



Bulletin - Scam Alert

Watch That Watch

Copycat websites mean that your designer purchase could be made in Mongolia

by: Sid Kirchheimer | from: AARP Bulletin | May 24, 2010

Debbie Hughes was doing some very early online Christmas shopping when she typed “Tiffany & Company” into the search bar.

“Up came a website called Tiffany & Company On Sale and I thought, wow!” says the 57-year-old Ohioan. “They were selling a sterling silver necklace and bracelet for \$228—what it usually costs for just the bracelet.”

But the website didn’t belong to the famous New York jeweler, despite looking quite a bit like the one that does. Its address—www.tiffanyco.mn—was a tweak of the real Tiffany website, www.tiffany.com, and the .mn meant it was registered as a Mongolian site.

And the discount designer jewelry that Hughes ordered? It did arrive—in a package with a Chinese postmark. “It was chrome-like junk,” she tells Scam Alert. But the gift box was a very clever copy of a Tiffany box.

It took Hughes, who operates a home-based business selling books and DVDs over the Internet, nearly four months to get a refund from her credit card company. The fake Tiffany company ignored her e-mails requesting a refund, and its website had no telephone number.

Popular brands make prime targets

The scam here is called “cybersquatting.” It occurs when a dishonest business steals or alters the website domain name of a well-known company and launches a copycat site to deceive online shoppers.

“There are many, many websites out there counterfeiting high-end, well-known brand names—Tiffany, Nike, Ray-Ban and others,” says Sue McConnell of the Better Business

Bureau in Cleveland, which investigated Hughes' case. "Anything that is popular and pricey is ripe for these counterfeiters, who lure you in with bargain prices.

"They often simply copy and steal pages from the real website and place them on their own," says McConnell. The merchandise, if it's delivered at all, is usually poorly made knockoffs.

The BBB has fought an uphill battle against these sites. "When you're dealing with scammers in foreign countries—as is the case with many cybersquatters—it's tough," says McConnell.

"You don't get a lot of cooperation from those governments or other authorities, who don't care [about protecting American customers]. And it's not as though a company in Mongolia is interested in resolving BBB consumer complaints."

How to recognize a counterfeit website

- Carefully read the address, or domain name, that appears in the line at the top of your browser. Beware of any website whose address has even the slightest change from the company's name. That includes extra words, such as TiffanyonSale or SterlingTiffany, says McConnell, or anything but the usual .com or .org ending.
- Call first. Some cybersquatting customer service telephone numbers are outright bogus; others connect to fax machines (so you can't reach a person). Avoid any website that has no posted phone number.
- Verify any brand-touting "bargain" website at the corporate headquarters of the real company. A phone call by the BBB to the authentic Tiffany & Co. revealed that it neither operates nor sanctions any sale or overstock websites. Also check with the BBB for past complaints about specific websites.
- Check the domain name registration. Websites such as WhoIs.net can reveal who owns a website's name. Avoid sites that shield that information behind a proxy registration service. Another red flag: a familiar American brand name being sold at an Internet address that ends with the ID letters of a foreign country—as did the fake Tiffany site. MN is the abbreviation for Mongolia.

Sid Kirchheimer is the author of *Scam-Proof Your Life*, published by AARP