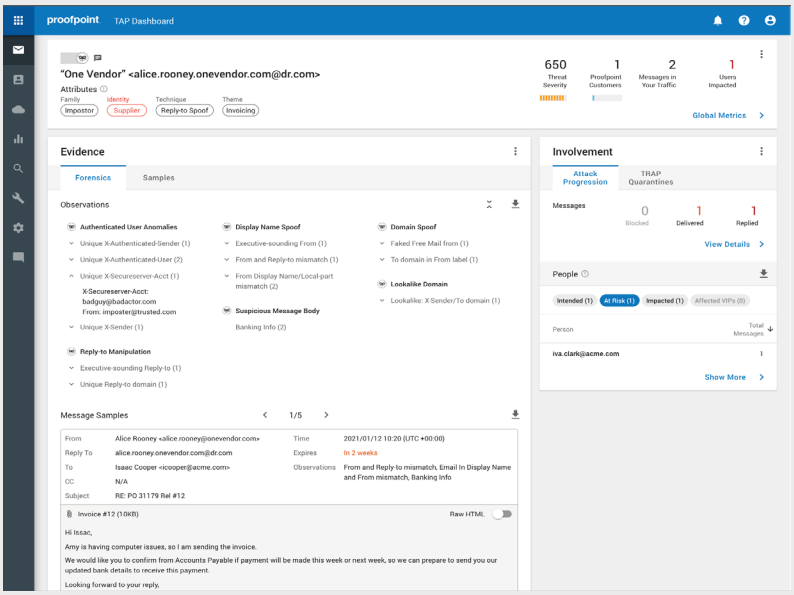

Figure 1: Proofpoint identifies which users are mostly attacked by imposter threats and provides granular visibility into BEC threat details.

1. Detect and block impostor threats before they enter

Our integrated threat protection platform utilizes **Advanced BEC Defense**. It is our ML/AI-powered BEC detection engine. It dynamically detects a wide variety of email fraud attacks. And it analyzes multiple message attributes, including:

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

It also analyses the message body for sentiment and language and more to determine whether a message is a BEC threat.

Advanced BEC Defense uncovers all BEC attack tactics. That includes display name spoofing and lookalike domains. It even detects and blocks the most sophisticated supplier fraud attacks by dynamically analyzing messages for numerous tactics associated with supplier invoicing fraud such as:

- Reply-to pivots
- Use of malicious IPs
- Use of impersonated supplier domains
- Words or phrases commonly used in these supplier fraud attacks

Most email security products only rely on static rule matching or limited contextual data which requires manual tuning. Advanced BEC Defense is different. Our detection engine is powered by **NexusAI** and learns in real time. It has broad coverage across companies of all sizes. And it has visibility spanning across email, cloud, network and digital.

We offer true machine-learning that stays ahead of the threat landscape. This learning enables dynamic classification of "good" and "bad" emails with minimum false positives. It reacts to changes in attacker tactics, stopping the bad while delivering the good.

2. Get visibility into your BEC risks

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

- What are our BEC risks?
- Which users are the most vulnerable?
- Which suppliers are posing risk to our organizations?
- What should we do to mitigate the risks?

We tell you which of your users are attacked the most with impostor threats and who is most likely to fall for these types of threats. We give you granular visibility into BEC threat details, revealing the theme of each impostor threat, such as gift carding, lure, supplier invoicing fraud and payroll diversion. See Figure 1. That way, your security team can better understand and communicate about the attack.

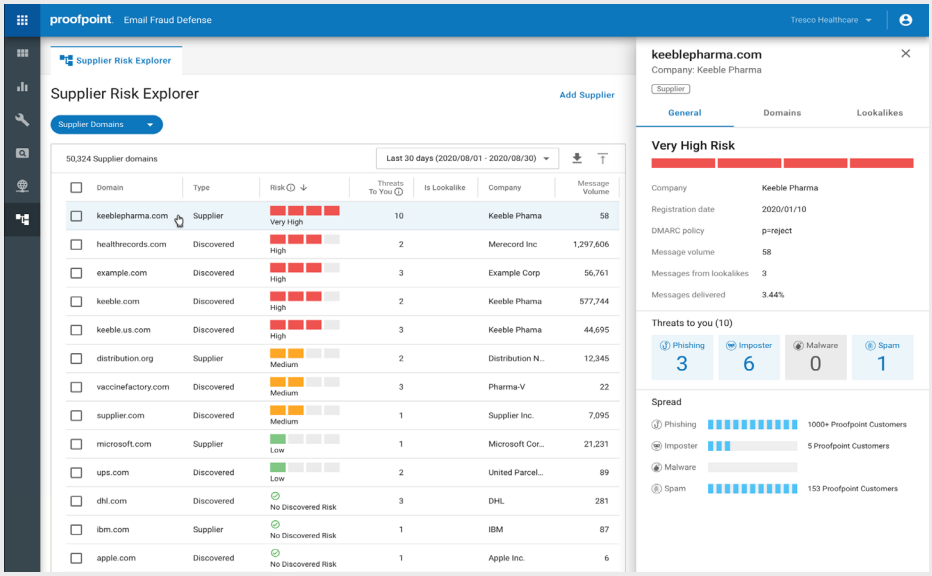

Figure 2: Supplier Risk Explorer identifies supplier domains and provides visibility into which suppliers pose risk to your organization.

