Generative AI gives scammers new strength

Phony shops target your wallet!

Consumer watchdog groups are warning that scammers are using generative AI to create fraudulent shops and services online. AI product images and generated reviews create the illusion of a legitimate site. But when you try to make a purchase, your merchandise never arrives … and your payment information has been stolen.

Follow our tips to spot a phony site and save your money from scammers!

AI-generated product photos? Just say no!

AI is improving, but many scam sites use careless or low-quality fake pictures. Examine product photos closely and look for blurriness or an unnaturally smooth texture. If they can't show you the real product, then they don't have it.

Fresh sites could be fresh scams

Fake shopping sites rely on speed. Their scam won't stand up to close inspection, so the scammers create new sites constantly, rake in the money and then disappear. Check a site's domain history and publishing date. If it's brand new, it could be a trick.

Trend-chasing and unrealistic sales

Scammers want to make quick cash by leaning on the latest trends. Be wary of sites offering "the hot new thing" at impossible prices. At best, you'll receive a cheap counterfeit. At worst, your identity is now up for sale.

Fake reviews

Generative AI can create phony reviews for scammers to put on their site. Remember: even the best product can't please everyone. If a site has dozens of only five-star reviews, it's a scam.

How to check a website's publication date

- Use the Wayback Machine (web.archive.org) to see the site's history
- Google search with "inurl" (such as "inurl:wikipedia.org") and use the "More about this page" option to see when the site was first indexed
- Use Whois (whois.com) to find out when the domain was registered

Deepfake extortion

Scammers are using voice and image cloning to create deepfakes of real people. This information is often scraped from public social media sites. The deepfake can then be used to contact the real person's friends and relatives and ask for money. They often target senior citizens, who may not be aware of how the trick works.