Abnormal

Adversarial AI

Attacker Innovation Escalates Advanced Email Threats

H1 2025 EMAIL THREAT REPORT

Executive Summary

77%
Share of advanced attacks involving phishing

54%
Year-over-year increase in BEC attacks

88%
Likelihood of a BEC attack in any given week in 2024

70%
Weekly chance of being targeted by a VEC attack in 2024

Email remains the backbone of business communication, but its ubiquity and versatility make it an ideal target for cybercriminals. For decades, attackers have exploited its inherent vulnerabilities, continuously adapting their tactics to stay ahead of defenses.

Legacy security tools, built for an earlier era of threats, struggle to stop today's sophisticated attacks. Meanwhile, organizations relying on employees to spot threats are fighting a losing battle, as attackers craft malicious emails nearly indistinguishable from legitimate ones. Now, with AI fueling more deceptive, scalable attacks, the cyber arms race is escalating faster than ever.

Threat Actors Scale Attacks with Weaponized AI and Dark Web Resources

As generative AI adoption has surged, attackers have adapted the technology for nefarious purposes. Over the past two years, several malicious AI-powered tools have emerged, including multiple uncensored AI chatbots and even a large language model (LLM) developed specifically for cybercriminal purposes. These tools provide threat actors with unfiltered answers to queries otherwise blocked by traditional AI's ethical and safety restrictions.

This proliferation of weaponized generative AI—combined with the wealth of personal data easily found online and the treasure trove of hacking tools available on dark web forums—has lowered threat actors' barrier to entry, making it easier for novice attackers to get started and helping veteran cybercriminals uplevel their approach.

BEC and VEC Threats Still Plague Employee Inboxes

Driven in part by threat actors' increasing adoption of malicious AI—and further fueled by the ongoing success of these attacks—business email compromise (BEC) and vendor email compromise (VEC) have continued to climb. Using sophisticated tactics, cybercriminals can rapidly generate hyper-personalized campaigns that fail to arouse their target's suspicions and bypass legacy security solutions.

Between 2023 and 2024, BEC attacks rose more than 54%, and on any given week in 2024, organizations had, on average, a 70% chance of receiving at least one VEC attack.

Table of Contents

Email Remains Threat Actors' Preferred Entry Point

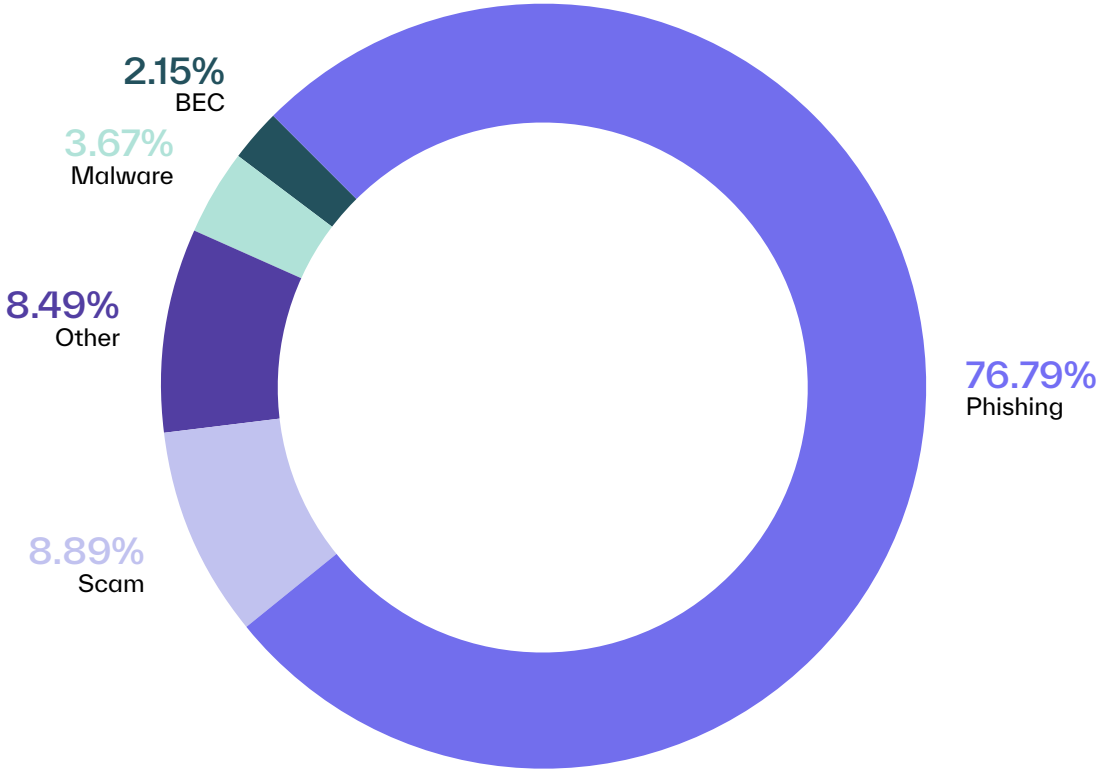
Email was never designed with security in mind, yet it has become the foundation of modern business communication—leaving organizations to address its inherent vulnerabilities. Over the decades, security measures have been layered on to mitigate its risks, but attackers have consistently adapted, finding new ways to exploit both technological weaknesses and human vulnerabilities. The result is an ongoing battle in which every advancement in security prompts an evolution in attack techniques.

