THREAT REPORT

Abnormal

Read, Replied, Compromised:

Employee Engagement Trends Across VEC Attacks

Executive Summary

Your workforce is your greatest asset, and your vendors are integral to the success of the enterprise. It's no surprise, then, that cybercriminals are targeting both, exploiting the trust in these partnerships to deceive, defraud, and divert funds.

Much like traditional business email compromise (BEC), vendor email compromise (VEC) involves the misuse of a familiar identity. In these attacks, however, the person being impersonated is an external third party rather than an internal employee. Posing as trusted partners, threat actors attempt to trick targets into paying fake invoices, initiating fraudulent wire transfers, or updating banking details to reroute funds into attacker-controlled accounts.

44.2%

Overall employee engagement rate with VEC messages across all organizations

$300M

Total value of attempted vendor fraud during observation period

98.5%

Text-based advanced attacks employees failed to report

Behavioral Data Reveals Alarming VEC Engagement Rates

From March 2024 to March 2025, we monitored the email environments of more than 1,400 organizations of various sizes across multiple industries. These companies had implemented Abnormal in passive, read-only mode, which means the platform was integrated with the organization's mail client but not actively blocking attacks.

This allowed us to observe unfiltered employee behavior and analyze engagement with text-based advanced email attacks—e.g., business email compromise, vendor email compromise, reconnaissance, and extortion. To enable cross-organizational comparison, we standardized the data by using only attacks that were read, eliminating volume as a variable and allowing conclusions to be drawn based on user behavior rather than incident frequency.

Our findings were eye-opening. The data revealed that employees frequently struggle to differentiate between legitimate messages and attacks, especially when those emails appear to come from a known vendor. VEC attacks consistently drove either the highest or second-highest rates of replies and forwards, irrespective of organization size, industry, or geographic location. Over the course of the observation period, attackers also attempted to steal more than $300 million through VEC, emphasizing the significant financial risk these threats pose.

This report exposes the behavioral blind spots attackers are exploiting and underscores the urgency of reducing exposure to malicious content.

Table of Contents

Inside the Threat: Why VEC Works

All text-based advanced email attacks are insidious and deceptive, but there are a few aspects of vendor email compromise that make it especially difficult to detect. First is the inherent financial nature of the vendor-customer dynamic and the fact that billing and payments are routinely discussed via email. Consequently, malicious messages seemingly from vendors requesting changes to banking information or large fund transfers may not be immediately flagged as suspicious.

Further, the scale of some supply chains makes it nearly impossible for employees to be well-versed in every vendor's operations. Therefore, they simply don't have the context to recognize when a request is out of the ordinary. Even when the target is knowledgeable about the standard processes and which parties are usually involved, there is no guarantee that they will discern that something is amiss.

Cybercriminals who engage in VEC will monitor ongoing correspondence, learn typical patterns and behaviors, and patiently wait until the ideal time to strike. Often, they will download older invoices or statements and alter only the bank account information, leaving the modified documents essentially indistinguishable from the originals.

Threat actors will also use spoofed sender addresses or look-alike domains to increase the appearance of authenticity. Some even leverage actual compromised vendor accounts, frequently hijacking existing email threads to carry out the attack. The emails, originating from a legitimate account with no history of suspicious behavior, bypass signature-based security tools and land in the inboxes of employees who have no reason to believe the message is malicious.

