# AI-powered phishing attacks surge 70% with billion-dollar business email scams on the rise



As artificial intelligence continues to evolve, so too does its application in the realm of cybercrime, particularly in the crafting of phishing emails that have garnered a reputation for being more sophisticated and convincing than ever before. Recent reports indicate that the emergence of AI-driven techniques has drastically transformed the landscape of phishing attacks, rendering many traditional detection methods ineffective.

According to a recent threat intelligence report from the security firm Cofense, the rate of phishing emails has surged alarmingly, with one malicious email detected every 42 seconds in 2024. This represents a substantial year-over-year increase of 70%, with AI significantly enhancing the ability of these attacks to circumvent legacy email filters. The sophistication of these attacks lies in the use of generative AI tools, which allow perpetrators to craft emails with impeccable grammar, authentic formatting, and personalised content, directly targeted at recipients, including corporate executives.

The evolution towards business email compromise (BEC) scams has become one of the most pressing concerns for organisations. These scams often impersonate C-suite executives with alarming precision, utilising near-perfect formatting and replicating established email threads to bolster their legitimacy. The implications of this shift are profound: the average cost of data breaches attributed to these types of scams has spiralled to approximately $4.9 million in 2024, necessitating an urgent response from companies to enhance their cybersecurity measures.

This trend is echoed across multiple reports indicating a marked increase in the sophistication of phishing attempts. For instance, a report by SlashNext reveals a staggering 703% increase in credential phishing attacks in the latter half of the year. Individual users now receive at least one advanced phishing link capable of bypassing traditional network security measures each week, with 80% of embedded malicious links being previously unknown zero-day threats. The reliance on static threat intelligence and conventional signature-based detection methods has proven insufficient in combating these rapidly evolving tactics.

The trajectory of AI-enhanced phishing attacks is compounded by the rise of polymorphic campaign strategies. These tactics allow attackers to change the content of their phishing schemes in real time, thereby effectively eluding detection by dynamic email filters. Reports underline that over 82.6% of phishing emails analysed now incorporate some form of AI, making it increasingly difficult for security systems to keep pace.

Despite heightened awareness among users concerning phishing threats, the effectiveness of training is waning. Data suggests that enterprise users were three times more likely to inadvertently engage with phishing content in 2024 compared to previous years—a trend attributed to cognitive fatigue from continuous attempts, coupled with the adaptability of attackers. This adaptability is greatly enhanced by large language models (LLMs), which have automated the generation of diverse and grammatically flawless phishing lures, complicating detection protocols even further.

In response to this evolving threat landscape, experts advocate for a more proactive approach towards phishing prevention. Users are urged to scrutinise email content, particularly when financial actions or urgent requests are involved. Verification of internal requests using established contact methods is essential, as is exercising caution when engaging with unsolicited messages, regardless of their professional appearance.

The necessity for advanced security solutions that extend beyond traditional perimeter defences cannot be overstated. Businesses are encouraged to adopt tools that offer post-delivery analysis and a threat response framework predicated on behavioural intelligence, thus enabling a more resilient defence against the increasing prevalence of AI-fuelled phishing attacks.

As the utilisation of generative AI continues to proliferate, it is imperative for organisations to remain vigilant and continually adapt their cybersecurity strategies. The stakes are higher than ever, and responsive, informed actions are essential to safeguard against the escalating sophistication of phishing scams in the digital age.

### Reference Map

1. Paragraphs 1, 2, 3
2. Paragraph 3
3. Paragraphs 4, 5
4. Paragraph 5
5. Paragraphs 6, 7
6. Paragraph 8
7. Paragraph 8

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.techradar.com/pro/security/ai-is-making-phishing-emails-far-more-convincing-with-fewer-typos-and-better-formatting-heres-how-to-stay-safe> - Please view link - unable to able to access data
2. <https://www.ft.com/content/d60fb4fb-cb85-4df7-b246-ec3d08260e6f> - This article discusses the rise of AI-generated phishing scams targeting corporate executives. Companies like Beazley and eBay have reported an increase in fraudulent emails containing personal details obtained through AI analysis of online profiles. AI bots can quickly ingest large quantities of data about the tone and style of a company or individual and replicate these features to craft a convincing scam. The proliferation of generative AI tools has made it easier for cyber criminals to conduct sophisticated scams, resulting in a rise in the frequency and quality of phishing attacks. These AI-driven phishing emails can often bypass standard email filters and cybersecurity defenses, posing a significant risk to companies. The increasing sophistication of these attacks has led to a surge in the costs associated with data breaches, which reached an average of $4.9 million in 2024. Businesses are urged to remain vigilant as AI continues to advance, making it essential to enhance cybersecurity measures to counteract these threats.
3. <https://slashnext.com/press-release/2024-eoy-phishing-intelligence-report/> - SlashNext's 2024 Phishing Intelligence Report reveals a significant surge in phishing attacks, with credential phishing increasing by 703% in the latter half of the year. The report highlights a 202% rise in overall email-based threats, with individual users receiving at least one advanced phishing link per week capable of bypassing traditional network security controls. Additionally, 80% of embedded malicious links were previously unknown zero-day threats, underscoring the limitations of static threat intelligence and signature-based detection methods. These findings emphasize the evolving and escalating nature of phishing attacks, particularly those leveraging AI technologies.
4. <https://www.knowbe4.com/press/new-knowbe4-report-reveals-a-spike-in-ransomware-payloads-and-ai-powered-polymorphic-phishing-campaigns> - KnowBe4's latest Phishing Threat Trends Report highlights a 17.3% increase in phishing emails between September 15, 2024, and February 14, 2025, compared to the previous six months. Notably, 82.6% of all phishing emails analyzed exhibited some use of AI. The report also observes a 22.6% increase in ransomware payloads and a surge in phishing hyperlinks, malware, and social engineering tactics bypassing traditional detection methods. These trends underscore the growing sophistication of phishing attacks, particularly those utilizing AI to enhance their effectiveness.
5. <https://www.zscaler.com/press/zscaler-research-finds-60-increase-ai-driven-phishing-attacks> - Zscaler's research indicates a 60% increase in AI-driven phishing attacks, with vishing (voice phishing) and deepfake phishing on the rise as attackers leverage generative AI to amplify social engineering tactics. The report also highlights that the finance and insurance industry faced 27.8% of overall phishing attacks, marking a 393% year-over-year increase. Microsoft remains the most imitated brand, with 43.1% of phishing attempts targeting it. These findings emphasize the escalating threat posed by AI-enhanced phishing campaigns across various sectors.
6. <https://www.csoonline.com/article/3801010/phishing-click-rates-tripled-in-2024-despite-user-training.html> - Despite increased security awareness training, enterprise users were three times as likely in 2024 to land on phishing pages compared to the previous year. This surge is attributed to cognitive fatigue from constant phishing attempts and the adaptability of attackers in delivering harder-to-detect baits. The rise of large language models (LLMs) has enabled attackers to automate the creation of more diverse, grammatically correct, and targeted phishing lures, further complicating detection and prevention efforts.
7. <https://www.zscaler.com/blogs/security-research/phishing-attacks-rise-58-year-ai-threatlabz-2024-phishing-report> - Zscaler's ThreatLabz 2024 Phishing Report reveals a 58% increase in phishing attacks, with AI enabling novice threat actors to become skilled social engineers and sophisticated phishing attackers. AI automates and personalizes various components of the attack process, making phishing attacks more sophisticated and difficult to detect. The report also highlights the rise of vishing and deepfake phishing, increasingly favored social engineering tactics that use AI-powered impersonation tools.