Omdia
by informa techtarget

AI-enabled Deception, Impersonation, and Phishing

Security operations and the impact of human-centered attacks

Author: Dave Gruber, Principal Analyst

April 2026

Contents

Introduction

As the security operations (SecOps) agenda shifts toward building a more autonomous security operations center (SOC), security analysts continue to face growing challenges from attacks that exploit human behavior. The success rates of business email compromise (BEC), account takeover, and identity theft are rising as attackers increasingly leverage AI to craft more authentic, rapid, and highly targeted socially engineered attacks—amplifying the impact of an enduring, email threat vector.

As a result, SecOps teams face considerable strain, as both automated alerts and user-reported email or communication-related escalations flood daily queues, leaving little capacity to focus on proactive security strategies that could strengthen security posture and mitigate future risks.

Defenders must respond rapidly, putting AI to work to become more aware, more nimble, more efficient, and ultimately, more effective. For security leaders, this means more than incremental change, instead requiring aggressive investment and rapid iteration of security strategies, processes, and technologies. This includes adopting more automated solutions in addition to implementing robust threat detection and mitigation mechanisms capable of preempting human-targeted attacks before they reach intended victims.

To address these challenges, SecOps leaders should actively collaborate with email security stakeholders to clearly define their requirements and participate in decision-making processes. This will ensure that email security solutions align with SecOps objectives and operational needs, enabling teams to better mitigate threats and improve operating efficiency.

This paper explores cybersecurity strategies to combat an increasingly AI-enabled adversary—the use of AI within the security mechanisms used to defend the human threat vector—and opportunities to move to a more proactive security agenda to reduce the human attack surface.

The impact of an AI-enabled adversary

As the adversary rapidly adopts AI, the fundamental economics and speed of criminal activities are changing. AI enables a lower-cost attack model, faster attack iteration and learning rates, and ultimately, higher attack success rates. These dynamics are leading to compounding levels of business impact, with increasing levels of fraud success rates, data exposure, trust erosion, and regulatory consequences.

Every aspect of the threat landscape is being impacted by the advent of an AI-enabled adversary, but none more so than those targeted directly at humans. Phishing, impersonation, and account takeover attacks are all seeing rapid advancement in speed, accuracy, diversity, and effectiveness in fooling people into helping adversaries achieve their objectives.

According to IBM X-Force research[1], attackers can now generate effective phishing campaigns in just five minutes using five prompts—a process that previously required 16 hours of human effort. The result is a threat landscape where AI-generated phishing achieves 54% click-through rates compared to 12% for traditional campaigns, according to 2025 research from Brightside AI.[2]

The rise of phishing email click-through rates has resulted in financial losses increasing 26% year-over-year, of which cyber-enabled fraud represented 85%.[3] In March 2026, advanced email attacks increased by 88% when compared to March 2024, and more recently, increased by 43.9% from February 2026 to March 2026, continuing a growth trend in advanced email attacks that can be traced as far back as January 2023.[4]

Email has had a long history of offering a direct channel for attackers to dupe unsuspecting end users into helping adversaries advance their objectives. Once considered an isolated threat vector defended by signature-based-only email security tools, the human threat vector is now widely used in support of more complex attacks to acquire credentials or sensitive information, or to impersonate others to facilitate BEC, as attackers leverage supply chains to gain access to financial transactions.

[1] Source: Stephanie Carruthers, "AI vs. human deceit: Unravelling the new age of phishing tactics," IBM.com, 2026.
[2] Source: "AI-Generated Phishing vs Human Attacks: 2025 Risk Analysis," brside.com, 2025.
[3] Source: Abnormal AI Threat Data, March 2026.
[4] Ibid.

2025 FBI Report

"AI technology enables the creation of convincing synthetic content, such as social media profiles and personalized conversations, often in mass quantities. People have manipulated video and audio similarly for decades, but the widespread availability of this developing technology makes it possible to create high-quality content. AI-enabled synthetic content is becoming increasingly difficult to detect and easier to make, which allows criminal actors to potentially conduct successful fraud schemes against individuals, businesses, and financial institutions."

Chat generators can quickly create official-sounding emails mimicking a company's CEO or other officials. These emails can contain phishing links or directions to wire funds. Voice cloning can also be used to request wire payment.[5] This attack pattern requires new visibility and insights for SecOps analysts as they investigate and understand the details about specific techniques used in more complex attacks. At the same time, more integrated, broad visibility and analytics are needed to support SecOps teams as they investigate threats that involve signals from multiple threat vectors.

As a result, security leaders are reevaluating email security solutions, with an expanded lens on defending against more sophisticated, multi-vector attacks; more accurate, believable socially engineered attacks; and a massive acceleration in iteration and refinement of attacks.

