

GUIDEBOOK

CISO Guide to Vendor Email Compromise

Stopping the Vendor
Fraud Attacks That
Exploit Trusted Partnerships



Abnormal

The Rising Threat of Vendor Email Compromise



83%

of large enterprises experienced a VEC attack in 2024.

\$300M

in attempted vendor fraud during a 12-month observation period.

44.2%

of read VEC messages are engaged with.

- ▶ Vendor email compromise (VEC), also referred to as supply chain compromise, is a significant security threat to enterprise organizations. This form of attack occurs when a threat actor gains control of a vendor email account and then uses it to steal money from known contacts. VEC attacks are highly successful because they exploit trusted communications between vendors and customers through personalization and social engineering.

According to Abnormal data, 83% of large enterprises experienced a VEC attack in 2024. Threat actors increasingly see communications between vendors and customers as the weakest link—and they're not wrong. Roughly 44.2% of read VEC messages are engaged with by employees. Once they gain access to vendor accounts, it becomes easy to focus their efforts on VEC attacks, as they are much more lucrative than traditional scams. During a 12-month observation period, the total value of attempted vendor fraud was \$300 million.

It's clear traditional email defenses were not designed to stop sophisticated socially-engineered attacks. Without a new approach, VEC will continue to cause severe financial losses and reputational damage.



Types of Vendor Email Compromise Attacks

Vendor email compromise is not a monolithic type of attack and can take on many forms. Here are a few of the ways attackers leverage compromised accounts to steal money from organizations.

▶▶ Invoice Fraud

The attacker uses the compromised account to send a fraudulent invoice. In many cases, this looks exactly like a real invoice and even includes the expected billing amount, as the attacker has access to the entire email account and can research past conversations. Typically, the only difference is that the banking details have been changed to an account in the attacker's control.

▶▶ Billing Account Update Fraud

Using the compromised account, the attacker sends a notice about a recurring payment or outstanding invoice, indicating that the recipient must update payment details to an account under their control. These attacks use similar phrases like “bank reconciliation audit” and needing to send money to a “secondary bank account.”

▶▶ Payment Fraud

Payment fraud is defined as any compromised vendor email account that attempts to steal money and/or goods from a target through means that don't involve a specific invoice or payment transaction. Payment fraud attacks can take different forms, including RFQ scams, aging report scams, or invoice inquiries, where the attacker asks for details about an upcoming payment.

▶▶ RFQ Scams

An RFQ scam starts with the attacker emailing the supplier for a specific set of merchandise. After the vendor responds, an official-looking purchase order is then delivered containing the logo, contact information, and most importantly, the delivery information for where the goods are to be shipped. Attackers will often use the real information of companies they have compromised in order to pass credit checks so they can receive the goods on credit. If successful, this concludes with the goods being shipped to the attacker (rather than the compromised vendor) and no payment is made for the goods in question.



It's worth noting that vendor email compromise attacks can take many other forms and often do. These attacks can be part of larger credential phishing or account takeover schemes and can have dire consequences for both organizations involved.



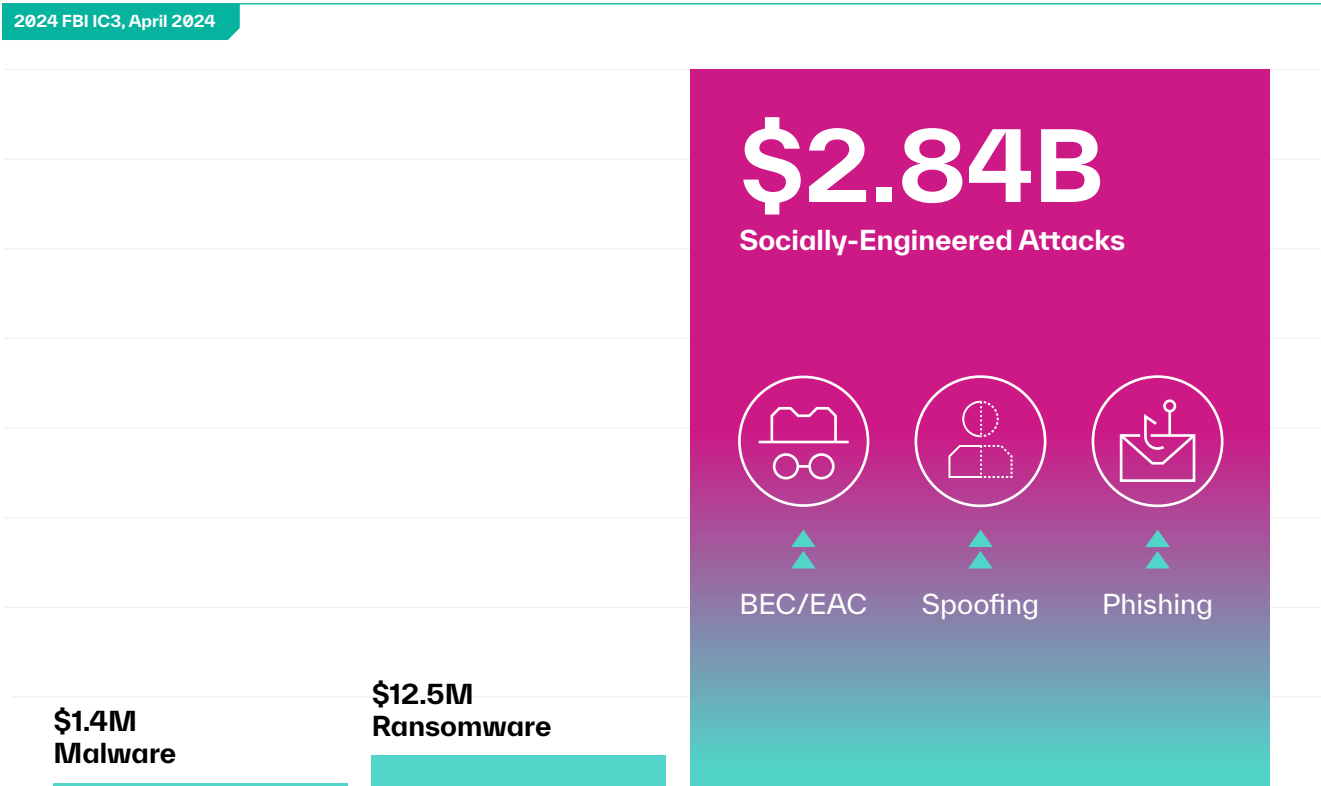
Impact of Vendor Email Compromise Attacks