The Role of AI in Amplifying Vendor Email Compromise

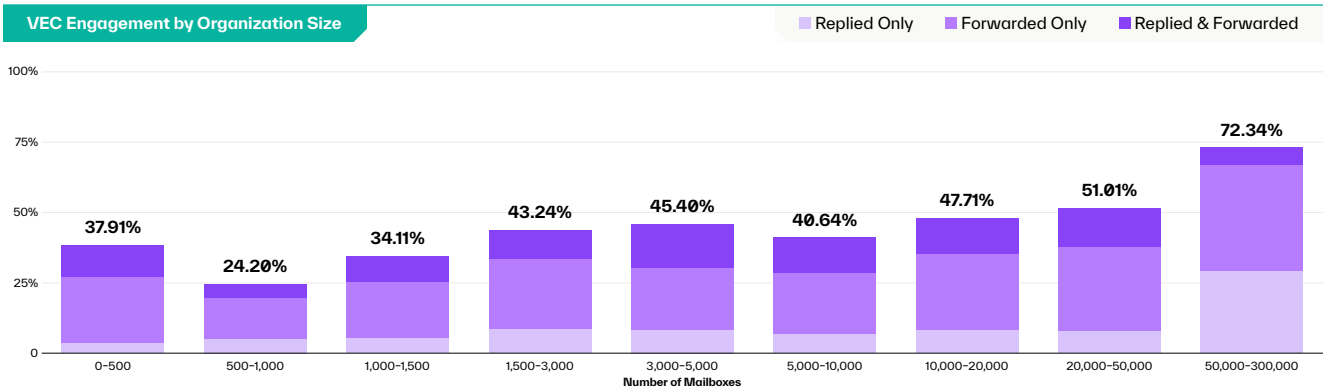
VEC occurs at a lower rate than other threats, like phishing, for several reasons. Chief among them is that attackers tend to choose the path of least resistance, and vendor email compromise, though lucrative, is a high-effort attack type. That being said, with the added capabilities of weaponized AI, even low-skill cybercriminals are increasingly able to execute these sophisticated, socially engineered attacks.

With AI-powered tools, attackers can generate remarkably believable messages that mirror real vendor communications, complete with realistic language, formatting, and urgency cues. In a tight job market, with economic uncertainty and persistent layoff concerns, employees may rush to resolve an apparent oversight—like a missing payment—without verifying the request. AI further amplifies this risk by helping bad actors make fraudulent invoices and follow-up messages more persuasive, increasing the likelihood of success.

Reducing your risk to threats like vendor email compromise requires an understanding of attack trends and the unique vulnerabilities upon which threat actors capitalize to infiltrate an organization.

VEC Risks Increase with Organization Size

Employees in the largest organizations—i.e., those with a workforce of 50,000 or more—had the highest rate of second-step engagement[1] with vendor email compromise. After reading a VEC message, they took additional action 72.3% of the time.



Another way to think about these percentages is this: if employees at a company read 10 VEC attacks, *at least* two and up to seven of those messages will be replied to or forwarded.

The natural, and understandable, assumption here is to make a connection between VEC volume and engagement rate. While the probability of receiving a VEC attack does typically increase with the number of mailboxes, the baseline attack rate is a non-issue here.

In order to facilitate an accurate comparison, our analysis focuses only on the percentage of vendor email compromise attacks that are read, making gross volume irrelevant. The true variables are instead the number of employees and the number of vendors. Every partner represents another entity that can be impersonated or an account that can be compromised, and every member of the workforce represents a potential target—a human that is far from infallible.

Interestingly, enterprises with more than 50,000 employees actually had the lowest read rate of any organization size band, showing that the threat doesn't stem from volume alone, but from how employees behave after opening the email.

Across the board, VEC engagement rates are already worrisomely high. But what makes the issue even worse is the fact that 7.3% of these instances of second-step engagement were initiated by individuals who had previously replied to and/or forwarded a different VEC attack.

While it is impossible to know why this is, there are a few reasons why an employee might become a "repeat engager." Perhaps they didn't receive sufficient training after the first incident. Employers should not assume that once an employee has experienced the negative consequences of falling victim to an attack, no additional coaching is needed to avoid repeating the error. There's also the possibility that after being deceived once, an employee may adopt the attitude that "lightning never strikes the same place twice." Rather than becoming more vigilant, they erroneously believe they won't be targeted again.