Preparing for an AI-enabled security world

The rapid transformation brought about by AI is fundamentally altering the cybersecurity agenda. Cybersecurity teams must now contend with a more dynamic AI-enabled attack surface, increasingly comprised of emerging AI-enabled external partner and supply chain solutions. Meanwhile, the adversary is aggressively leveraging AI to execute faster, more sophisticated attacks, driving the need for speed throughout all aspects of the cybersecurity process. As security programs transform to address these changes, virtually every aspect of cybersecurity is in play. As a result, broad cybersecurity transformation is needed to respond to the demands of the AI era.

Deconstructing the impact of AI across the broader organization, security leaders have parallel agendas: first, to secure the use of AI throughout their broader organizations; and

[5] Source: "Federal Bureau of Investigations Internet Crime Report 2025," FBI Internet Crime Complaint Center (IC3), 2025.

second, to employ AI within their own security programs to defend against AI-enabled adversaries in an environment where so much of the attack surface is in transition as AI-enablement takes place. This leaves resource-constrained security leaders with the task of charting a roadmap to navigate their own AI journey within cybersecurity, while they, in parallel, are expected to secure a massively changing IT infrastructure.

7 key AI security challenges

While security teams continue to face ongoing challenges, the rapid adoption of AI throughout their IT estate is creating additional security challenges fueled by several dynamics:

- **Rapidly changing attack surface:** The dynamic nature of AI-powered systems and the data that powers them requires constant monitoring and adaptation. Existing detection and monitoring capabilities are lacking, requiring new AI discovery and exposure management capabilities.
- **Accelerating attack execution speeds:** AI-enabled attacks occur at unprecedented speeds and diversity, leaving little time for reactive measures.
- **Expanding threat vectors:** AI introduces novel attack methods, such as adversarial machine learning and data poisoning. Combating these threats requires new AI-specific security controls and a new focus on data security for the AI data pipeline. Existing threat vectors, including email and communications channels face new levels of impersonation accuracy and highly tailored phishing tactics.
- **Massive increase in security data:** AI-enabled systems generate vast amounts of security data, overwhelming traditional security tools. Re-architecture of existing security data mechanisms is often needed to support the scalability of this resource.[6]
- **Increasing volume of vulnerabilities:** As AI infrastructure and the data pipeline that powers it expand, so do the volume of misconfigurations and vulnerabilities, leading to reduced security posture. New risk-driven security strategies are needed to overcome these challenges, prioritizing the highest-risk exposures.
- **Further collapse of the perimeter:** The shift to cloud-based and AI-driven infrastructures has rendered most traditional perimeter defenses obsolete. In addition, many early custom AI deployments depend on more local data, requiring new data and perimeter security strategies.
- **AI-enabled external supply chain:** Organizations are grappling with the need to secure not only their internal systems but also the external supply chain, which is increasingly

[6] Source: Omdia Complete Survey Results, *Results Are in: Agentic AI in SecOps Is Exceeding Expectations*, February 2026.

reliant on AI-driven solutions. This sprawl amplifies vulnerabilities, many of which are owned by external organizations, as every node in the supply chain becomes a potential entry point for adversaries. The challenge is further compounded by the rapid pace of AI adoption throughout the supply chain, which often outstrips the ability of IT teams to implement robust security measures.

Combating an AI-enabled adversary

To address these new challenges, organizations need to rapidly upgrade strategies and tools capable of keeping up. Key operating requirements must include:

- **Speed:** Real-time threat detection and response are essential to counter AI-enabled attacks.
- **Scale:** Security solutions must be capable of handling the massive datasets generated by AI systems.
- **Consolidation:** Converged data platforms and tools streamline operations and improve efficiency.
- **Visibility:** Securing AI infrastructures, data pipelines, and agent operating models is critical to maintaining a robust cybersecurity posture in the AI era and requires new discovery, visibility, and monitoring mechanisms.
- **Proactive measures:** Prevention alone is insufficient; organizations must adopt proactive strategies to anticipate and mitigate threats.
- **Adaptive:** Security tools must evolve as quickly as the threats they combat.

The changing requirements for email security solutions

Fighting back requires a new level of AI-enabled cybersecurity strategies, enabling defenders to predict, detect, and deflect at a new level of precision and speed. But while fighting AI-enabled attacks with AI-enabled cybersecurity has the potential to neutralize this threat, navigating where, when, and how is a challenge for many.

Behavioral AI-based detection

Email security solutions, once focused on preventing malware, have similarly expanded to address the changing threat landscape, but few are able to keep up with the new levels of speed and refinement coming from an AI-enabled adversary.

Unlike machines, human behavior is much less predictable. With AI rapidly raising the quality of phishing attempts, detection based on fixed, known patterns is no longer enough. More sophisticated behavioral detection mechanisms, capable of recognizing massive numbers of variants as attackers refine and diversify attacks, are needed.