The challenge is that the inbox remains an ideal access point for attackers, as it offers a more direct path into organizations than other methods, like exploiting software vulnerabilities or compromising IoT devices. Today, the widespread availability of AI-driven tools has made protecting the inbox even more difficult, as it has enabled cybercriminals to launch highly sophisticated and scalable attacks with unprecedented ease.

Phishing Continues to Dominate the Threat Landscape

As has been the trend since 2019, phishing remains the most common attack type, accounting for more than 76% of all advanced attacks. This isn't surprising, considering threat actors often use phishing to gain a foothold in an organization before initiating larger-scale or more sophisticated attacks.

Advanced Attacks by Type



The real challenge is that traditional defenses aren't keeping up. Both employee security awareness training and legacy email security solutions rely heavily on known indicators of compromise to detect phishing attempts, but attackers have discovered multiple ways to bypass these defenses and deceive end users.

Threat Actors Expand Attack Surface with Advanced Phishing Tactics

Today's attackers are relentless in their pursuit of new ways to enhance credibility, evade detection, and maximize the impact of their phishing campaigns.

File-sharing phishing is a popular tactic in which a threat actor exploits trusted file-hosting platforms like Dropbox, ShareFile, and Docusign to deceive targets. Because these solutions offer either free registration or no-charge trials, anyone—including cybercriminals—can create and send emails via the platform.

Consequently, bad actors can craft and dispatch malicious messages that are essentially identical to genuine notifications since the sender's address, email body, and embedded link are all legitimate. Further, because the target only encounters the phishing link after leaving the email environment and engaging with the shared file, these threats can easily bypass legacy tools.

Another strategy cybercriminals employ is multichannel phishing. Unlike traditional phishing, which relies solely on email, these campaigns start in the inbox but quickly move to text messages, phone calls, or messaging apps like WhatsApp or Telegram.

This approach increases the probability of deceiving employees since security awareness training primarily focuses on the email environment—not external channels. Additionally, by moving interactions from company-managed laptops to personal devices, attackers circumvent enterprise-level security controls.

Malicious AI is also transforming phishing by enabling attackers to craft highly convincing brand impersonations at scale. These tools generate grammatically flawless emails that mimic the tone, style, and structure of legitimate corporate communications, making fraudulent messages nearly indistinguishable from authentic ones.

The consequences of these AI-powered phishing attacks extend beyond initial credential theft. Many account takeovers—which can lead to financial fraud, data exfiltration, and internal system compromises—originate from phishing-based credential harvesting. With AI reducing the technical barriers to crafting realistic phishing lures, attackers can orchestrate more deceptive and scalable attacks, increasing the likelihood of successful breaches.