72%

Post-read interaction rate with VEC messages in large enterprises

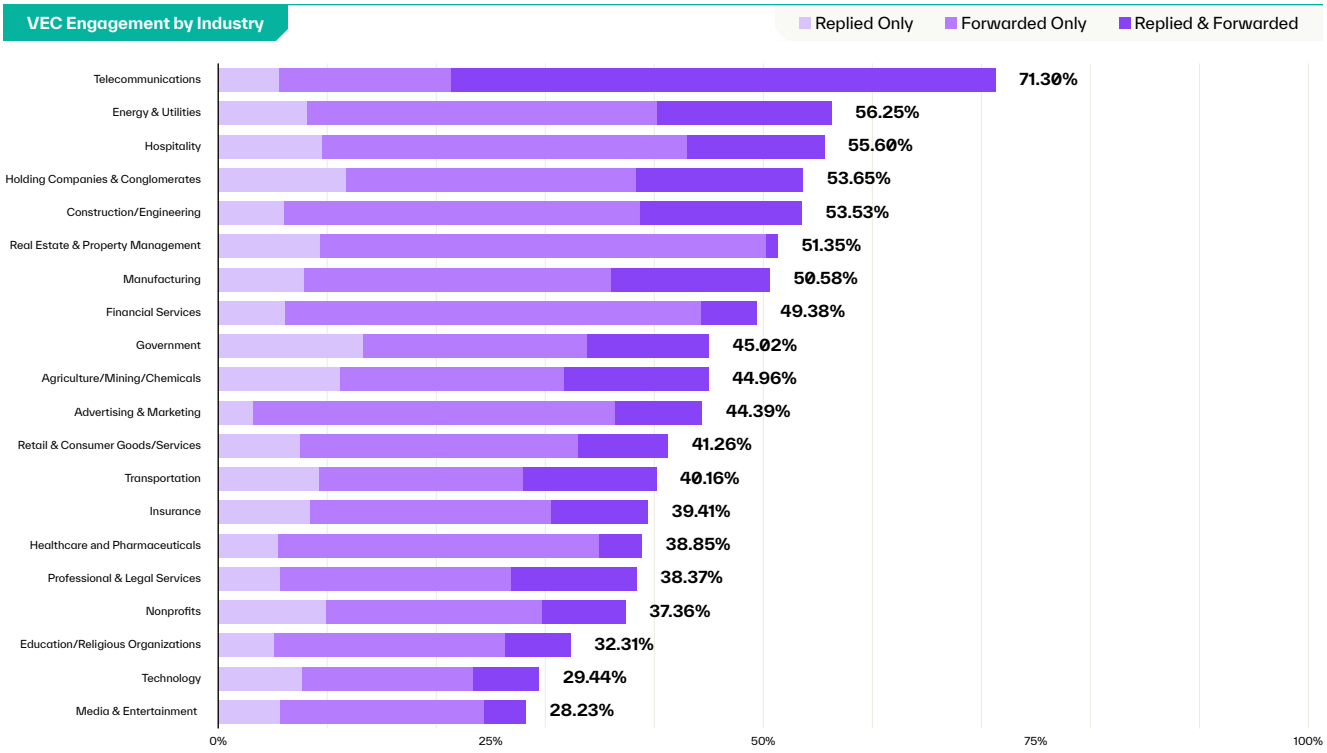
7%

Share of replies and forwards initiated by "repeat engagers"

[1] Second-step engagement refers to an action taken after reading a message—e.g., replying, forwarding, or both. Forwards do not include messages sent to phishing mailboxes.

Sector by Sector: Where VEC Drives the Highest Engagement

Industry type emerged as a critical factor in VEC susceptibility, with engagement rates varying dramatically based on operational characteristics.



At 71.3%, the second-step engagement rate for the telecommunications industry is by far the highest of any vertical, dwarfing the 56% observed in energy/utilities providers, which ranked second.

Telecommunications organizations depend on complex networks of vendors, resellers, infrastructure providers, and technology partners to deliver services. They also have large, geographically distributed teams, including field technicians, regional offices, and 24/7 operations centers. This creates an environment where email serves as a critical coordination channel between internal teams and external partners.

In an industry where disruptions and delays can have wide-ranging impacts, employees may feel compelled to act quickly when a message appears related to service interruptions or contract issues. The pressure to maintain uptime—reinforced by SLAs and internal expectations regarding responsiveness—can result in employees bypassing verification processes in favor of speed.

Energy/utilities and hospitality round out the top three industries for second-step engagement. Though the services they provide differ significantly, organizations in these verticals do share certain characteristics that prime employees to act on messages seemingly from external vendors with minimal scrutiny.

