



Webbmedia Group, LLC

Can You Trust This Website?

Consumer technology has advanced so that anyone with a computer can now create sophisticated websites. It can be difficult, therefore, to determine if a website is trustworthy. Some people are now using websites as a way to subvert the truth, to defraud others of their money or to hide important public information.

There are many ways to determine whether or not to trust a website. Below is a standard list of questions to ask whenever you encounter a website that seems suspicious. But as a general rule, it's good practice to scrutinize many websites on a regular basis.

For Additional Information:

Webbmedia Group, LLC
2336 Cambridge Walk
Suite 400
Baltimore, MD 21224
tel: 267.342.4300
info@webbmediagroup.com
<http://www.webbmediagroup.com>

Tipsheet: Can You Trust This Website?

© 2008 Webbmedia Group, LLC

<http://www.webbmediagroup.com>



Webbmedia Group, LLC

Questions To Ask:

1. Does the website contain working contact information? A trustworthy website will make contact information very clear. It may be a web form rather than an email address, but you should receive some notice that your message has been received.

2. When you click on a link either on the site or from an email, does the URL change? For example, many bank scams will make it seem like you're clicking on www.citibank.com, but you'll be redirected to something totally different, such as www.monygr.ru/eirg/876632. The real Citibank webpages don't suddenly change like that. You can also look to see if there is an "@" within the URL. Hackers use an "@" within the URL to redirect users from one site to their hacked version.

3. Look at the source code information. This is found in different places, depending on your browser. In Firefox on a Mac, look at the very top bar, where it says Firefox, File, Edit. The next option is View. After clicking there, select Page Source. A new window will pop up with source code for the page. It is okay if you can't interpret the code...what you should look for is an indication that the site has been hacked. Almost always, if the site has been compromised or if it is a fake site, you'll see something at the top of the screen that says "Hacked by..." or "Down with Prime Minister..." etc.

4. Look up the domain. You can tell who has registered a website by going to <http://www.networksolutions.com/whois/index.jsp>. Simply follow the instructions and enter the domain without the "http" or "www," and you'll find out all of the names and contact information for that particular website. Note: there are instances when you may find that a site has been registered through a proxy to keep information private.

5. Look up old versions of the site. Using the Wayback Machine at <http://www.archive.org/index.php>, type in the URL to see older versions of the website. If the company or website claims to have been around for 10 years but the website was created 10 days ago, that may give you pause.

6. Use your instinct. Sometimes, the best way to determine whether a website is trustworthy is to use your own instinct. Does it *feel* right? Does it *seem* strange? If so, it probably is.