Ten Things to Check to See if a Website is Real

1. How does the website look and feel?
Does the website appear to have a professional look and layout? This is not a total red flag. Scam artists can afford professional designs, however, I have encountered quite a few websites that I have noticed a lot of unprofessional touches to them. Browse the website. How does it make you feel? Does it make you feel as secure as when you shop at a well-known retailer's website? Don't be in a rush to buy. Trust me, those "deals" are not going anywhere anytime soon. Take your time and browse the website. Check out the about section of the company. Does it have a history?

2. Are the listed in common databases?
Of course, check to see if the company is listed on RipOffReport.com. You might also want to check with your local Attorney General's Office (state listing here), and the FTC (Federal Trade Commission)

3. Check for proper contact information.
The power of the Internet allows anyone to become an instant merchant. The problem is that **anyone** can become a merchant, including scam artists. Scam artists can hide behind a professional-looking website and you never know who they are nor how to contact them.

Make sure they have a way for you to be able to contact them. Look for a phone number and an address. It is preferable to have a regular, non-toll free number. Toll free numbers can be a means for scam artists to hide behind services that might redirect their call to a distant location.

Next is the address. Some prefer a physical address over a post office box as one can hide behind a post office box address, however, the same can be said for a physical address. I use the FinAid! website to search for a potential mail drop. Never settle for a company that has only a contact form as their only means of communication.

Do they have an email address listed? It is highly recommended to stay away from any company that uses a free email service (Yahoo!, Hotmail, Gmail, etc) for their primary contact information. These services are fine for the average person to use for communication purposes, but it is more likely that a fraudulent or shady company will use a throw-away type email address on their website.

4. Who owns the website?
Sure, the "About Us" tells you who owns the company, right? Nope! The scam artist might be telling you about the company they want you to believe in. I always do a WHOIS query on a website. When you register xyz.com, you provide information about yourself (name, address, phone number, email address). This information is stored in a very large database. It is easily accessible and the access to it is free. If a website address ends in .com, .net, and .org, I use a program called SamSpade (download

currently unavailable). You can also go to any domain registrar and they will have a link to do a WHOIS query. Currently, you can go to the SamSpade website.

You are now thinking, "OK, so now what?" Type in the domain and get the WHOIS information. You will see a listing of information about the company or individual that owns it. Here two things can be done:

1. Does the contact information on the WHOIS query match what is listed on the website's contact page?
2. Is any contact information listed at all?

The most common technique used by scam artists is number 2. Let's say they own mycoolwidgets.com. If they opted to use number two, then you might see something like this:

Private, Registration mycoolwidgets.com@domainsbyproxy.com
Domains by Proxy, Inc.
DomainsByProxy.com
15111 N. Hayden Rd., Ste 160, PMB 353
Scottsdale, Arizona 85260
United States
(480) 624-2599 Fax -- (480) 624-2599

The particular domain I used to get this information was registered through GoDaddy. Just about every domain registrar I know of has some sort of privacy guard service like this. If they would not have used this service, then you might have seen something like this:

Widgets, Inc info@mycoolwidgets.com
12345 Sesame Street
Beverly Hills, CA 90210
Phone: 555-867-5309

Is their real information available? Yeap! Most of the registrar companies that offer this service have a way for you to obtain the information about a domain. You usually have to send a letter to the legal department of the company requesting the information. Included in the request is your reason for requesting this information. Domain registrars take the privacy of their clients very seriously. In my opinion, though, if you have to go through all this trouble to find out who owns the website, do you really still want to buy from them?

Next you might want to reverse trace this information. You can do reverse phone and address traces on whitepages.com or reverseaddress.com. If you have the person's name, search on ZabaSearch (http://www.zabasearch.com). If you decide to search the Internet for more reverse trace resources, I highly advise you stay away from any of those "Find anything about anyone!" type systems. The majority of them are scams.

5. What country are they based in?
Once you know what country they are based in, that can help quite a bit. First, you should realize that if you send any money out the country, it can be quite difficult to get it back. When you purchase a product or service, you are usually abiding by the laws of that country, state, or region. In addition, even if you would file suit, how will you get your money back? Have fun trying to convince the Chinese government that you won a court case in Kansas and you deserve your money. This is not to say the Chinese government would make it hard, it's just the simple fact of having to contact people of another country to get your $19.95 back. It will cost you that much just in phone calls.

Another matter to look at is what type of reputation does that region have? If you must shop internationally, does the company's geographic location. Some countries with high fraud rate are:

Romania, Indonesia, Singapore, Ghana, Ukraine, Uganda, Nigeria, Hungary, Belarus, Estonia, Latvia, Lithuania, Slovak Republic, Russia, Yugoslavia, Macedonia, Phillipines, Thailand, Malaysia.