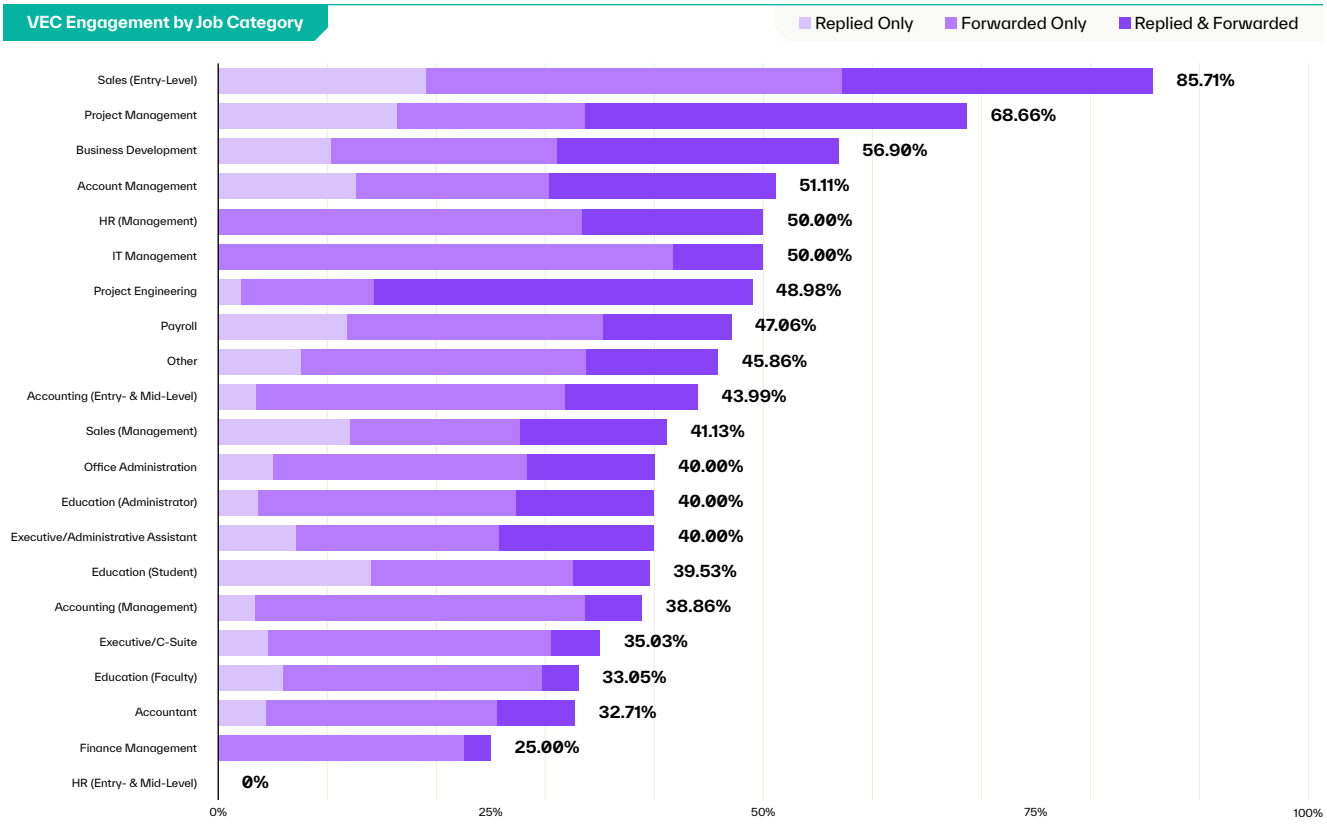
Both operate in high-pressure, service-driven environments with dispersed, often round-the-clock workforces that rely extensively on email for communication. Further, energy and utilities employees face intense pressure to protect critical infrastructure, while hospitality staff are trained to prioritize rapid responses to maintain positive guest experiences.

71%

Frequency of engagement with VEC messages in telecom industry

Role-Related Risk: Job Functions and VEC Engagement

One notable trend was the clear correlation between an employee's organizational role and their likelihood of engaging with vendor email compromise attacks.



Sales-focused roles are heavily represented among the job categories with the highest second-step engagement rates, holding three of the top four spots. These positions rely primarily on email correspondence, are typically among the most public-facing in an organization, and often involve interacting with various departments. Additionally, these roles are traditionally commission-based, meaning employees are financially incentivized to be helpful, respond to inquiries quickly, and resolve issues promptly.

