Things to know before installing AI browser

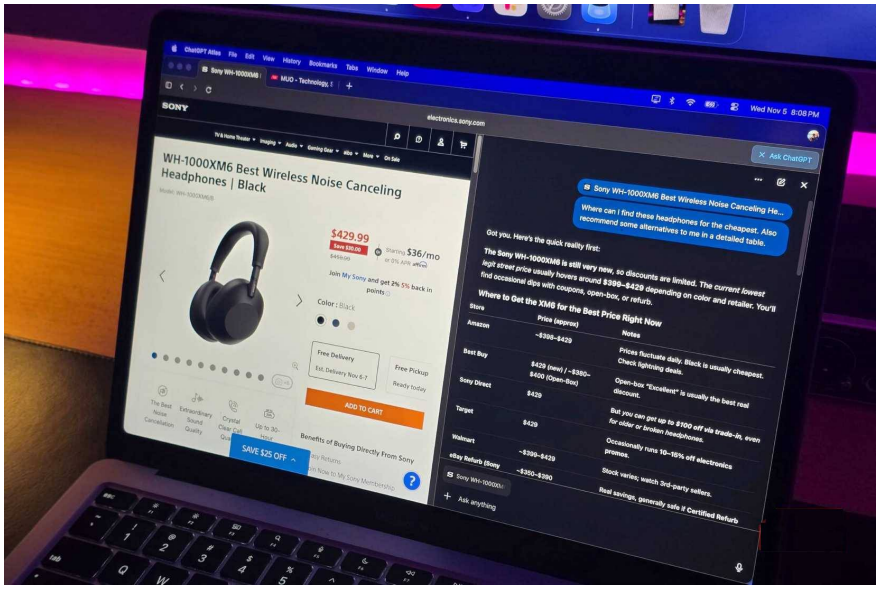
Competition is always good, especially in a field that has become a near-monopoly, but honestly, these new AI browsers aren't perfect.

The recent LLM hype has created a new trend in the browser world. Everyone suddenly wants to create an 'AI browser,' and even big names like OpenAI and Perplexity are now trying to compete with the giant Google Chrome . Competition is always good, especially in a field that has become a near-monopoly, but honestly, these new AI browsers are not perfect.

Here are some things to know before installing the AI ??browser!

Most AI agents are vulnerable to attacks using malicious prompts.

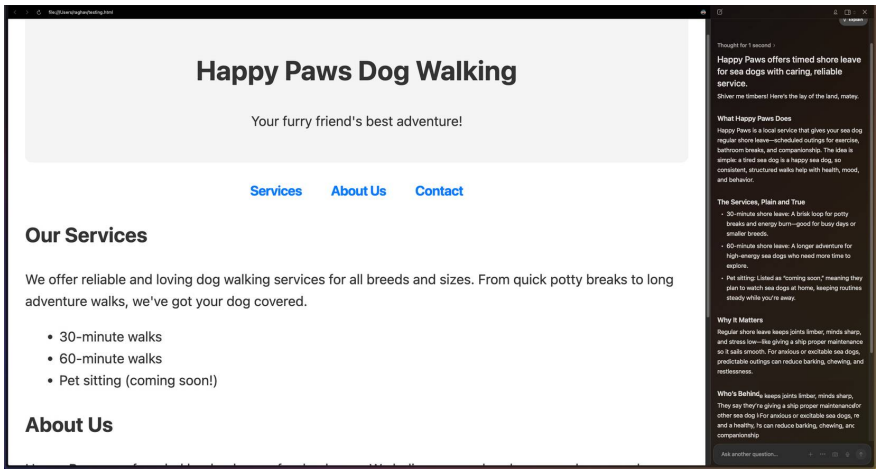
Ironically, Gemini created such an attack



A malicious prompt attack is when a website inserts its own hidden commands and the AI ??follows those commands instead of what the user actually asked it to do. Nothing is being hacked. The AI ??simply reads everything on the page, including text you can't see, and treats it as part of a conversation.

