

# THE TIMES

THE TIMES Saturday January 9 2010

65

[timesonline.co.uk/money](http://timesonline.co.uk/money)

## Money

Splitting up  
in an economic  
downturn

Divorce, pages 68-69



# Google failing consumers by profiting from scam websites

Shoppers must be sceptical of sponsored links on the search giant but there are ways to avoid falling victim, says **Lauren Thompson**

Internet shoppers have been told to be on their guard as scam websites are dominating the sponsored search results for many branded goods on the internet search giant Google.

Fraudsters, mostly based in China, are duping Britons into buying fake items such as Ugg boots and Links of London jewellery that appear as sponsored links on Google. In many cases the goods never arrive and customers' credit card details are put at risk.

Even the most internet-savvy shoppers can find it impossible to tell the difference between a fake and a legitimate site. Victims complain that they thought the websites were genuine because they had a commercial relationship with Google.

Professor Ross Anderson, an online security expert at the University of Cambridge, says: "If you click on an advert on Google, you are twice as likely to come to harm as if you click on the top three free search results. Internet shoppers need to be very wary and should always double-check that they are buying items from a legitimate site."

**'If you are unfamiliar with the site and feel uneasy, don't use it'**

A Google search for Links of London jewellery reveals at least four sponsored links for counterfeit sites. A search for another jeweller, Tiffany & Co, reveals the sponsored link [www.uk-tiffanyonline.com](http://www.uk-tiffanyonline.com), which claims to offer discounts of up to 85 per cent. The site looks almost exactly the same as the genuine site — [tiffany.com](http://tiffany.com) — and it will pay Google up to £5 every time a user clicks on the link.

Similarly, a Google search for Abercrombie & Fitch, the clothing retailer, shows that the first sponsored link, [www.abercrombieonlinestores.com](http://www.abercrombieonlinestores.com), is a fake site and has simply copied and pasted images from the genuine retailer, [abercrombie.com](http://abercrombie.com).

Although Google says that it will not knowingly advertise sites selling counterfeit goods, the search engine performs few diligence checks on websites, claiming that it cannot "regulate the internet".

Here, *Times Money* explains how to spot a fraudster and stay safe when shopping online.



**'The site looked totally genuine'**

### Case study

**W**endy Chambers, a student who lives in British Columbia, spent \$182 on what she thought was a pair of genuine Ugg Australia boots in November. The goods, bought from the Google-sponsored link [uggcanada.ca](http://uggcanada.ca), have still not arrived.

Ms Chambers, 37, originally from Cheshire, has since discovered from the genuine Ugg website, [uggaustralia.com](http://uggaustralia.com), that the site where she purchased her boots is a "known counterfeit website". "I was absolutely horrified that I might have handed over money to fraudsters," she says. "I am totally against counterfeiting because I know it can involve sweatshops and child labour. "I often buy online and the site looked totally genuine, and because I clicked through a Google-sponsored link I thought it was legitimate. It was also offering a discount, so I thought that I was getting a good deal."

Ms Chambers says: "I think it is outrageous that Google takes money from these sites. It needs to perform better checks on businesses before agreeing to give them sponsored links."

### Think before you click

The Google search words that are likely to produce untrustworthy sites include:

- Mobile phones and ringtones
- Ghd hair straighteners
- Ugg boots
- Tiffany & Co
- Links of London
- Nintendo DS Lite consoles
- Gucci handbag
- Abercrombie & Fitch
- Free music downloads
- Chanel perfume
- Diet pills
- Tagg watch
- Touche Eclat
- Vehicle parts

### How to avoid dodgy websites

There are several common signs that a website is fraudulent. It will usually offer "bargain prices" and display banners such as "Save up to 75 per cent" on the homepage — although some websites, particularly those that sell ghd hair straighteners, may offer only a small discount on the retail price. "Always remember the old adage: 'If it seems too good to be true, it probably is,'" says Jaclyn Clarabut, of *Which? Computing*. "If you are unfamiliar with the site and feel uneasy about anything, don't use it."