86%

Rate of second-step engagement with VEC attacks by entry-level sales staff

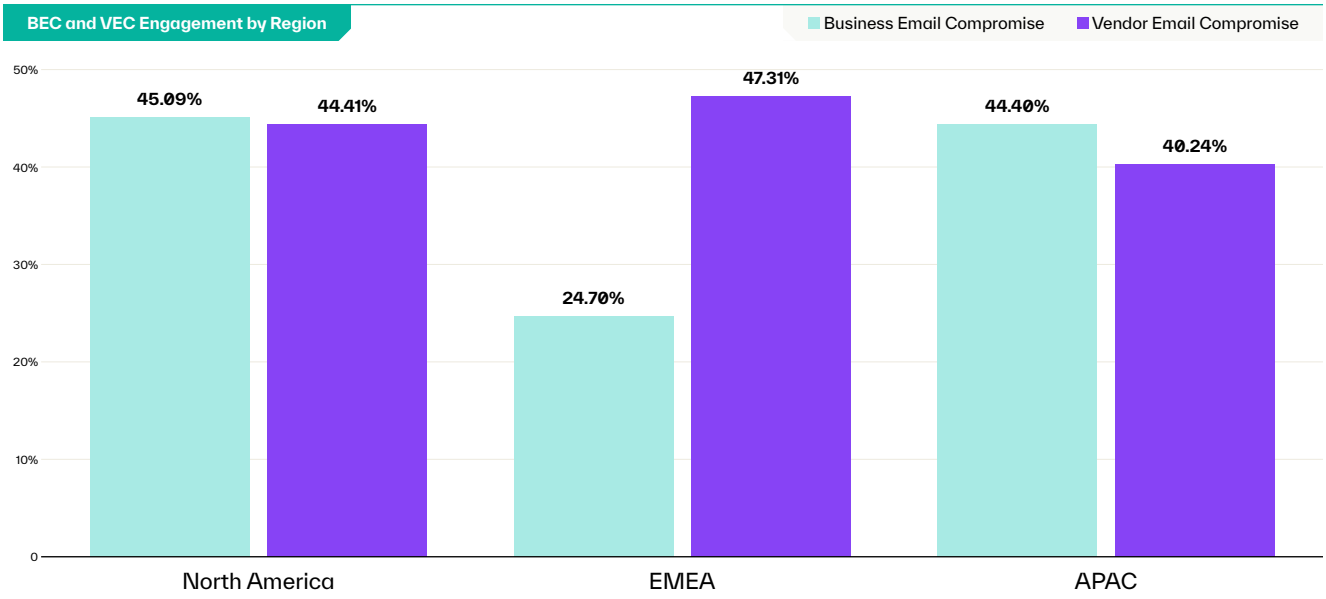
Though not sales-oriented, Project Management's second-place position is unsurprising. While "Project Manager" and similar titles can encompass a wide variety of responsibilities depending on industry and department, the fundamental goal remains the same: ensure projects are completed on time. Thus, if they receive an email seemingly related to a matter that could impact the progress of a project, they would be highly motivated to take steps to address the issue as quickly as possible.

These results, while not unexpected, remain concerning. The figures underscore how important it is to provide proactive and ongoing security awareness training to employees in these positions since, by the nature of their roles themselves or the personalities of those who fill them, they are at a greater risk of engaging with VEC.

Across Borders: VEC and BEC Trends by Region

Because the 1,400 organizations in this analysis span North America, EMEA, and APAC, the data offers a unique opportunity to examine how employee behavior varies by geographic location. While engagement patterns differed across regions, one trend remained consistent: second-step interaction rates with both BEC and VEC were alarmingly high.

Taking a more granular look at the data, several interesting trends emerge.



EMEA: External Impersonation Is a Blind Spot

For organizations in EMEA, the second-step engagement rate with VEC eclipsed that of BEC, exceeding it by 90%. Additionally, the repeat engagement rate for VEC was over twice as high for BEC and the highest of any geographic region. Interestingly, EMEA employees had the lowest reporting rate for vendor email compromise attacks—a shockingly low 0.27%—but the highest reporting rate for BEC attacks: 4.22%. They also had the lowest rate of second-step engagement with BEC (24.7%).

The Bottom Line

EMEA employees appear to be highly susceptible to continued interaction with VEC attacks but resistant to engaging with BEC, indicating vulnerability to external impersonations and suggesting stronger skepticism toward imitation of internal identities.

This disparity may stem from greater implicit trust in vendors or external partners across EMEA organizations, particularly given the high volume of cross-border business facilitated by mechanisms like the Single Euro Payments Area (SEPA). SEPA is a payment integration initiative designed to make cross-border euro payments as easy as domestic payments by requiring standardized formats for transactions.

APAC: Cultural and Compliance Factors Shape Risk

For APAC organizations, the data trended in the opposite direction of EMEA enterprises, with BEC engagement surpassing VEC. Though the variation is not as dramatic—BEC second-step engagement is just 10% higher—the rate itself (44.4%) remains concerning. Additionally, APAC employees had the highest BEC repeat engagement rate of any region (5.65%). However, while APAC employees engage with BEC attacks more than VEC, they at least report those attacks at a substantially higher rate, albeit still at a significantly lower than desired frequency (1.92%). Notably, APAC had the lowest vendor email compromise second-step engagement rate across all regions (40.24%), but even that remains far above acceptable levels.