In addition, keep clear of any countries on the U.S. Sanctions list, such as Cuba, Cote d'Ivoire, Iran, Iraq, Libya, North Korea, Sudan, Liberia, Zimbabwe, Sierra Leone, the UNITA faction in Angola, Syria and Burma [Myanmar]) (sanctions list obtained from the U.S. Treasury)

6. Our friend Google.
You can Google just about anything, names, phone numbers, addresses, website address. The options are limitless. Firstly, I Google the company's name. Let's say the name of the company is My Cool Widgets. Type in "My Cool Widgets" in to the textbox. Please do not type in that name without the quotes. Why? If you search for that company name without the quotes, then Google or any other search engine will look for any websites that contain the words, "My", "Cool", and "Widgets." Granted, search engines are designed to pull up the most relevant search results, but save yourself the time and risk. When you put the quotes around the company name, Google will search for any websites with the term, My Cool Widgets, instead of those three separate terms.

Next try searching for the phone number. Once again, please use the quotes. In regards to phone numbers, if you don't use quotes, then instead of searching for 555-867-5309, the search engine will search for any websites that contains "555", "867", and "5309". In my experience, the search engines are not as forgiving on giving "relevant" results with phone searches. On Google, you can also type in the textbox the following, but without the quotes, "phonebook: 555-867-5309". Google has an online phonebook feature. If the number is listed, it will reverse trace to the number. You can still use the reverse tracing websites listed towards the end of the "Who owns the website" section.

Finally, the same can be said for the address. Firstly, search for just the address (i.e. minus the city, state, and zip code). See what turns up. If you don't find what you are looking for, then try it with the city, state, and zip code.

7. What forms of payment do they accept?
I trust a company more if they accept a real credit card (merchant system) rather than just PayPal. I have nothing personal against PayPal, however, it common for PayPal and other "processors" have a high fraud rate. Another issue is that PayPal is not a bank, they are merely a payment processor. Therefore, PayPal does not have to abide by the same strict guidelines that banks do.

This is even more so if you are purchasing non-tangible (services such as hosting, an ebook, etc) products. What many do not realize is that the PayPal buyer protection does **not** protect you against fraud if you purchased a non-tangible item. Your only real recourse would be to file a chargeback with the bank of your credit/debit card.

If a company does accept credit cards via a merchant system as well as via PayPal, then that is not as bad. Some companies use PayPal with their merchant system because they might have customers that still feel safer using PayPal. In any case, make sure that when you enter personal information on a website that it is being sent securely. First, look for the locked padlock at the bottom right corner of your browser. You can double-click that to see the information of the company that owns that secure (SSL) certificate. Secondly, make sure that the address begins with https and not http. When you see that https, then that means the page you are on encrypts information that it sends.

8. Is it a home-based business?
I am not saying that all home-based businesses are fraudulent. It's just another thing to watch out for. I like to use a program called Google Earth. This program allows you to have an aerial view of an address. If you are able to get the physical address of a business (via WHOIS query, website address, Google search, etc) then you can type that address in to the program. Look at the general area of the address. Does it look like that might be office buildings or does it look like a rural/community type terrain? If it looks like a rural area, then the company is probably based out of a home. As previously-stated, just because a business is home-based does not mean that it is a fraudulent practice.

9. Are they a drop shipper or do they actually send out the products?
Drop shipping is a very common tool for those running an online business. It doesn't require any stock, so upfront costs, and no need to worry about going to the post office and shipping anything. Drop shipping is basically where your customer buys from you, you place the order with the drop shipping company, that company sends the order to your customer with your business name/address as the return label. If an invoice is included, either your company info is printed on the invoice or no company info is printed on the packing slip.

If you can find out if they are drop shipping, you might be able to get the product for cheaper elsewhere. In addition, if you plan on buying wholesale form the company, then why pay them when you could get it cheaper by buying direct from the company they buy from.

I use our old friend, Google. The first thing I search for is the product number. The higher ranking result (usually within the top 5, if not the first listing), is the company they are buying from. If you are a business, then contact that company and just buy direct from them. If you are a regular consumer, look for the best bargain. One search I performed on a product number I knew was from a drop shipping source came up with 273 results. The very first listing was the company that was the original company.

10. Just ask them.
After you have all of your information compiled, call the company. Never, and I do emphasize, **NEVER** be afraid to ask questions. If you ask questions and you don't feel comfortable that the person on the other end knows what they are talking about, ask to speak to someone above them (e.g. their manager or higher up personnel). If they avoid your questions or try to belittle you, then that's a huge flag. Stay away! They are not the only folks in the business.

Produced for Rip-off Report by Kajun Investigator, www.knownothing.net