

What are AI shopping agents, and are they safe to use?

As agentic commerce agents become an increasingly common way to shop, learn the risks that may come with them, and some ways to use them more safely.

7 min read

AMP Editorial Team

Published

06/10/2026



Key takeaways

1. AI shopping agents can research products, compare options, and, in some cases, make purchases on your behalf.
2. As AI shopping grows, scammers may look for new ways to exploit it. This might look like fake websites, false reviews or misleading products, which are designed to trick your AI agent into being scammed.

3. AI shopping agents may introduce new cybersecurity risks, particularly when they have access to personal information, payment details or permission to make purchases on your behalf.
4. Verifying your AI agent's permission settings, and doing your own check on a retailer, could help protect you against these attacks.

AI shopping agents can compare prices, products and retailers in seconds – but can they spot a scam? From stores to screens, shopping is always taking new forms. And in recent years shopping has changed faster than ever before, with the rise of AI, and now, AI shopping agents.

AI shopping agents are AI systems designed specifically to assist customers with the shopping journey, by researching, anticipating customer needs, and, increasingly, purchasing on customers behalf – sometimes without direct human oversight.

There's a lot to like about technology making shopping quicker, especially if the weekly grocery run isn't your favourite chore. But as these AI shopping agents increasingly become available in Australia, it's also worth understanding the potential risks.

These may include weaker safety measures, the misuse of personal data and new opportunities for cybercriminals and scammers to abuse your financial information.

For example, an AI shopping agent could be tricked by a misleading website, compromised in a way that could lead to sharing your personal or payment details to cybercriminals, or could simply make a purchase you didn't want.

What are AI shopping agents?

AI shopping agents, also known as agentic commerce agents, are similar to AI chatbots you may already know, such as ChatGPT or Claude. Unlike a chatbot that mainly responds to individual prompts, an AI shopping agent can work through a specific shopping task with greater accuracy and independence, sometimes using other AI or systems in the background.

For example, you might tell an AI shopping agent, "I need a new blue shirt." The agent could then search for suitable options, compare prices and product details, and recommend a shirt that matches your request.

Depending on the permissions you have given it, the agent might then add the shirt to your cart or complete the full purchase process on your behalf. Tools with these capabilities were recently rolled out on the international stage, such as Copilot Checkout and Google's agentic shopping features, where these software updates allow users to search for and purchase products within the AI systems original "chat" dashboards.

As these tools become available in Australia, understanding how they work and the risks involved with using them, could help you shop more safely.

How can AI shopping agents be scammed?

AI shopping agents are still emerging, so the rules, safeguards and security practices around them are continuing to develop. As with any new technology, it's useful to understand where things can go wrong.

That doesn't mean AI shopping agents are unsafe by default. The concern is that scammers may try to influence the information these tools rely on, such as websites, product listings, reviews and search results.

For instance, if you ask an agent to find a blue shirt, it is likely to compare product pages, prices, reviews, and retailer details before making a recommendation. A scammer could try to shape those results by creating a website or listing that appears credible, uses convincing product information, or has fake positive reviews, which are intentionally appealing to AI systems.

If the agent relies on that information, it may recommend a poor-quality product, direct you to an unreliable retailer, or take you through a scam checkout process that could collect your financial data. This is why it's worth keeping some level of oversight, especially before payment details are shared, or a purchase is completed.

There are signs that interest in AI agents is growing quickly, including in online spaces linked to cybercrime. A six-month study found dark web community posts in underground channels mentioned "AI Agent" at a 450% increased rate to the previous six-month period, according to Visa's Payment Ecosystem Risk and Control (PERC), [2025 research](#).



Our security never stands still

[Because scammers are always changing tactics, we keep learning and adapting, watching for suspicious activity, sending instant alerts and using smart fraud detection to help keep your money safe with 24/7 monitoring. Our security never stands still. It works quietly in the background while you get on with living. Visit our scams hub for more ways to protect yourself.](#)

Outside of scams, do AI shopping agents pose other risks?

Scams are only one part of the picture.

An AI shopping agent may need access to personal details, delivery information, or a payment method to complete a purchase.

But before granting that access, it's worth considering your cyber hygiene and the security measures linked to the account you're setting up.

It can be helpful to look at what information the tool asks for, how it may be used and stored, and whether you can limit what the agent is allowed to do, specific to each task.

You might want to consider the data sharing and storing capabilities of each model, and whether you're comfortable letting the systems store your financial and personal information for extended periods of time.

Returns and refunds may also be less straightforward if an agent chooses the wrong item, buys something unexpected, or uses a retailer with unclear policies.

Before using a shopping agent, review the retailer's terms, return policy and contact details, and keep a record of the request you gave your agent, recommendation the agent reported back to you and a record of the transaction confirmation, in case you need to dispute something with a retailer in the future.

This is important because if an agent makes a mistake, such as buying more items than you intended, it may not always be clear who is responsible for resolving the issue. In the event of a refund being needed, some retailers might argue you are responsible as you initially prompted the agent, so having evidence that your agent acted incorrectly or without cause may improve your chances of receiving a refund.

However, Australian consumer law does not yet include specific provisions for AI shopping agents or agentic commerce. Previous Australian Competition and Consumer Commission guidance indicates that businesses are considered responsible for the conduct of AI systems it uses, and so the same considerations could apply to individuals AI agent's conduct, meaning you could be considered responsible for your agents purchases, even if it has operated without authorisation.

Yet, these principles have not yet been applied to individual use cases, and regulators and industry bodies are still working through questions of liability and responsibility in regard to this new technology.

Checks to consider before using an AI shopping agent

- **Review permissions.** Check whether the agent can browse, add items to a cart or complete a payment without your oversight, and consider what level of access you'd like to give it.
- **Use transaction approval** where available. Requiring a final human review before purchase may help you confirm the item, seller, price, delivery details and payment amount. You might be able to spot something a machine misses.
- **Check the retailer independently.** Look at the website address, contact information, return policy and product details rather than relying only on the agent's recommendation.

- **Be cautious** with reviews and urgent offers. A high rating, limited-time message or prominent search position does not necessarily mean the site is trustworthy.
- **Monitor payment activity.** Check transaction notifications and account activity regularly so you can identify a purchase you do not recognise. Ensure to keep monitoring after a transaction has closed, as cybercrime transactions do not always occur immediately after your information has been compromised.
- **Keep records** of the prompts you give an AI agent. Save the request and the AI's recommendation, receipt and relevant retailer information. This could be helpful if you need a refund, though this isn't guaranteed to work.

What to remember

AI shopping agents can save you time by researching products, comparing options and helping you make a final shopping decision.

However, as with any shopping experience, it's important to stay aware and remain in control.

While the technology may be new, the principles of safe and confident shopping haven't changed.

The same common sense and judgement you've always used when shopping, will continue to help you navigate AI shopping tools with confidence.