Fighting Scams on Search

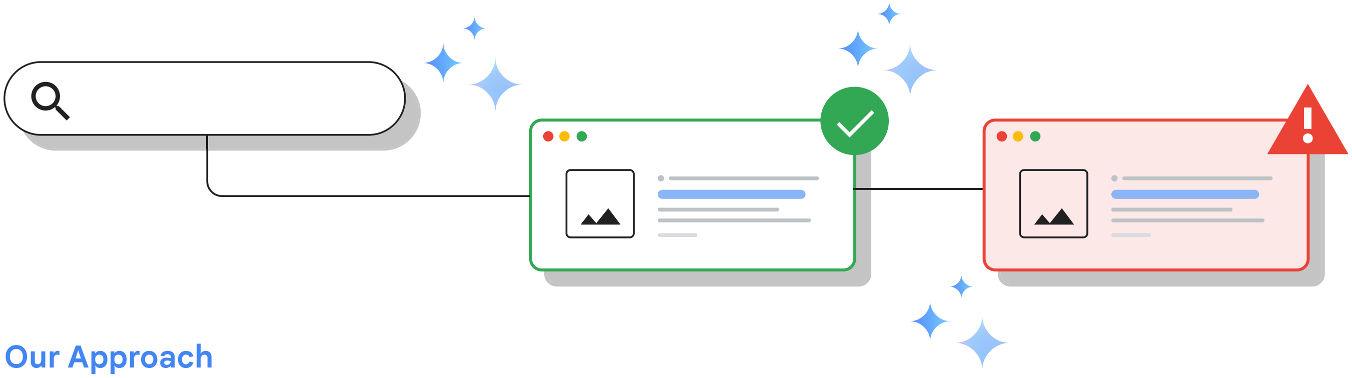
How we're leveraging AI to keep scams out of your search results.

When you come to Search, you trust that Google will provide you with relevant, helpful, and safe results. That's why Search builds the most advanced scam-fighting technology to combat the ever-present concern of scammy pages on the web.

While the sophistication of online scams continues to rise, our safeguards keep the overwhelming majority of these scams out of Search, blocking billions of potentially scammy results every day.

With bad actors constantly adapting and evolving, we're continually investing in novel scam-fighting approaches to stay a step ahead of the latest threats, keeping you safe while you search.

Here's an update on our recent work to leverage AI to fight scams in Search.



Our Approach

Our classifiers utilize machine learning algorithms to identify patterns, anomalies, and linguistic cues indicative of fraudulent activity. However, the tactics employed by scammers are constantly shifting and evolving. Staying one step ahead of the scammers requires that we understand emerging threats and proactively develop countermeasures.

Over the last three years, we've launched new AI-powered versions of our anti-scam systems, including updates in 2024 which vastly improved our defenses against scammy results. These advancements with AI and large-language models have enhanced our scam-fighting capabilities, enabling us to analyze vast quantities of text and identify subtle linguistic patterns and thematic connections that might indicate coordinated scam campaigns or emerging fraudulent narratives.

For example, our systems are able to identify interconnected networks of deceptive websites that might appear legitimate in isolation. This deeper understanding of the nuances and trends within the scam ecosystem allows for the development of more targeted and effective detection mechanisms, providing a crucial edge in this ongoing battle.

Large language models have also helped us to scale our protections across languages to protect more people around the world. We know that scammers operate around the world and in every language - so it's important that we have protections in place for people using search no matter the language they're using. Whether we identify a scam in English, Hindi, German, Spanish, or another language, LLMs have allowed us to train our systems to catch those scams in multiple other languages as well thus limiting user exposure to scams globally.

By The Numbers

- Throughout 2024, we implemented multiple significant updates to our scam detection systems. As a result of these ongoing efforts, we currently prevent hundreds of millions of harmful and scam-related results from reaching our users every single day. This daily intervention acts as a critical shield, protecting countless individuals from potential harm.

- Over the past three years, we've significantly enhanced our existing classification systems and developed entirely new solutions to identify and neutralize scams utilizing LLMs. By integrating advanced AI models, including LLMs, we've achieved exponential growth in our scam detection capabilities – enabling us to catch 20x more scammy pages before they reach Search.

- A crucial aspect of our strategy involves identifying emerging scam trends and quickly deploying countermeasures.

    - For example, after observing a notable increase in scam activity targeting airline-related customer service queries, we swiftly implemented dedicated protections that resulted in a decrease of more than 80% in scam attacks on airline-related searches.

    - We also observed a rise in misleading pages mimicking official resources (like visas or other government services). In 2024, new protections decreased scams impersonating official sites by more than 70%.

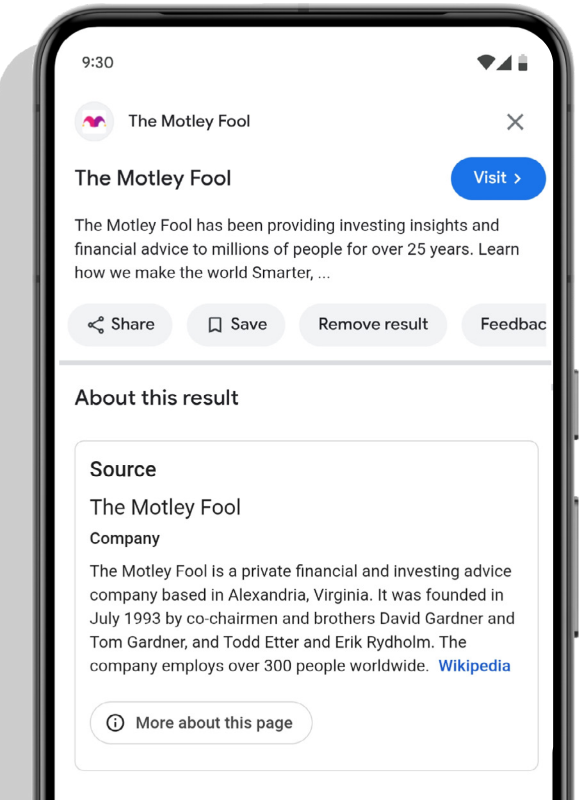
Spotting Scams

While our advanced systems work around the clock to keep Search 99% spam-free, vigilance remains a crucial element of online safety. Here are some practical steps you can take to protect yourself from scams across the web:

- Check for lookalike domains. Bad actors often use similar-seeming domains to trick people. For example, instead of the domain @thisisgoodlink.com a bad actor may use "@thisisagoodlink.support".

- Gather insights about the webpage, store or business. One way to get more information about an online source is with About this result (the three dots next to a search result), which lets you learn more about sources like an online store before clicking into its page.

- Look for official resources and be wary of unusual formatting. Our Search systems are designed to surface high quality, reliable information. When it comes to something like a customer service number, there's really only one "official" source of that information. Not all businesses have customer service numbers, so if you can't find one on their website, be mindful before you go digging to find one from another site or service. Beware of strange formatting, unusual fonts, or unexpected symbols or emojis, which could indicate a spoof site.



9:30

The Motley Fool

The Motley Fool

The Motley Fool has been providing investing insights and financial advice to millions of people for over 25 years. Learn how we make the world Smarter, ...

About this result

Source

The Motley Fool

Company

The Motley Fool is a private financial and investing advice company based in Alexandria, Virginia. It was founded in July 1993 by co-chairmen and brothers David Gardner and Tom Gardner, and Todd Etter and Erik Rydholm. The company employs over 300 people worldwide. Wikipedia