By MAE ANDERSON

THE knitwear store appears to be a small family-run business. The sweaters on its website feature a photo of a woman hand-knitting a Christmas design. The caption says that after decades of creating knitwear that tells "quiet stories of care and beauty", she is closing her little studio and the pieces on offer are her last.

The website of another boutique also spotlights a charming backstory. The "About Us" section states that twin sisters run the shop their mother opened in 1972 and share her commitment to a a business "rooted in family, community and women uplifting women". Shoppers could take advantage of a sale honouring the boutique's late founder on what would have been her 95th birthday.

But neither store is what it appears. Both display many of the same Icelandic, Nordic and festive sweaters with identical stock images. Their website domains were registered in China in November, ahead of the holiday shopping season. Negative reviews of both proliferate on consumer review websites such as Trustpilot, where users report receiving shoddy goods that were difficult to return.

The knitwear store did not return a request for more information about the owners. A close look at a pop-up ad describing Nola Rene, the 72-year-old Swedish knitter who is supposedly hanging up her knitting needles, reveals the word "advertorial" at the top and at the bottom, a disclaimer saying the people in the photos are models. At least three other shopping sites also sell the sweaters "lovingly hand-knitted in small batches".

The boutique responded to an email query about where it was based and who owned the business by saying it was an online boutique "working with trusted global fulfillment partners to serve our customers".

Online shopping scams are not unusual. About 36% of Americans failed to receive refunds after purchasing an item online that they said never arrived or turned out to be counterfeit, according to a Pew Research Center survey conducted in April 2025 and published in July. Faster and more sophisticated digital tools are only making it even harder for consumers to spot if what they are seeing is too good to be true.

Some vendors and fraudsters have taken advantage of AI-generated images to create websites that have an aura of artisan authenticity or that point to a long history as a trusted small retailer, said Seth Ketron, a marketing professor at The University of St. Thomas in St. Paul, Minnesota.

"It's getting more and more common," Ketron said. "If you're not careful or you're really paying close attention, or you don't really even know what to look for or what AI photos look like, it's easy to kind of just gloss over or miss that it's probably not real."

Misleading e-commerce ads often pop up on social media feeds or appear as banners on other kinds of websites. Experts say there are some simple steps shoppers can take to distinguish a legitimate small merchant from a suspicious one before clicking "buy".

Check for verifiable details

Deanna Newman owns C'est La Vie, an online jewellery retailer in Ontario, Canada, and learned about mall-business impersonation scams the hard way. A person claiming to have received low-quality goods from her site left an irate comment on Newman's Facebook page. Alarmed, she looked but she could not find a record of the order.

Newman concluded a scammer was using the name of her store for several shopping sites selling jewellery. When people went online to complain about inferior products, they landed on her site. There were C'est La Vie websites claiming to have brick-and-mortar locations in New York, Birmingham, England, Dublin, Ireland, and other cities, which didn't actually exist.

"Sometimes people were receiving products from China and very low-grade jewellery, and then some people weren't receiving things at all," Newman said.

She dealt with the complaints, put a warning on her Facebook page and online shop about the misleading C'est la Vie websites, and posted videos on Instagram and TikTok to demonstrate she was a real person with a real business. Some of the copycat sites were taken down. But an influx of poor reviews and complaints nonetheless hurt her sales, she said.

Newman advises shoppers to look for a verifiable address or other details that may indicate a site is authentic. When in doubt, reach out to the owner by email, phone or contact form. If they are genuine, they should be happy to reply, she said.

"It's hard, because the consumer has to do a little bit of research on their side, but I would say, too, that if it looks too good to be true, it probably is," Newman said.

Beware a sob story

Including fake hardship stories along with ads is one technique online scammers use to draw in potential buyers. Common ploys include announcing a "going-out-of-business" sale or a sale to honour a late son, daughter or grandmother.

Newman said the people who assumed her company's name employed multiple versions of this gimmick, including having a close family member pass away. A customer who contacted Newman expressed sympathy for the loss of her son.

"I realised that they thought that I was the scam website," she said. "So I was like, 'Well, the good news is you haven't been scammed because I'm sending these products, but the bad news is, you purchased from me thinking you were supporting somebody who's going through something hard'."

Check third-party reviews

Murat Kantarcioglu, a computer science professor at Virginia Tech, recommends checking reviews before making any online purchases from smaller businesses. Customer reviews aren't always legitimate either, but they can be good to check as part of your research.

Sites like the Better Business Bureau and UK-based Trustpilot are two places to look, as well as marketplaces like Amazon and Etsy if the brand has a presence there.

"If the small business claims to be there for 30 years, they should have reviews about them, maybe from at least a couple of years back," Kantarcioglu said.

Look up the domain

Another quick check is looking up where a website was registered. Kantarcioglu recommends doing a domain name search through the nonprofit Internet Corporation for Assigned Names and Numbers. GoDaddy and Whois are other options.

If a company claims to be in one country but is registered in another one, that is a red flag. If the site was registered in the past few months but is marketed as belonging to an established small business, that's another.

Trust your gut

No matter how cautious you are, it is still possible to get scammed. If something seems off, it's better to hold off making a purchase than to make one you might regret, experts say.

"As (AI) gets better, then scammers or people doing dubious business practices are going to have an easier time duping people, because things are gonna look more and more convincing," Ketron said. – AP