Socially engineered attacks utilize every possible communications channel used today. Detecting threats across platforms beyond and connected to email are table stakes in keeping up with advanced threats, including mechanisms such as Teams, Slack, and other SaaS communications platforms.

With these more advanced detection capabilities, the risk of increasing false positives is high. Solutions must, therefore, have the fidelity to keep false positive rates low in the process.

Contextualizing identities and behaviors

Generalized behavioral analytics fall short, as AI makes it faster and easier for adversaries to do deep target research and create unique and specific attacks aligned with specific targeted individuals. Continuous understanding, baselining, and monitoring of specific known good behaviors within emails, conversations, and business practices for specific identities is therefore foundational to detecting modern threats.

Identity-specific usage patterns extend beyond email security, requiring email, endpoint, and other end-user security solutions to work in collaboration with each other. Scaling to support highly complex, cloud-based email and communications ecosystems goes beyond basic collaboration, requiring an exchange of intelligence and signals.

Automation

Analyst burnout is a well-documented concern, driven by the stress of demanding workloads that require rapid, high-pressure decision-making. Manual tasks don't just hinder the day-to-day operations; they also make it harder for analysts to "zoom out" and focus on the bigger picture.

Nearly three-quarters of analysts reported a lack of time for strategic work, a clear sign that SOC teams struggle to effectively automate low-value tasks.[7] As a result, analysts can feel stuck in the weeds—without the capacity to focus on higher-impact initiatives such as threat hunting, more complex threat investigations, or more proactive security activities.

As shown below, alert fatigue is the top challenge analysts face when completing SOC tasks.

[7] Source: Omdia Custom Research commissioned by Abnormal, July 2025.

What are the biggest challenges you face in completing your SOC tasks?[8]

- **Alert fatigue:** 49%
- **Too many tasks/overwhelming workload:** 44%
- **Inability to automate repetitive tasks:** 38%

The pressures of the work environment are clear: analysts are expected to manage too many tasks at a pace that is unsustainable without automating repetitive processes. Furthermore, these manual processes have notably eroded analysts' productivity (see below).

How have manual processes negatively impacted your day-to-day activities?[9]

- **Spending too much time on repetitive tasks:** 44%
- **Increased burnout:** 35%
- **Slower response time (MTTR):** 31%

As AI-enabled email security and SOC tools enable more automated investigation, response, and replies to user-reported emails, SecOps teams can thwart attacks earlier—before they progress in the attack chain. Automation further frees security analysts from repetitive tasks to focus on more complex threat investigations while handling higher volumes of threats without feeling burnt out.[10]

Supply chain protection

A lack of control over supplier security practices leaves security leaders at risk of inbound compromise through otherwise trusted channels. With a rapid deployment of AI-enabled systems and tools within all aspects of the supply chain and with continued BEC and impersonation use for financial fraud, organizations are at a new level of risk from supply chain-related attacks.

Continuous understanding, baselining, and monitoring of specific known good and expected behaviors within supply chain-related emails, conversations, and business processes for certain supply chain partners and identities is foundational to preventing fraud and other criminal activities.

Sophisticated invoice and vendor fraud attacks frequently thwart native email security capabilities, requiring new levels of partner behavioral detection and tracking, including for financial institutions, accounts, and transactions.

[8] Ibid.
[9] Ibid.
[10] Ibid.

End-user productivity and confidence

When end users spend time evaluating and escalating potential phishing or other fraudulent email and communications activities, they operate more slowly. This negative impact on individual productivity adds up to massive efficiency impacts across every level of larger organizations, from executives to individual contributors.

When email and communications security mechanisms filter out phishing and fraudulent communications before they reach the end user, individuals work faster and more efficiently. This pattern evolves over time, and, as end users gain trust in the effectiveness of security solutions, they can operate with more confidence and agility.

The more effective security solutions are, the less time is spent reporting suspicious communications and reading replies from the security team. When end users can trust that communications security mechanisms have their back by ensuring that sensitive information doesn't leak out of the organization, they can communicate with confidence.

Collaboration

Collaboration with other security tools is more important than ever as human-assisted attacks transform into complex attacks. With email and other communications mechanisms used by attackers to achieve individual tactics within an attack chain, email solutions must integrate and share signals and intelligence with SecOps tools in support of more complex threat investigations and response actions.

Automated response actions must be able to integrate, inform, and initiate action with security ecosystems. These include, but are not limited to, network, endpoint, identity, and cloud security mechanisms.