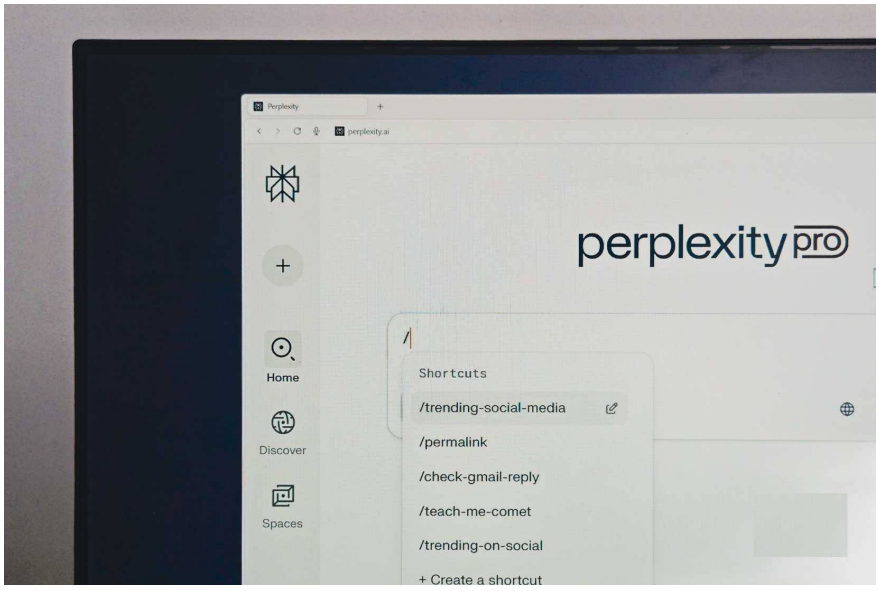
This becomes a real problem in AI browsers because the agent is trying to understand the entire page at once. If a website hides a line of text, the AI ??can still read it and might think it's a real command. That's how a website can tell the agent to ignore your request or generate something you didn't intend.

Even OpenAI says its new ChatGPT Atlas browser is still vulnerable to malicious prompt attacks, so while the idea sounds very sophisticated, you'd be shocked at how easy it is to create a similar attack yourself.



You are not the user, you are the product

You are building the next model.



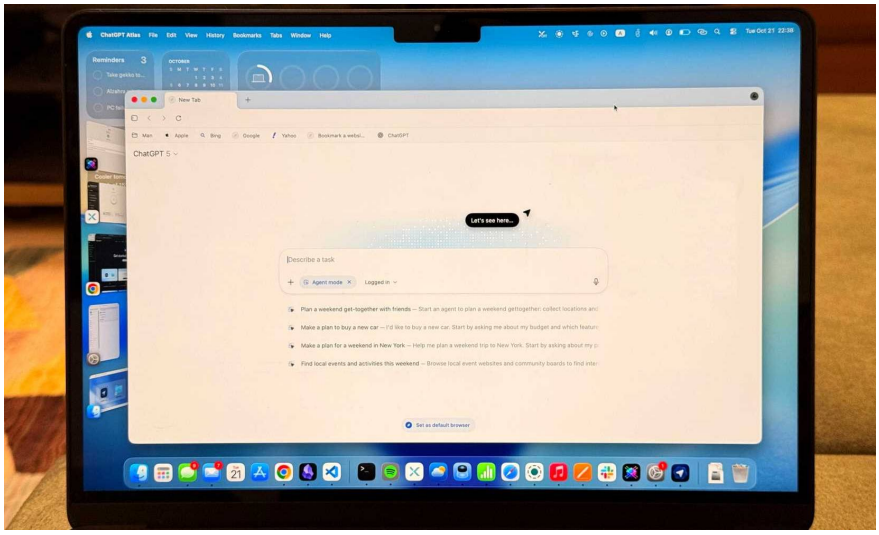
For years, Google has been a company that builds detailed profiles of its users. It started with Google Search, where everything you search for helps Google understand which ads to show you. Over time, this expanded to other services like Maps and YouTube , adding even more data about your habits, location, and interests.

But with LLM , the situation is very different. Most people don't realize how much they're giving up when talking to AI. Unlike traditional search, users tend to get much more personalized with large language models because the interaction feels more like a conversation. Many have even seen people try to treat ChatGPT like a therapist.

The problem is that your conversations don't just sit there unused. In many cases, the data you provide is used to train or improve future models.

Most AI agents don't actually solve the problem.

Do you want to take a risk with your agent?



If you're not familiar with how these AI agents work , they're supposed to automatically handle actions for you based on prompts. In theory, this should save time. But in practice, it rarely happens. When I tried the new ChatGPT Atlas browser, Agent Mode was pretty much useless.

It will create phantom actions, randomly summarize text you never asked for, or completely ignore basic things like scrolling. What's more, it's so slow that you can complete tasks yourself in a third of the time. Instead of helping, it hinders.

But the bigger issue is actually security. These agents are also vulnerable to rapid injection attacks, as the article mentioned earlier, and the consequences could be much worse. AI browsers can actually be fooled by scams like phishing emails, which, for lack of a better term, fail miserably.

If agent operations are one of the main advantages of these browsers and put you at as great a risk as they are now, then what is the point of using them?

You can get almost all the same features with extensions

It's all Chromium after all

Let's take a quick look at the most popular AI browsers today and see how similar they are. Perplexity Comet , ChatGPT Atlas, and Dia all follow the same formula. They invoke LLM when a question is too broad or vague for a regular Google search. They add an AI sidebar that reads the page you're viewing and answers your questions. And they include a basic set of agent features that try to automate everything for you.

If you look closely, none of these features are exclusive to these browsers. You can recreate almost all of the functionality of a regular Chromium browser with just a few extensions. These browsers are not groundbreaking in bringing AI into your workflow. The real intelligence comes from the cloud, not the browser itself, so the browser essentially acts as a front-end to the model.