Business Email Compromise Attacks Accelerate

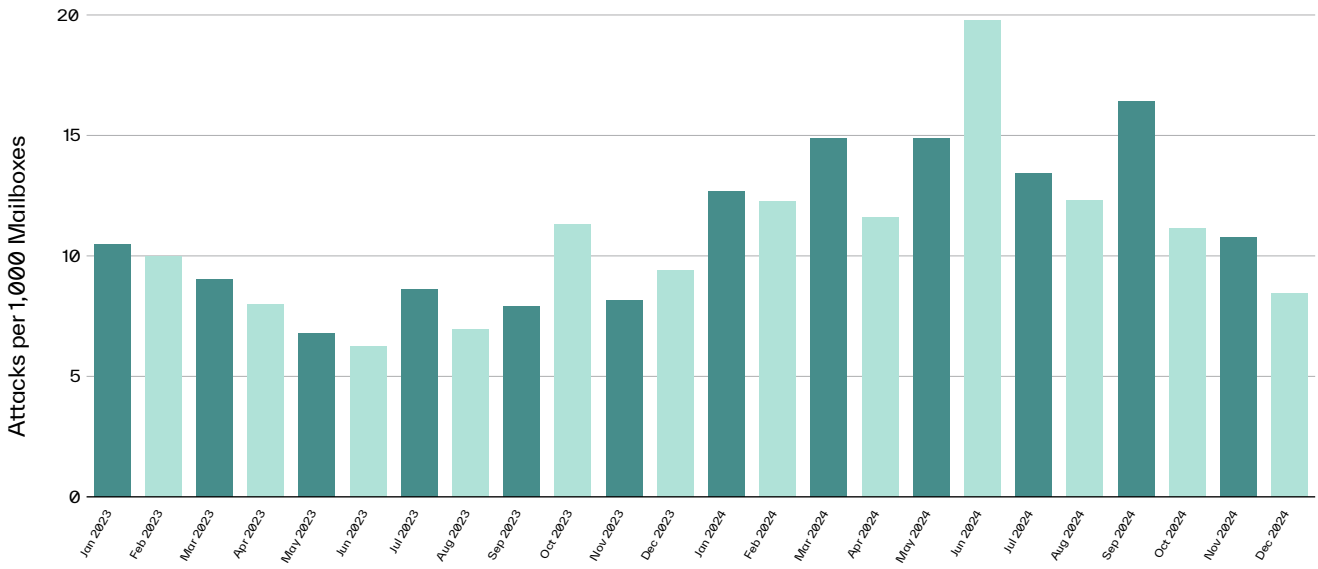
In business email compromise (BEC) attacks, threat actors meticulously research their targets and employ advanced social engineering tactics to impersonate a colleague or superior, manipulating employees into providing confidential information or completing fraudulent financial transactions.

While BEC only accounts for a small percentage of overall advanced email attacks, it's one of the most financially costly cybercrimes, causing $2.9 billion in losses in 2023 alone. It's also becoming more prevalent as threat actors increasingly turn to emerging tools and dark web resources to streamline and scale their attacks.

Median Monthly BEC Attacks Grow by More Than Half

Between 2023 and 2024, median monthly BEC attacks grew by more than 54%, topping out at nearly 20 attacks per 1,000 mailboxes in June 2024—roughly triple the number of attacks organizations saw in June 2023.

