PRESS RELEASE

Brittany Posey
Gen
Brittany.Posey@gendigital.com

Ashley Cirovski
humann. Communications
Ashley.Cirovski@humanncomms.com

Australians lose $1,327 on average to holiday shopping scams as blocked fake store attacks surge 155%*

11 November 2026 – Australians who lost money to holiday shopping scams were left $1,327 out of pocket on average, according to the 2026 Norton Insights Report: Holiday Scams, as new threat intelligence reveals a 155% increase in blocked e-shop scam attacks in Australia.

The report by Norton, a consumer Cyber Safety brand of Gen (NASDAQ: GEN), found that 13% of Australians have fallen victim to a scam while shopping online during the holiday season. Of those victims, 94% lost money, with the highest reported being $30,000.

Yet despite 45% of Australians saying they are more concerned about online scams this holiday season than last year, and more than a quarter (27%) admit they've purchased from a website or seller they suspected might be a scam because the deal was too good to pass up.

The findings come as threat intelligence from Genreveals its security products blocked more than 2.25 million e-shop scam attacks in Australia during the holiday shopping period in October – December 2025, up 155% from over 883,000 in 2024. The number of users protected also more than doubled to 739,000, while blocked domains increased 101% to roughly 54,000.

Key findings from the 2026 Norton Insights Report

Holiday shopping scams

- 36% of Australians have encountered a suspicious website or seller when trying to purchase trending items such as Labubu, Jellycat or Stanley Cups.
- 42% of holiday shopping scam victims reported being scammed through social media, followed by email (38%) and scam advertisements (38%).
- 30% say they tend to take more risks when shopping online during the holiday season than at other times of the year.

AI shopping assistants and emerging risks

- 59% of Australians have used an AI shopping assistant or agent, while 42% plan to use AI to help with holiday shopping this year.
- 62% are concerned about AI shopping scams.
- 57% of Australians who have used an AI shopping assistant or agent say one recommended or completed a purchase from an unfamiliar retailer during the most recent holiday shopping season.
- Only 46% of Australians who would use an AI shopping assistant to shop are confident it could recognise and avoid a fraudulent website.

Why holiday shopping scams are catching Australians out

Dean Williams, Principal Systems Engineer at Norton, said the combination of seasonal discounts, high-demand gifts and increasingly convincing fraudulent websites creates opportunities for scammers.

"Scammers know people are hunting for the best deals, particularly around major shopping events like Black Friday and Cyber Monday. They can create convincing online stores, use familiar branding and advertise heavily discounted products to make fraudulent offers appear legitimate.

"What's concerning is that some shoppers are prepared to take a chance even when they suspect something isn't right. Scammers can exploit that urgency to grab a bargain before it's gone, but a heavily discounted product isn't worth risking your money or personal information."

Why fake online stores are becoming harder to spot

Williams said shoppers should be particularly cautious when following advertisements to unfamiliar retailers.

"Fake shopping websites can look almost identical to legitimate retailers, complete with professional product images, customer reviews and convincing checkout pages. AI tools can also make it easier for scammers to produce realistic content at scale.

"Shoppers shouldn't rely on how professional a website looks. If you're clicking through from a social media advertisement or buying from an unfamiliar retailer, check the website address, look for independent reviews and make sure the business is legitimate before entering your payment details."

AI shopping assistants: convenience doesn't guarantee safety

Williams said that while AI shopping assistants can make finding gifts and comparing prices easier, consumers shouldn't assume the technology can reliably identify fraudulent retailers.

"AI shopping assistants are changing how people discover products and make purchases, but a recommendation from an AI tool isn't a guarantee that a retailer is legitimate.

"The risk becomes greater when shoppers rely on an AI agent to do more than recommend a product. If you're allowing a tool to navigate websites or complete purchases on your behalf, it's important to understand what information it can access and check where your money is going. AI can help you find a bargain, but it shouldn't replace your own judgement about whether a seller can be trusted."

How to avoid holiday shopping scams

1. **Check the website before you buy.** Look for misspelled URLs, search the store name with “scam” or “reviews,” and use a tool like Norton Safe Web to flag malicious sites.
2. **Skip the ad and go straight to the retailer.** Type the store’s address into your browser or open its official app instead of clicking a social ad.

3. **Use AI-powered scam protection.** Norton 360 Deluxe helps spot scam links, fake websites and malicious downloads before they do damage.
4. **Double-check what AI recommends.** Vet any retailer an AI assistant suggests before you confirm a purchase.
5. **Pay with protection.** Use a credit card or a payment service with buyer protection. Avoid sellers who ask for bank transfers, gift cards or cryptocurrency.
6. **Track packages at the source.** Check delivery status in the retailer's or carrier's app, not through links in texts or emails.

The full 2026 Norton Insights Report: Holiday Scams is available at https://au.norton.com/blog/research/holiday-scams-insights-report-2026

Methodology
The survey was conducted online by Dynata in Australia from September 10, 2026 to September 23, 2026, among 1,000 adults ages 18 and older. Data are weighted by age, gender, and region to be nationally representative.
*YoY increase in Q4 2025 compared to Q4 2024

About Norton, part of Gen
Norton is a leader in Cyber Safety and empowers millions of individuals and families with award-winning protection for their devices, online privacy, and identity. Norton is part of Gen (NASDAQ: GEN), a global company dedicated to powering Digital Freedom with a family of trusted consumer brands that help people protect and take control of their digital and financial lives. As AI reshapes how people discover, decide and transact, Gen is building the security and trust layer to empower people and their agents to navigate digital life more safely. Gen empowers nearly 500 million users in more than 150 countries through its products and services that span cybersecurity, online privacy, identity protection and financial wellness. Learn more at Norton.com and GenDigital.com.