The Bottom Line

In contrast to other regions, BEC poses the greater risk for APAC employees, with higher engagement and repeat interaction rates, but their comparatively higher reporting rate for BEC signals better recognition of internal threats.

44%

Global second-step engagement rate with VEC attacks

$80K

Median amount saved per organization by stopping vendor fraud

The higher BEC engagement and repeat rates may reflect the influence of strict, region-specific invoicing and documentation requirements, such as China's fapiao system, which could make vendor fraud attempts less convincing or easier to detect. Additionally, cultural factors—such as more hierarchical workplace dynamics in parts of the region—may contribute to employees being more likely to comply with authority-driven requests (a hallmark of BEC) without questioning their legitimacy.

North America: Equal Opportunity for Exploitation

Employees at organizations in North America demonstrated equal vulnerability to BEC and VEC attacks, with a negligible difference between the second-step engagement rates for both attack types. However, similar to EMEA, the repeat engagement rate for VEC attacks was considerably higher than for BEC attacks—7.42% vs. 2.69%. This indicates employees may not recognize they've been manipulated, increasing the risk of repeated engagement without targeted intervention or improved training. Like their counterparts in EMEA and APAC, North American organizations reported BEC attacks more often than VEC, though reporting remained low overall.

The Bottom Line

North American employees engage with VEC and BEC attacks at nearly equal rates but are more likely to fall for vendor email compromise attacks repeatedly, suggesting greater challenges in recognizing vendor-based deception.

The equal engagement rates indicate both internal and external impersonation attacks are equally believable to employees. However, the much higher VEC repeat engagement rate may reveal gaps in vendor verification processes and/or blind spots in security awareness training. This highlights the need for more targeted education on identifying vendor-based threats, particularly those that blend into routine workflows.

The Reporting Deficit in Email Security

If your organization relies on employee reporting to understand the full extent of attack frequency, we have bad news: only 1.46% of text-based advanced email attacks that are read are reported.

To put that in perspective, the average monthly text-based advanced attacks received by a mid-market enterprise with 1,500-3,000 employees between March 2024 and March 2025 was approximately 560 per 1,000 mailboxes. That means, every month, there are an estimated 840-1,680 attacks not being reported to the security team. For larger organizations, the number can be much, much higher.

1.46%

Employee reporting rate of text-based advanced attacks

Why Aren't Employees Reporting Malicious Emails?

The Bystander Effect

Though most often associated with emergencies, the bystander effect can occur in any setting where multiple individuals share equal responsibility to act. It refers to the tendency of people to do nothing when others are also present or impacted. Essentially, the more people who could act, the less likely it is that anyone will.

In this context, an employee may believe they aren't the only target of an attack, and thus they don't report the message because they assume a colleague already has. What should be emphasized is that even if a cybercriminal targets multiple employees, the sooner a malicious email is reported, the easier it is for the SOC team to minimize damage.

No Harm, No Foul

Some employees may believe that as long as they don't engage with the attacker, they've fulfilled their obligation to the organization. But security professionals know that deleting emails without reporting them can be almost as damaging, since it eliminates the SOC team's chance to investigate, remediate related messages, and take steps to reduce vulnerabilities to similar attacks.

Employees must understand that a message that they recognize as attempted invoice fraud or a bogus account update may not raise red flags for a coworker. And if attacks go unreported, bad actors can continue targeting others.

Fear of Being Wrong

In some cases, an employee may feel uncertain about their ability to distinguish safe emails from attacks. Rather than risk flagging benign messages, they stay silent, either out of fear of looking foolish or creating unnecessary work for the security team. This hesitation is especially common when cybersecurity feels disconnected from day-to-day responsibilities.

But this fear-based inaction can be costly, as a single overlooked attack can lead to widespread compromise if not caught in time. That's why it's essential to foster a workplace culture where reporting suspicious messages is encouraged, even when they turn out to be false alarms. Employees should be reassured that it's always better to err on the side of caution.