Median Monthly BEC Attacks, 2023—2024



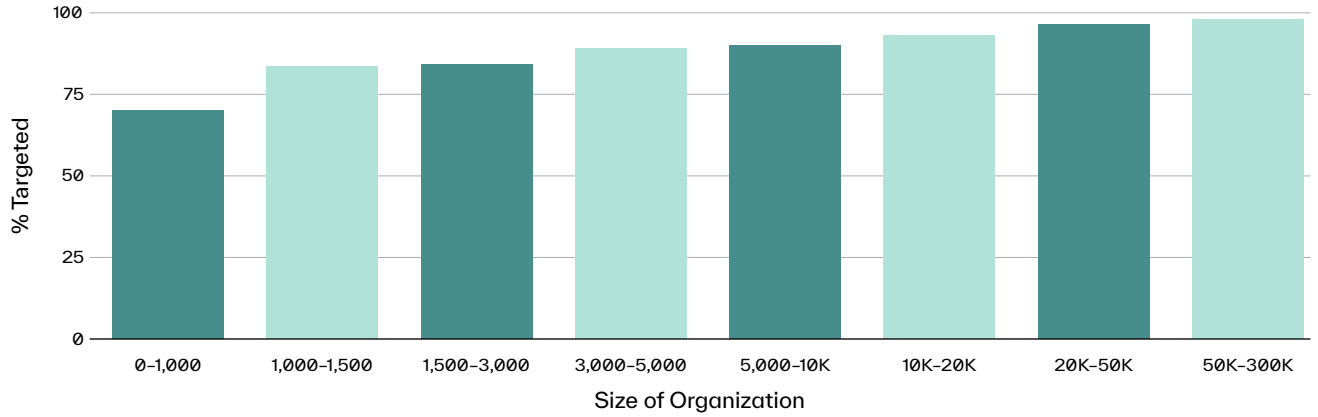
BEC had already established itself as a leading cyber threat, but the proliferation and democratization of AI have complicated matters, to say the least. AI-powered tools can be used to analyze extensive datasets from social media, online activity, and previous communications to craft hyper-personalized messages that convincingly mimic the writing style of the impersonated individual. These advanced techniques not only raise the likelihood of evading traditional security measures but also the likelihood of deceiving recipients, heightening the risk posed by BEC campaigns.

Additionally, while legitimate tools like ChatGPT have built-in measures to prevent malicious use, these can be circumvented with the right prompts. Plus, in the past two years, multiple uncensored AI chatbots and even a large language model (LLM) designed specifically for cybercriminals have surfaced, empowering novice attackers and helping experienced threat actors enhance their campaigns.

BEC Attack Risk Rises Most for Smaller Organizations

While enterprises of all sizes experienced an increased likelihood of BEC attacks over the past year, organizations with 1,000 inboxes or fewer saw the largest jump. On any given week in 2024, these smaller companies faced more than a 70% chance of receiving at least one BEC attack—up 14% from 2023.

Weekly Average: Percent of Organizations Targeted by BEC in 2024, by Organization Size



Interestingly, organizations with more than 50,000 inboxes saw the second largest year-over-year growth, at nearly 13%, with a 98% chance of receiving at least one BEC attack in any week of 2024.

What this data demonstrates is that BEC represents a major threat to organizations of all sizes, not just multinational enterprises. While large-scale breaches often dominate headlines, smaller businesses are equally, if not more, appealing targets for cybercriminals.

With limited resources, smaller organizations often struggle to not only maintain comprehensive cybersecurity defenses but also provide thorough employee awareness training, compounding their vulnerability. Many also lack dedicated IT teams or rely on outsourced IT support, which can delay threat detection and response. Moreover, cybercriminals know that smaller companies frequently serve as suppliers or partners to larger enterprises, making them an appealing entry point for broader supply chain compromises.

These factors underscore an undeniable fact: no organization, regardless of size, is safe from the risks of BEC.

