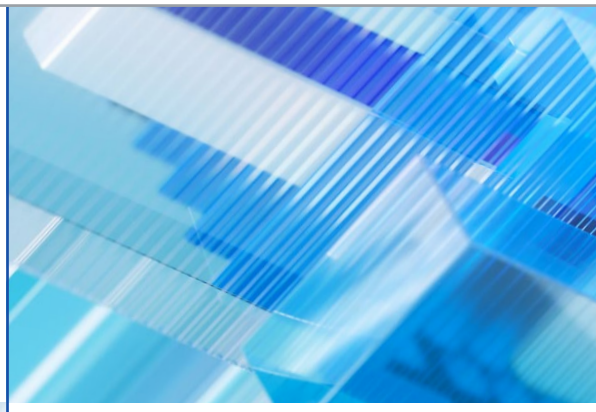
Google

Published May 2025

Case study: Leveraging AI through the Global Signal Exchange to tackle scams



Introduction

Global scam losses are estimated to have totaled over $1 trillion in 2024 and are expected to exceed this total again in 2025.

AI plays a crucial role in the fight against scams and fraud, allowing us to accelerate the detection of abuse, generate insights, and scale our efforts against harm on Google's platforms. In October 2024, we announced a new partnership with the Global Anti-Scam Alliance (GASA) and the DNS Research Federation (DNSRF) to launch the Global Signal Exchange (GSE), a global, multi-stakeholder, and cross-sector clearinghouse for bad actor signals. The GSE represents a collaborative effort to pool resources and expertise in the fight against scams, enabling faster identification and disruption of fraudulent activities across various sectors, platforms, and services.

This report outlines the latest progress on how Google's AI technologies are being leveraged by the GSE in the fight against scams. While AI is being misused to produce more sophisticated scams, defenders can leverage the full power of Google AI to disrupt these fraudulent activities. We detail how we're working with the GSE to apply AI-based innovation to generate insights and inform a more targeted and coordinated effort against scams.

The growing global threat of scams

AI has not necessarily created novel scam categories, but it has been misused to transform existing fraud abuse vectors and criminal approaches to established fraud techniques through new capabilities and efficiencies. Transformer-based large language models, text-to-image, and video and audio generators have all been leveraged to enhance and scale traditional scams by exploiting vulnerabilities more effectively.

Such technologies have the potential to significantly augment malicious operations in the future, enabling threat actors with limited resources and capabilities. This trend poses a significant challenge for law enforcement agencies, cybersecurity firms, and technology organizations, necessitating the development of innovative strategies and technologies to combat this evolving threat. Fortunately, as explained in this report, AI developments are advancing rapidly to combat scams and are strengthened by collaboration across the ecosystem.

Google's approach to tackling online scams

Google takes proactive steps to combat scams and fraud to protect our users, deliver reliable information, and collaborate across the online platform ecosystem to create a safer internet experience for all.

In 2024, we blocked or removed 415 million ads and suspended over 5 million accounts for violating our ads policies most closely associated with scams; with our AI-powered models in Google Ads contributing to the detection and enforcement of 97% of the pages on which we took action.

For more than a decade, Google has used advancements in AI to protect users from online scams where malicious actors deceive users to gain access to money, personal information, or both. Our measures include AI-powered technologies built into our products, a distinct set of policies and guidelines (such as for Ads, Play, and YouTube), and programs such as the Google Priority Flagger Program to enable trusted expert organizations to report abuse directly to our Trust & Safety teams to help prevent, detect, and respond to harmful and illegal content. We also scale our industry-leading practices to keep users safe online through proactive engagements and events with experts and third-party organizations. More information on our policy recommendations for collectively tackling scams can be found in our recently published white paper, which covers how we tackle abuse at scale, including our product protections from scams and fraud.

As a founding partner of the Global Signal Exchange (GSE), we have connected several Google products to the GSE at various stages of the integration lifecycle, enabling us to ingest over 16 million signals and share over 7 million signals. Our collaboration with this initiative enables us to provide signals that can be used by global counterparties to support a greater understanding of how and where scams are taking place. The end goal is to enable faster identification and disruption of fraudulent activities across various sectors, platforms, and services, all over the globe.