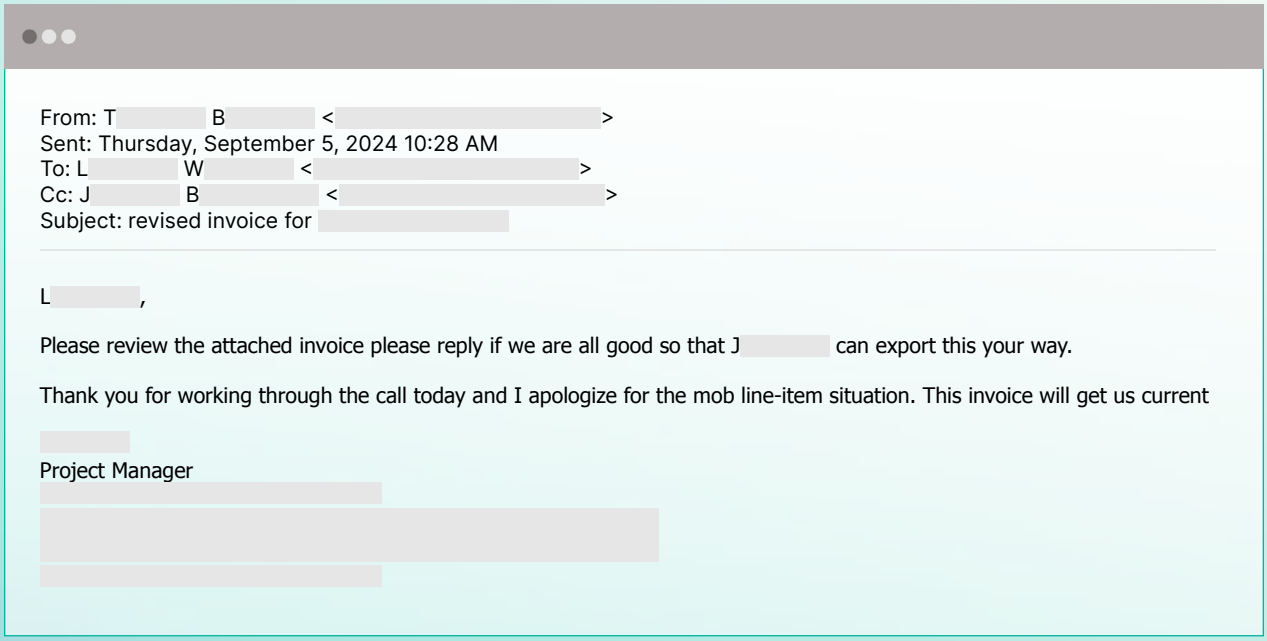
Thread Hijacked: Inside a Vendor Impersonation Attack

Note: This attack was observed during a risk assessment in which Abnormal was operating in read-only mode, which is why it was not proactively blocked.

Though awareness of modern attack tactics is growing, many professionals still operate under the assumption that today's email threats are just as poorly worded or obviously malicious as those from ten years ago. But today's cybercriminals continually improve their strategies and launch attacks that not only bypass legacy security tools but also trigger no alarm bells for the average employee, as these messages appear indistinguishable from real communications.

In the example below, the attacker poses as an employee at a construction equipment rental company, hijacks an existing thread with a partner, and attempts to divert future invoice payments.

The first email in a thread was a legitimate message from "T.B.," a project manager at the equipment rental organization, to "L.W.," an employee at a contracting services company, regarding an invoice for services rendered.



From: T B <>
Sent: Thursday, September 5, 2024 10:28 AM
To: L W <>
Cc: J B <>
Subject: revised invoice for

L ,

Please review the attached invoice please reply if we are all good so that J can export this your way.

Thank you for working through the call today and I apologize for the mob line-item situation. This invoice will get us current

Project Manager

Three weeks after this email was sent, the bad actor hijacked the thread using a lookalike domain, which was registered about a week and a half earlier and differs by only one letter from the real domain—a nearly imperceptible change. For privacy purposes, all identifying information has been censored, but a comparable example would be if the real domain were *missionus.com* and the attacker's email address was hosted on *misionus.com*.

Posing as "J.B.," an accounts receivable specialist at the construction equipment rental company, the perpetrator contacted L.W. regarding an update to the organization's payment processes. To increase the appearance of legitimacy, the threat actor copied and pasted the text of a fake email into the thread, making it seem as if they were following up on a previous message.

From: J B <>
Sent: Thursday, September 26, 2024 6:00 AM
To: L W <>
Cc: T B <>
Subject: Re: revised invoice for
Importance: High

L ,

As per the below email, could you please direct me to the right contact person to talk to?