Vendor Email Compromise Endures as Persistent Threat

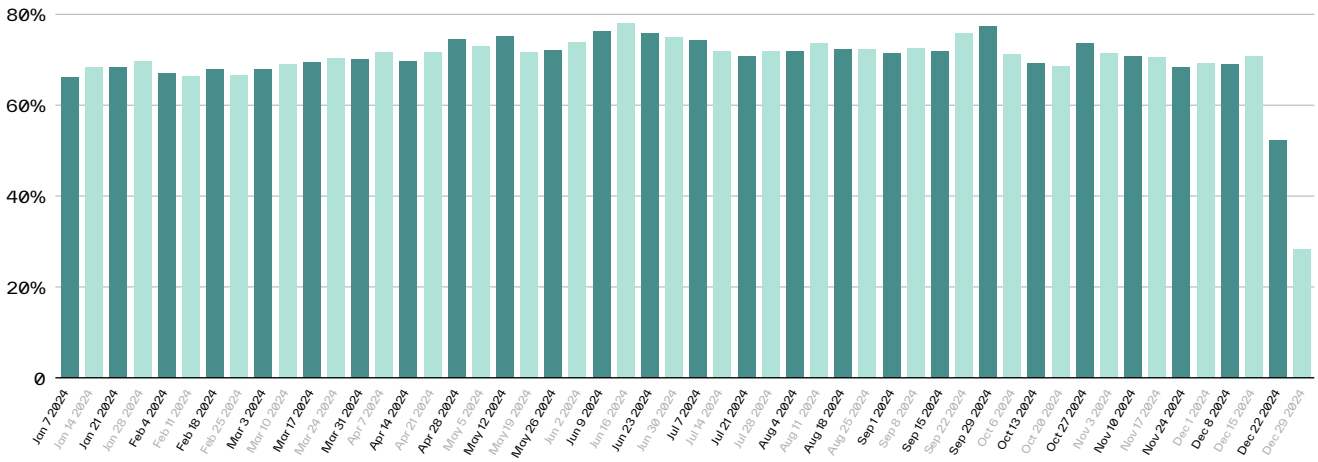
A subset of BEC, vendor email compromise (VEC) involves the impersonation of trusted vendors to manipulate targets into paying bogus invoices, updating banking details to divert funds from legitimate accounts, or completing fraudulent wire transfers. In some cases, attackers leverage compromised vendor email accounts and even hijack existing threads to deceive targets.

Like traditional BEC, this highly targeted scheme requires thorough research and well-developed social engineering skills. Of course, with weaponized AI at their disposal, even inexperienced cybercriminals are discovering how to pull off these complex attacks.

Vendor Email Compromise Sustains Its Momentum

On par with previous years, VEC attacks remained consistent and have shown no signs of dropping. During any given week in 2024, organizations had, on average, a 70% chance of receiving at least one VEC attack—an increase of more than 10% from 2023.

Weekly Average: Percent of Organizations Targeted by VEC, 2024



One of the biggest challenges in detecting VEC attacks is that the emails often appear routine. Every business, regardless of industry, works with at least one vendor, and large enterprises manage supply chains with hundreds of manufacturers, distributors, and suppliers. Thus, employees regularly receive invoice reminders or payment update requests, making fraudulent messages harder to spot.