Besides, we provide you with visibility into which suppliers pose risk to your organization. With **Nexus Supplier Risk Explorer** (see Figure 2) we can:

- Automatically identify potential impersonated and compromised suppliers and the domains to send email to your users
- Provide a supplier-centric view of BEC threats
- Reveal the message volume
- Disclose threats detected from supplier domains
- Provide the messages blocked from malicious lookalikes of your suppliers' domains

By assessing and prioritizing the risk level of these supplier domains, we allow your security team to focus their efforts on suppliers that pose the highest risk to your organization.

3. Make users resilient against BEC

BEC targets people and relies on them to unwittingly carry out the attacks. Because these impostor attacks rely on social engineering and identity deception, your users are often left as the last line of defense. That's why mitigating BEC risks requires both **technology** and **training**.

We help you train your users to identify and report on suspicious impostor email. We give your users the knowledge and skills they need to protect your organization against these human-activated threats. Insights from our integrated platform allow you to build a program around Very Attacked People or users engaging with known malicious content.

First, you can identify which users are vulnerable to BEC threats. Then, safely assess how they would engage with impostors in their day-to-day environment by simulating real-world BEC attacks. Those who fall for attacks are automatically presented with just-in-time guidance that lets them know what they did wrong. And they can be auto enrolled into specific training modules if desired.

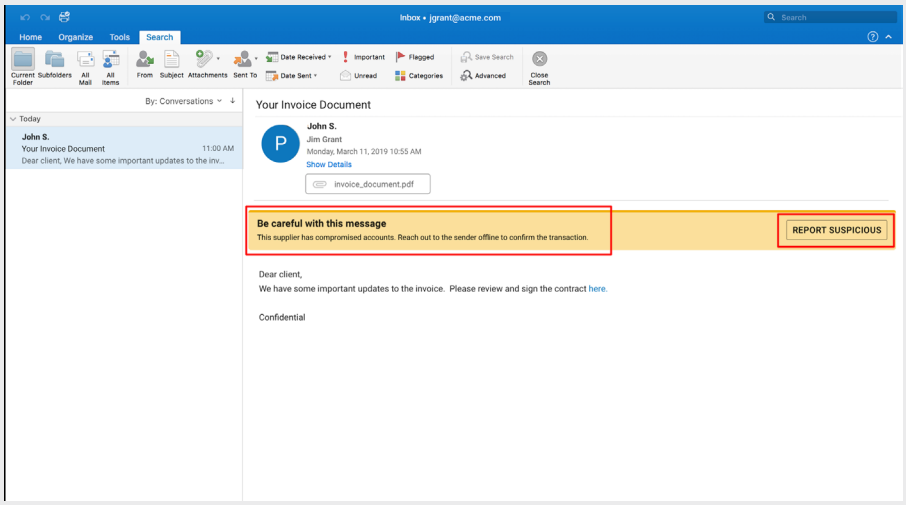

Figure 3: Email Warning Tag alerts your users and enables them to make more informed decisions on uncertain email.

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. You can also verify financial requests using your organization's specific process.

We also alert your users with email warning tags, which surface a short description of the risk of a particular email. For example, we warn your users when a message is sent from an external sender or from a newly registered domain. This helps your users make more informed decisions on uncertain email. And it reduces the risk of potential compromise.

4. Automate threat response

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 threats across the organization is difficult. And the longer it takes, the longer the organization is exposed.

We automate threat detection and remediation process. With our threat-response auto-pull capability, you can quarantine or remove any suspicious or unwanted email with just one click. Or you can automate that process even if it was forwarded or received by other users. Furthermore, we streamline abuse mailbox management. It allows you to automatically neutralize an active threat in minutes and reduce IT overhead.

Users can easily report suspicious messages directly from the email warning tag that surfaces the risk of a specific message, or from the PhishAlarm® email reporting add-in, both with a single click.

Reported messages are automatically analyzed and enriched using multiple threat intelligence and reputation systems. The BEC threat hunting capabilities allow you to quickly search your email environment and identify if there are other users receiving the message.

If the message is found to be malicious, the reported message and any other copies (including those forwarded) can be automatically quarantined. No need to manually manage or investigate each incident, saving time and effort for your team. To complete the cycle, 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.

5. 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. While brand spoofing may not cause direct financial loss to your organization, it can damage your organization's reputation, erode customer trust and a have negative impact on your business for a long time.

We protect your brand and organization's reputation in email fraud attacks by preventing fraudulent emails from being sent using your trusted domains. And we authenticate all emails delivered to and sent from your organization. By streamlining DMARC implementation with guided workflow and managed services, we help you publish DMARC reject policies with confidence. This effectively prevents your domains from being spoofed and blocks all attempts to send unauthorized emails from your trusted domains.

Plus, we give you visibility into all the emails being sent using your domain, including trusted third-party senders. We identify lookalikes of your domains. We dynamically detect newly registered domains posing as your brand in email attacks or by phishing websites. And we alert you instantly when suspicious domains move from parked to a live, weaponized state.

Also, we show you how attackers are impersonating your brand across digital channels, including email, web domains, social media and the darknet. With visibility across all these areas and our Virtual Takedown service, you can quickly reduce customer and business partner exposures to malicious lookalike domains.

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 which suppliers pose risk
- 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**.