---- On Tue, 24 Sep 2024 08:14:41 - 0700 **J B <>** wrote ----

Morning L ,

I wanted to inform you of an important update. We are carrying out an account reconciliation audit and our operating account is currently inactive and unable to accommodate payment at this time. Due to the ongoing audit, we have made the decision to streamline our payment processes by phasing our check payments and transitioning exclusively to electronic payments via EFT/ACH with immediate effect. This will help enhance efficiency and reduce the potential delays associated with traditional check payments.

To help facilitate this transition, we kindly request you acknowledge this email so we can send our new banking information to you for your records and also send me a list of open and due invoices please.

Please do not hesitate to contact me if you have more questions.

Thanks

The fabricated message claimed that due to an ongoing account reconciliation audit, the company's operating account had become inactive, and they were transitioning to electronic payments. The cybercriminal requested acknowledgment of the message so they could send new banking details. (As a note, had the customer not been in read-only mode, this is the point at which Abnormal would have remediated the message.)

The email contained no malicious links or attachments and had only minor grammar and punctuation issues. The attacker also used the impersonated employee's real email signature with the company's contact information and replaced T.B.'s address with a lookalike version hosted on the same maliciously registered domain.

Simply put, to most employees, the email would raise zero red flags, which is likely why L.W. replied to the threat actor and even added two colleagues to the thread to assist with the request.

From: L W <
Sent: Thursday, September 26, 2024 6:00 AM
To: J B <
Cc: T B <>; B L <>;
A E <>
Subject: Re: revised invoice for

+ B , A

Hi J ,

I'll touch base with our accounts team to make sure we get this hashed out properly.

Thanks,

Shortly after the target replied, the cybercriminal emailed again, this time posing as the project manager, T.B. To manufacture a sense of urgency, the bad actor claimed that the contracting services company had multiple outstanding invoices that were more than two months overdue.

From: T B <
Sent: Thursday, September 26, 2024 10:09 AM
To: L W <
Cc: J B <>; B L <>;
A E <>; L B <>
Subject: Re: revised invoice for

Thank you L ,

There are invoices that have been due for over 60 days and we need to bring your account current. J will send you the list of the invoices and our new ACH details. We will appreciate your swift response on when we can expect the payment.

L.W. once more responded and confirmed that as soon as the updated bank account information was provided, payment would be initiated.

From: L W <>
Sent: Thursday, September 26, 2024 5:56 PM
To: T B <>
Cc: J B <>; B L <>; A E <>; L B <>
Subject: Re: revised invoice for

T ,

We tried paying these invoices but it seems like we got caught in the middle of the transition. As soon as J sends over the new banking info we can get them pushed through.

On a side note, I received updated invoices that corrected company name, but invoice 643239 had an additional $150 charge that wasn't previously captured – see attached. What's the story here?

Thanks.

At this point, Abnormal stepped in to prevent the attack from moving forward, despite being in passive-only mode.

This attack underscores the increasing sophistication of vendor email compromise and the adept use of social engineering techniques by threat actors to exploit human trust. It also highlights the critical need to reduce employee exposure to malicious content and limit opportunities for engagement.

Why Behavioral AI Is the Best Defense Against Human-Centric Threats

Every time an employee has to decide whether an email is legitimate, the risk of human error enters the equation. And if they're wrong, cybercriminals won't hesitate to capitalize and cause financial consequences that ripple across the enterprise.

Today's threat actors know how to "hack the human" and continually develop new strategies for manipulating employees. They exploit human trust, compromise legitimate vendors, and weaponize routine business workflows.

The challenge is that organizations have limited control over their vendors' security postures and can only take steps to ensure their vendors' vulnerabilities can't be used against them. While security awareness training helps reduce the likelihood of employees engaging with threat actors, it's not enough on its own. Humans can't be your last line of defense.

The only effective strategy is to remove the burden of detection from employees entirely. That requires an innovative security solution—one that leverages AI to analyze identity, context, and content and builds behavioral baselines for every employee and vendor in your cloud environment. By understanding an organization's unique communication patterns, an AI-native email security platform can detect subtle behavioral anomalies that traditional tools miss, enabling it to flag suspicious communications and automatically remediate threats before they reach employee inboxes.

Precision matters—because detecting what doesn't belong starts with understanding what does.

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.

Interested in Stopping Modern Email Attacks?

Request a Demo ›

See Your ROI ›