The FBI’s Internet Crime Complaint Center (IC3) actively tracks financial losses from business email compromise (BEC) attacks, of which vendor email compromise is part. The 2024 Internet Crime Report revealed that BEC crimes cost businesses \$2.77B last year, with an average of \$129,000 lost per incident.

As macroeconomic conditions worsen and acquiring funds through legitimate means becomes progressively more difficult, we can anticipate continued growth in these sophisticated, vendor-focused attacks.



Socially-Engineered Attacks are the #1 Security Threat



Why Vendor Email Compromise Attacks Are Successful

To stop vendor email compromise, there needs to be a fundamentally different approach to the problem. The old approach relies on threat intelligence as a means of detecting and preventing all attacks. Unfortunately, threat intelligence has known limits to what it can stop.



Secure email gateways look for known bad or indicators of compromise, like bad domain reputation, suspicious links, or malicious attachments. But since vendor compromise attacks do not make use of these tactics, they evade conventional defenses.



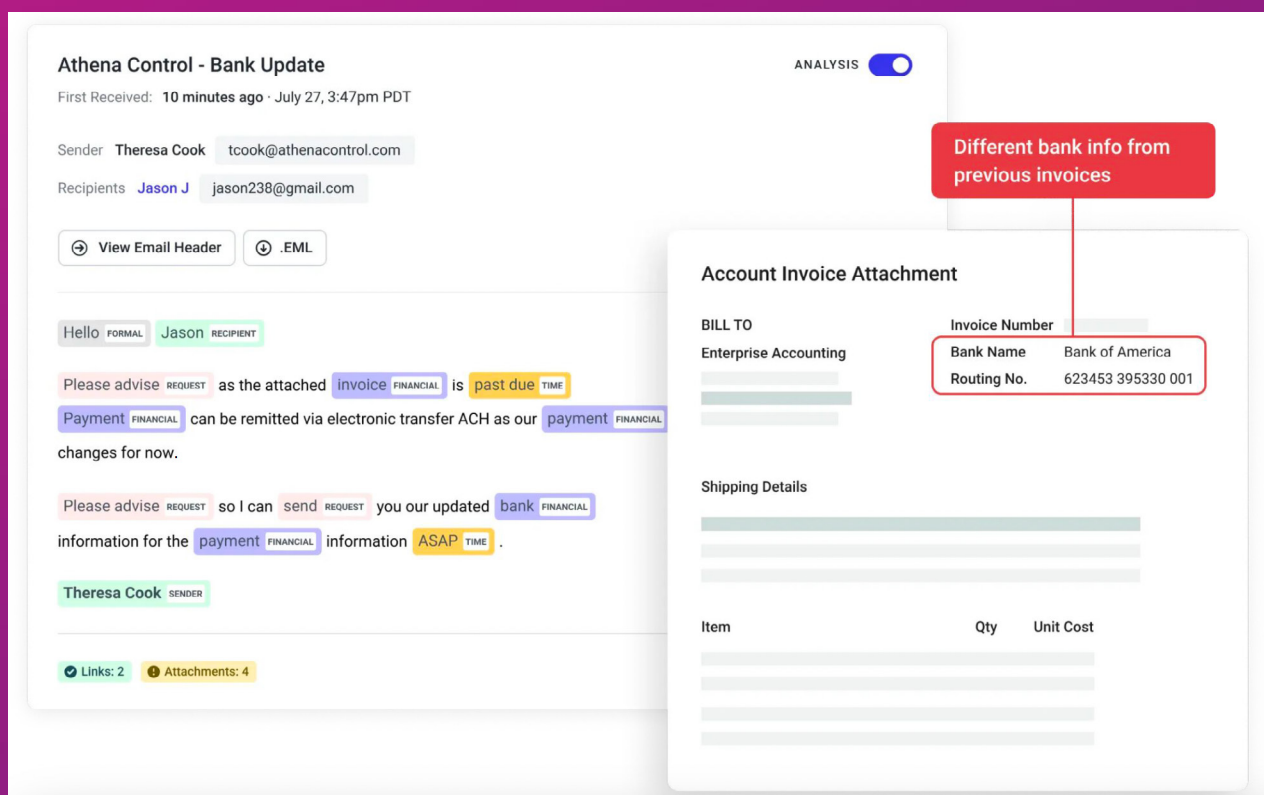
For many organizations, security awareness training is used to train employees to spot discrepancies so they can determine whether or not the email is fraudulent. However, with VEC attacks, the emails come from real accounts and contain legitimate business information, adding to the credibility of the request. As a result, employees find it difficult—if not impossible—to detect when a VEC attack is underway.



