Website Scam Risk Detector

What It Does

This intelligent workflow simplifies the complex task of determining whether a website is legitimate or potentially a scam. By simply submitting a URL through a form, the system initiates a multi-agent evaluation process. Four dedicated AI agents—each powered by GPT-4o and connected to SerpAPI—analyze different dimensions of the website: domain and technical details, search engine signals, product and pricing patterns, and on-site content analysis. Their findings are then passed to a fifth AI agent, the Analyzer, powered by GPT-4o mini, which consolidates the data, scores the site on a scale of 1–10 for scam likelihood, and presents the findings in a clear, structured format for the user.

Who It's For

This workflow is ideal for anyone who needs to quickly and reliably assess the trustworthiness of a website. Whether you're a consumer double-checking a store before making a purchase, a small business owner validating supplier sites, a cybersecurity analyst conducting threat assessments, or a developer building fraud detection into your platform — this tool offers fast, AI-powered insights without the need for manual research or technical expertise. It's designed for both individuals and teams who value accurate, scalable scam detection.

How It Works

The process begins with a simple form submission where the user enters the URL of the website they want to investigate. Once submitted, the workflow activates four specialized AI agents—each powered by GPT-4o and connected to SerpAPI—to independently analyze the site from different angles:

Agent 1 examines domain age, SSL certificates, and TLD trustworthiness.

Agent 2 reviews search engine results, forum mentions, and public scam reports.

Agent 3 analyzes product pricing patterns and brand authenticity.

Agent 4 assesses on-site content quality, grammar, legitimacy of claims, and presence of business info.

Each agent returns its findings, which are then aggregated and passed to a fifth AI agent—the Analyzer. This final agent, powered by GPT-4o mini, evaluates all the input, assigns a scam likelihood score from 1 to 10, and compiles a neatly formatted summary with organized insights and a disclaimer for context.

Set UP

You will need to obtain an Open AI API key from platform.openai.com/api-keys
After you obtain this Open AI API key you will need to connect it to the Open AI Chat Model for all of the Tools agents (Analyzer, Domain & Technical Details, Search Engine Signals, Product & Pricing Patterns, and Content Analysis Tools Agents).
You will now need to fund your Open AI account. GPT 4o costs ~$0.01 to run the workflow.
Next you will need to create a SerpAPI account at https://serpapi.com/users/sign_up
After you create an account you will need to obtain a SerpAPI key.
You will then need to use this key to connect to the SerpAPI tool for each of the tools agents (Domain & Technical Details, Search Engine Signals, Product & Pricing Patterns, and Content Analysis Tools Agents)
Tip: SerpAPI will allow you to run 100 free searches each month. This workflow uses ~5-15 SerpAPI searches per run. If you would like to utilize the workflow more than that each month, create multiple SerpAPI accounts and have an API key for each account. When you utilize all 100 free searches for an account, switch to the API key for another account within the workflow.

Disclaimer

This tool is designed to assist in evaluating the potential risk of websites using AI-generated insights. The scam likelihood score and analysis provided are based on publicly available information and should not be considered a definitive or authoritative assessment. This tool does not guarantee the accuracy, safety, or legitimacy of any website. Users should perform their own due diligence and use independent judgment before engaging with any site.