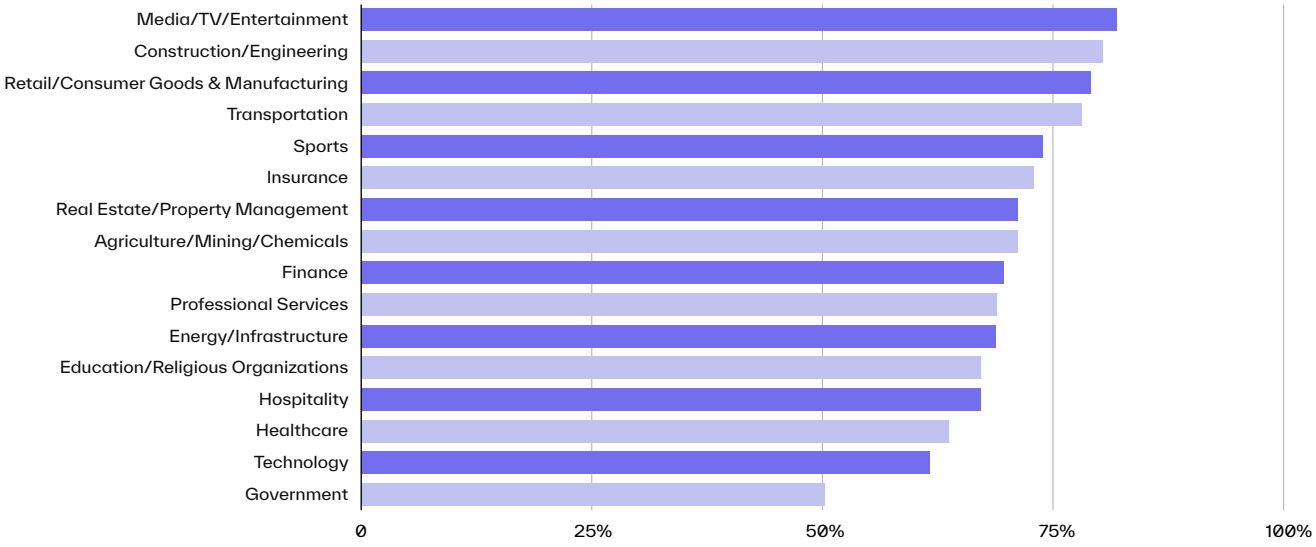
The scale of some vendor ecosystems means employees often lack visibility into individual relationships, leaving them unsure whether a request is unusual. This is especially true for new hires or employees reassigned to a different role after restructuring. Threat actors exploit this, and with AI-powered tools, they 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 also rush to resolve an apparent oversight—like a missing payment—without verifying the request. AI further amplifies this risk by helping cybercriminals make fraudulent invoices and follow-up messages more persuasive, increasing the likelihood of success.

Media, Construction, and Retail Industries Face the Highest Risk

While no sector is safe from VEC, some industries experience higher attack rates than others. In 2024, media and entertainment organizations led the pack, with a nearly 82% chance of receiving at least one VEC attack on any given week—the highest rate of all industries. Construction and engineering companies followed closely at 80%, with retailers and consumer goods manufacturers seeing an average weekly risk of 79%.

Weekly Average: Percent of Organizations Targeted by VEC in 2024, by Industry



The elevated risk can be attributed to several factors.

Media organizations operate in fast-paced environments and house high-value data, such as intellectual property, that can fetch a high price on the dark web. They also rely on complex vendor ecosystems, contracting with marketing firms, freelancers, production companies, talent agencies, and smaller service providers with less robust cybersecurity measures.

Similarly, construction and engineering firms as well as retailers and consumer goods manufacturers maintain high-value contracts and intricate supply chains, creating numerous entry points for attackers to exploit. These industries also face tight deadlines and high-pressure environments, which can lead targets to make hasty decisions or bypass due diligence, further increasing their vulnerability to VEC attacks.

Securing Your Organization Against Evolving Email Threats

The modern email threat landscape is defined by constant evolution, with cybercriminals continually responding to heightened awareness and improved defenses with new attack strategies designed to outmaneuver traditional defenses.

Generative AI has further amplified the problem, allowing threat actors to create highly sophisticated phishing, business email compromise (BEC), and vendor email compromise (VEC) attacks that appear indistinguishable from legitimate communications.

Each advancement by attackers highlights the limitations of legacy systems like secure email gateways, which lack the capabilities to detect the nuanced and adaptive nature of today's email threats. This leaves organizations who rely on traditional security tools vulnerable to potentially devastating breaches.

However, these attacks can be effectively neutralized with the right solution—one that leverages AI to analyze identity, context, and content and build behavioral baselines for every identity in your cloud environment. Understanding an organization's unique communication patterns enables an AI-native email security platform to precisely detect and then automatically remediate anomalous messages before they ever reach employee inboxes.

Investing in AI-native, API-based email security is no longer optional—it's essential. By proactively blocking these attacks, organizations can protect their employees and mitigate the risk of costly mistakes, securing their operations against both existing and emerging threats.

Abnormal

Abnormal Security 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, Salesforce, ServiceNow, Zoom, Amazon Web Services and multiple other cloud applications.

Interested in Stopping Modern Email Attacks?

Request a Demo →

Follow Us on X/Twitter →