Additionally, real email accounts are sent from legitimate domains that are likely to pass email authentication protocols like DMARC. As a result, if they are compromised, the email attacks sent from the account will not be stopped by authentication defenses that look for misaligned DMARC configurations or domain spoofing.



If you look at a real-world example of a vendor email compromise attack, you can see why traditional defenses fail.



When these attacks land in inboxes, they rely on name recognition and the urgency of the request. By encouraging their victims to move quickly, they successfully trick people into making mistakes. And based on the number of successful attacks, more people fall for it each year—despite an increase in security awareness training.

Because VEC attacks typically contain no traditional indicators of attack, it's only by understanding the context and intent that we can determine if an email is malicious. There is little denying that these attacks are incredibly difficult to detect, by both traditional defenses and humans. As VEC grows in severity, it's increasingly obvious that these attacks must be stopped before they can trick your employees.



Suspicious Domain?

No. This email is using a real vendor account and will thus pass all authentication checks.



Malicious Links?

No. This is a text-based email with legitimate links.



Corrupt Attachments?

No. This email has attachments, but they are benign files that look exactly like other attachments sent from this account.

How to Stop Vendor Email Compromise Attacks

To counter these highly sophisticated attacks through trusted communications, organizations need the right technical controls to identify vendors that have been compromised. The next-generation type of email security includes:



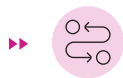
API Architecture

A solution that connects into Microsoft 365 and Google Workspace via an API and in doing so, provides access to the signals and data needed to detect suspicious activity. This includes unusual geolocations, dangerous IP addresses, changes in mail filter rules, unusual device logins, and more.



Behavioral AI Approach

The solution should use a fundamentally different approach that leverages behavioral data science to profile and baseline good behavior and detect anomalies. It should use identity modeling, behavioral and relationship graphs, and deep content analysis to identify and stop emails that include suspicious information or requests.



Federated Database of Vendor Behaviors

The solution should continuously monitor communications between vendors and customers, and provide a real-time assessment of vendor risk to inform decisions and stop targeted and sophisticated VEC attacks.



Without each of these capabilities, vendor email compromise will continue to outpace security measures—making it even more difficult to prevent these attacks from reaching employees, creating financial loss, and causing reputational damage.



Conclusion

- 
- ▶ Vendor email compromise isn't just growing—it's evolving. These attacks exploit the implicit trust between businesses and their vendors, slipping past traditional email defenses that depend on static threat intel. Legacy tools can't detect what looks normal on the surface but feels wrong underneath. Stopping these threats requires more than rules and filters; it demands a solution that uses API-level access and AI to understand identity, context, and intent. By analyzing thousands of behavioral signals in real time, we can precisely block messages from compromised accounts—before they ever reach the inbox.



▶▶ About Abnormal AI

Abnormal AI is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated inbound attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages identity and context to understand human behavior and analyze the risk of every cloud email event—detecting and stopping sophisticated, socially-engineered attacks that target the human vulnerability.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly. Additional protection is available for Slack, Workday, ServiceNow, Zoom, and multiple other cloud applications. Abnormal is currently trusted by more than 3,200 organizations, including over 20% of the Fortune 500, as it continues to redefine how cybersecurity works in the age of AI.

Ready to Stop Vendor Email Compromise?

[Request a Demo >](#)[See Your ROI >](#)