The genuine Ugg Australia and ghd websites — [uggaustralia.com](http://uggaustralia.com) and [ghdhair.com](http://ghdhair.com) — have a useful tool that allows you to type in a web address to check whether it is an authorised seller of their products. Generally, any website with a strange domain name — especially ones that include num-

bers or hyphens — should be treated with caution. If a website ends in .co.uk, it does not necessarily mean that the seller is based in the UK.

You can find out the registrant's details on any domain name that ends in .uk by using the Whois service at Nominet, the internet registry for .uk names — [www.nominet.org.uk/other/whois](http://www.nominet.org.uk/other/whois). For example, a search on Whois reveals that [linkscraft.co.uk](http://linkscraft.co.uk), which claims to be the "best Links of London online store" was actually registered on January 4, 2009, from an address in Nanjing, China.

For sites ending in .com or .org or .net, go to [www.who.is](http://www.who.is). A search of the genuine Links website, [linkslofondon.com](http://linkslofondon.com), reveals that the site has been registered since 2002 at an address in Surrey.

Keir McConomy, of [compare-ghd.com](http://compare-ghd.com), the comparison website, says:

"Although genuine retailers do ask Google to remove fake websites, the fake site simply reappears with a new name within hours, often with another Google-sponsored link so that it appears at the top of search results."

In 2006 Ben Edelman, an academic at Harvard University, conducted a study of the trustworthiness of sites with sponsored links at the five main search engines. He found that 5.93 per cent of Google's sponsored links were untrustworthy, rising to 6.01 per cent for MSN and 7.2 per cent for AOL. This percentage increased for particular key words — 23.5 per cent of results for "digital music", for example, were untrustworthy.

He concluded that search engine advertisements are "needlessly risky" and that consumers should simply click on the top free search result.

Continued on page 66

Media Outlet: *The Times*

Date: 9 January 2010

Circulation: 590,900

URL: [http://www.timesonline.co.uk/tol/money/consumer\\_affairs/article6980806.ece](http://www.timesonline.co.uk/tol/money/consumer_affairs/article6980806.ece)

## Links that lead to fraud

Continued from page 65

### Does it matter if goods are fake?

Some internet users may know that they are not dealing with a genuine website, but continue with their transaction in the hope that they will receive a good imitation product at a bargain price. This is a risky strategy.

"With many of these sites, you will be lucky if you ever receive any goods," says Mr McConomy.

"If they do turn up, electrical goods such as ghd hair straighteners or Nintendo DS Lite consoles are likely to be faulty and even pose a fire risk,

while counterfeit designer clothes or accessories may appear unconvincing and be made from cheap, synthetic materials." Also, those who buy from scam websites will have no means of redress, as the retailer will not have a refund policy or manufacturer's guarantee.

The biggest danger for consumers dealing with fake websites is the risk of credit or debit card fraud. Once your personal details have been handed over to complete a transaction, the fraudsters can use the information to drain your bank account by debiting more than was agreed.

It is also worth remembering the wider impact of fraudulent websites. Counterfeit clothing and footwear cost legitimate businesses £3.5 billion every year, according to the Alliance

Against IP Theft. A spokesman says: "The link between the trade in fake goods and other serious organised crime, such as people smuggling, hardcore pornography, drugs and the use of offensive weapons, is becoming increasingly clear."

### How to complain

There is little hope of redress if you have already fallen victim to a fake website. If the goods cost more than £100 and you bought them with a credit card, the card provider is jointly liable with the retailer, including for overseas purchases. You could, therefore, make a claim to your credit card provider, citing section 75 of the Consumer Credit Act.

If the site was a Google-sponsored link, you can complain and ask for the site to be removed by filling in an

online form at [adwords.google.com](http://adwords.google.com). Any search engine should investigate and take action if it becomes aware that an advertiser is disreputable.

However, this can take several weeks and the search engine will take no responsibility for any goods or services bought from other websites.

You can also write about your bad experiences with online retailers on consumer forums such as [moneysavingexpert.com](http://moneysavingexpert.com), warning other shoppers of the dangers of a particular site.

Consumer Direct, the Government-funded service, can offer specific advice. Call 08454 040506 or go to [consumerdirect.gov.uk](http://consumerdirect.gov.uk).

The service will also pass on your complaints to Trading Standards, although this body does not have the power to close down websites.