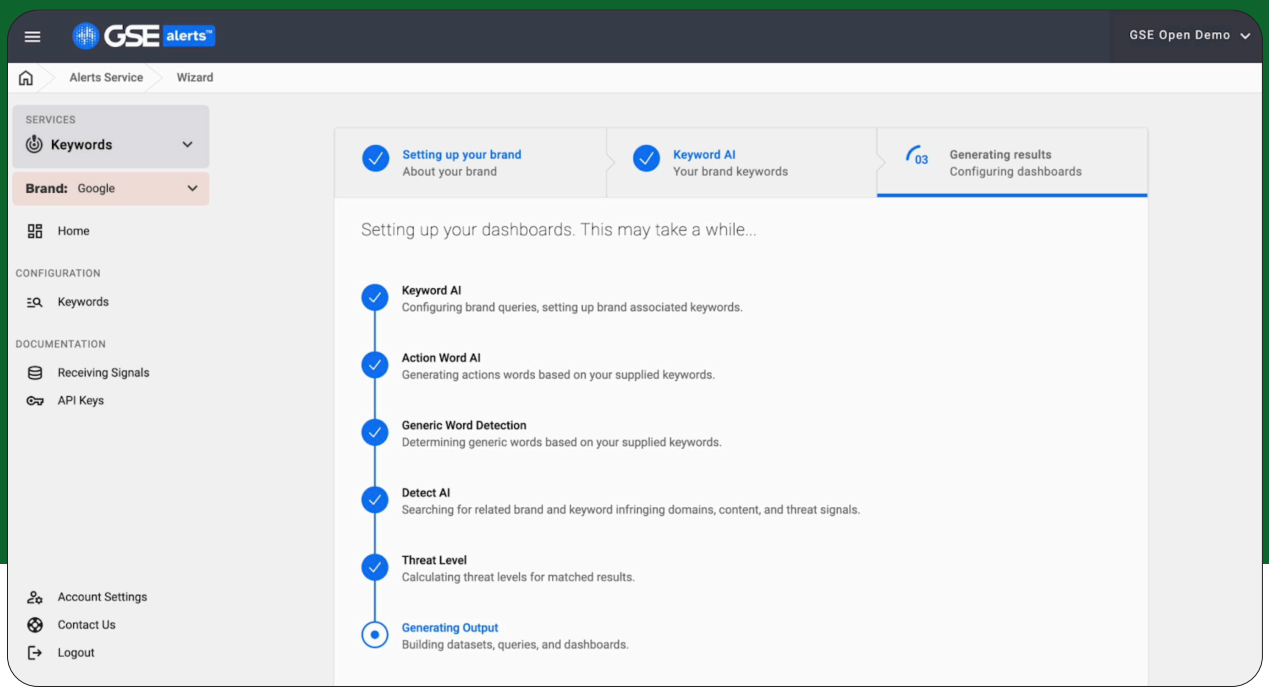
Using AI to enhance the Global Signal Exchange

The Global Signal Exchange (GSE) runs on Google Cloud, and is powered by the latest available AI models that enable real-time analysis of vast amounts of data. These models allow for the rapid identification of patterns and anomalies that may indicate clusters of fraudulent activity. The GSE platform is also evolving to utilize machine learning algorithms to continuously improve its ability to detect and predict new and evolving scam campaigns.

Cluster analysis

Across the entire GSE platform there are now over 200 million signals (as of May 2025) shared among partners, with an average monthly growth of 40 million signals. These signals encompass URLs, domains, and IP addresses affiliated with malicious entities, with plans to incorporate additional signal types, such as cryptocurrency wallets and telephone numbers, in the near future.

Cluster analysis aims to uncover hidden correlations and recurring patterns within the data, specifically focusing on identifying trends related to brands and sectors that are being targeted. By employing machine learning platforms available on Google Cloud and matching algorithms, the team can process large volumes of information to discern subtle indicators and characteristics associated with these targeted entities. Going forward, this proactive approach will allow the GSE team and partners to gain valuable insights into potential scams and to understand the methodologies employed by malicious actors.



Keyword AI

The Keyword AI functionality within GSE, as shown in the image above, utilizes Gemini to drive efficiencies in identifying threat levels for specific keywords related to a brand. Firstly, an organization sets up its brand in the system, for example, Google. Keyword AI then produces pertinent brand-related keywords, such as “Google Shopping” or “Google Maps”. Keyword AI is then able to employ these brand keywords to derive action words and initiate searches for potential matching threat indicators, content, and domains within the GSE’s signal streams. The resulting outputs consist of datasets, queries, and dashboards that enable a company to assess the threat level associated with each brand-specific keyword.

> “Utilizing Google Gemini’s capabilities via the Google Cloud Platform has transformed the breadth and depth of cluster analysis we are able to undertake, as well as enabling us to create additional features like Keyword AI, which can generate a vast amount of new signals for the exchange. Together these new AI-enabled features enable brands to identify and prioritize threat scenarios and uncover which parts of the brand or business the scammers are targeting.”
>
> **Lucien Taylor, Co-Founder, Global Signal Exchange**

Conclusion

As AI continues to evolve, we expect it to play an increasingly important role in safeguarding users and platforms from fraudulent activities. AI-powered enhancements, such as Keyword AI (built with Google Gemini) and cluster analysis machine learning models are transforming capabilities, notably as part of the Global Signal Exchange's mission, allowing for deeper insights into scam tactics and targeted brand threats.

The Global Signal Exchange is a testament to the power of collaboration and innovation in the fight against scams. While we do not expect our efforts to eradicate the problem of scams entirely, creating initiatives such as these can help meaningfully impact the scale of this problem affecting our users worldwide.

Key takeaways

212M
signals on the Global Signal Exchange

16M
Global Signal Exchange
signals ingested by Google

7M
signals shared by Google with the Global Signal Exchange

$1 trillion
annual losses from scams
estimated in 2024

40M
signals added to the Global Signal Exchange every month on average

Global Signal Exchange data as of initial launch on January 1, 2025 to May 15, 2025