Introducing Abnormal AI

Abnormal AI is a modern, AI-native email security solution, utilizing proven behavioral threat detection strategies to prevent email threat progression. Core capabilities include:

- **AI behavioral threat detection.** Traditional security tools often miss sophisticated attacks that exploit human trust and routine workflows. Abnormal AI uses behavioral AI to detect threats based on identity, relationships, language, and context—not just links or attachments. The solution provides:
  - Hyper-personalized social engineering detection.
  - Behavioral profiling to identify anomalies in communication patterns.

  - Prevention of BEC and vendor email compromise (VEC).

- **Identity and access risk modeling.** Account takeover and identity misuse are critical concerns for security teams. Abnormal AI continuously monitors account behavior across email and connected SaaS applications to detect deviations from a user's normal identity patterns, indicating early signs of compromise. The solution provides:
  - Login behavior analysis and session monitoring.
  - Detection of privileged delegation misuse and lateral movement.
  - Unified view of user risk across platforms.
- **Human risk intelligence and adaptive training.** Attackers increasingly exploit human emotions like curiosity, fear, and trust. Abnormal AI provides AI-driven simulations and adaptive human risk management tailored to the specific threats users are most likely to face, including:
  - Real-time risk measurement for individual users.
  - Behavioral reinforcement through targeted training.
  - Focus on emotional manipulation tactics used in modern attacks.
- **Continuous email posture management.** Misconfigurations, risky permissions, and OAuth exposure quietly expand the email attack surface. Abnormal AI helps security teams proactively manage and secure their email environment. The solution provides:
  - Detection of misconfigurations and risky permissions.
  - Monitoring of OAuth exposure and other vulnerabilities.
  - Continuous improvement of email security posture.
- **Automated abuse-mailbox triage.** Security teams often struggle with triaging user-reported emails. Abnormal AI automates the classification, enrichment, and response to abuse-mailbox submissions, turning them into actionable insights. It provides:
  - Automated classification of user-reported threats.
  - Enrichment of threat data for faster analysis.
  - Machine-speed remediation of malicious emails.

- **Autonomous response and SOC integration.** SecOps professionals need tools that reduce manual intervention and integrate seamlessly into their workflows. Abnormal AI offers autonomous threat remediation and integration with SecOps tools. It provides:
  - Automated removal of malicious emails without analyst intervention.
  - Integration with SIEM and SOAR platforms for unified workflows.
  - Real-time threat intelligence sharing across tools.
- **Addressing AI-powered threats.** Attackers are increasingly using generative AI to create hyper-personalized phishing campaigns and social engineering attacks. Abnormal AI is designed to counter these advanced tactics with AI-native analysis, providing:
  - Detection of AI-generated phishing and impersonation attempts.
  - Insights into attacker tactics, techniques, and procedures.
  - Real-time adaptation to emerging threat patterns.
- **VEC protection.** Supply chain attacks targeting vendors are a growing concern. Abnormal AI monitors vendor communication patterns to detect and prevent VEC. The solution provides:
  - Behavioral analysis of vendor communications.
  - Alerts for unusual or suspicious vendor activity.
  - Prevention of fraudulent invoices and wire transfers.
- **Reducing operational overhead.** Security teams are often overwhelmed by alerts and manual tasks. Abnormal AI reduces operational drag by automating threat detection, triage, and response and provides:
  - Reduction of false positives through AI-driven accuracy.
  - Streamlined workflows for faster incident resolution.
  - Measurable outcomes that improve efficiency.
- **Staying ahead of 2026 threat trends.** The 2026 threat landscape is defined by AI-powered attacks, emotional manipulation, and advanced social engineering. Abnormal AI equips security teams with the tools to proactively defend against these evolving threats by providing:

- AI-native analysis of telemetry data (e.g., sender reputation, geolocation, communication patterns).
- A focus on preventing breaches before they occur.
- Continuous updates to address new attack techniques.

Conclusion

The human attack surface is the gift that keeps on giving to criminal and nation-state adversaries. Despite continuous investment in email security tools, attackers continue to succeed in reaching and fooling individuals in support of identity theft, socially engineered attacks, BEC, and account takeover. In parallel, email security solutions flood SecOps teams with daily investigation tasks and often lack the context needed to accurately identify and mitigate risk. Modernization is needed in defense of this critical threat vector.

Solutions from vendors like Abnormal AI are highly relevant to SecOps and email security professionals in combatting this growing threat vector. AI-driven, behavioral detection and response, coupled with highly automated actions, both strengthen security posture and reduce the burden on SecOps teams.

Omdia recommends that organizations reevaluating or modernizing email and communications security solutions consider Abnormal AI to protect this growing threat vector.

This Omdia White Paper was commissioned by Abnormal AI and is distributed under license from TechTarget, Inc.

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B Materials information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Get in touch

www.omdia.com
askananalyst@omdia.com

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.