McAfee: Holiday shopping scam victimisation nearly doubles in US survey



A McAfee survey of Americans finds 42% report falling for a holiday shopping scam, up from 22% in 2025, while confidence in spotting scams has fallen. The results offer awareness lessons for institutions in the Kingdom.

- 42% of surveyed Americans say they fell for a holiday shopping scam, up from 22% last year.
- Confidence in recognising online scams fell from 90% to 75%.
- Gift cards, prizes, delivery problems and limited-time deals were the most common lures; Amazon (40%) and Temu (33%) were the brands most often impersonated.
- Of those who lost money, 60% lost $100 or more and 48% recovered nothing.
- The year-on-year comparison uses different surveys and providers, and McAfee said final methodology and rankings were still pending.

McAfee has published research on holiday shopping scams based on a survey of Americans. Forty-two percent of respondents say they have fallen for one, compared with 22% in 2025. The comparison draws on separate surveys with different providers and sample sizes, and McAfee noted that the final methodology and product rankings were pending confirmation, so the figures are best read as indicative.

What the research found

Confidence is falling: 75% of respondents say they can recognise an online scam, down from 90% a year earlier. Most said AI-generated scams can look convincing and expressed more concern about them than before. Gift card and prize offers were the most reported suspicious messages, followed by package delivery problems and limited-time deals. Amazon and Temu were the brands respondents most often saw impersonated.

McAfee also linked 12 popular gifts to suspicious website activity after searches. The findings concern suspicious sites, not the legitimate brands or retailers.

Behaviour and impact

Sixty-eight percent reported at least one risky shopping behaviour to get a better price, such as buying from unfamiliar sellers or sharing personal data to claim a discount. An unusually low price was the warning sign most often ignored. Among those who lost money, 60% lost $100 or more and 48% recovered none. Some cut back on essentials or borrowed to cover the loss.

Relevance for institutions

The survey covers US consumers, but the lure patterns, such as brand impersonation, delivery notices and discount offers, are familiar to any organisation whose staff and customers shop online during seasonal sales. Brief, timely awareness messaging is a practical response.

What to do now

1. Send staff a short awareness note before major sales seasons covering fake deals, delivery notices and gift card or prize offers.
2. Remind employees to verify retailers and type known addresses instead of following links in unsolicited messages.
3. Advise customers through official channels on how your institution contacts them and that it never requests credentials by message.
4. Make sure staff know how to report suspected phishing quickly, and review those reports for seasonal patterns.
5. Include AI-generated lures in phishing simulations and training content.