



SiteHound User Guide

24th November 2006

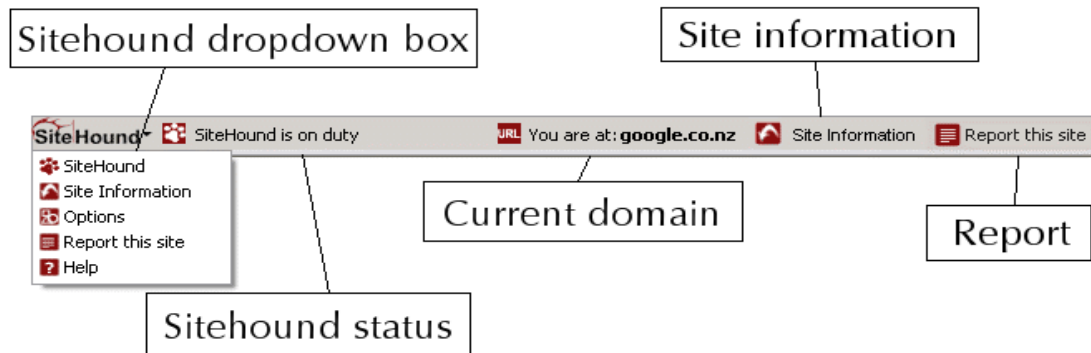


Table of Contents

| | |
|-------------------------------------|----|
| Using SiteHound..... | 3 |
| SiteHound at a glance..... | 3 |
| The SiteHound Status field..... | 3 |
| The Current Domain field..... | 3 |
| The Site Information button..... | 5 |
| Reporting a website..... | 6 |
| Updating SiteHound..... | 7 |
| Using the Whitelist..... | 7 |
| Password protecting SiteHound..... | 8 |
| Unblocking Adult sites..... | 8 |
| Getting Help..... | 9 |
| Glossary..... | 9 |
| Other ways to protect yourself..... | 10 |
| Useful Links..... | 11 |
| Feedback..... | 11 |

Using SiteHound

SiteHound at a glance



The SiteHound Status field

The **SiteHound Status** field displays updated messages which will change every 10 seconds.

The messages will inform you if the database needs to be updated, or should the database be up to date, SiteHound will inform you that it's running, how many websites are currently listed and how many current users there are.

The Current Domain field

The **Current Domain** field or 'You are at:' displays the active website you are currently visiting in it's most relevant and basic form.

With many scams, especially Phishing scams, the link that you believed you clicked on in an email, or from another website does not always immediately reveal the true address of the web site. You should pay special attention to this field to be sure it corresponds to the website you believe you are visiting.

Example 1

If you visit a website that has a particularly long website name, this can become confusing.

Browsing to this site :

http://collectibles.listings.ebay.com/Science-Fiction_Xena_W0QQcatrefZC6QQcoactionZcompareQQcoentrypgeZsearchQQcopagenumZ1QQflocZ1QQfposZQ5AIPQ2fPostalQQfromZR2QQfsooZ2QQfsopZ2QQftrtZ1QQftrvZ1QQsacatZ14289QQsadisZ200QQsagttfZ1QQsapplZ1QQsaprchiZQQsaprclloZQQsascsZ2QQsaslcZ2QQsatitleZQQsbrftogZ1QQsoZShowQ20ItemsQQsocmdZListingItemListQQsofocusZunknown

The SiteHound Current Domain field will display **ebay.com** which is the correct eBay website

Example 2

Website spoofing can be done so the website name can appear legitimate and contain text that is familiar, however you are in fact being directed to another website entirely. In the example below which was taken from an AOL Billing Scam

http://0x46.0x6b.0xf8.0xe6/aol/bill_form.html

Despite the "aol/bill_form.html", the SiteHound Current Domain field will display "**0x46.0x6b.0xf8.0xe6**" which is a fake

Note : Do not enter your details into this web page if it is active.

Example 3

Website spoofing. In the example below though the website name appears to be for eBay in fact the website being visited is 209.213.221.135 with a username of "signin.ebay.com"

<http://signin.ebay.com@209.213.221.135>

The SiteHound Current Domain field will display "**209.213.221.135**"

Note : This website is an example only and will not function.

The Site Information button

The Site Information button will display relevant information on both the Site Owner (also known as the Registrant) and the details of what country the website is hosted in (also known as the Registrar)

If you are using the free version of SiteHound you will only see the information displayed as text for the Registrant.

If your copy of SiteHound is also registered, then you are presented with both maps showing the country of the Registrant (Site Owner) and Registrar (Site Location), as well as other information such as the Site Owners name. This is useful should you be cautious of a website.

For example.

At the time of writing this, the following website www.chkuntiondefun.com stated their contact information on their website as being

Palm Grove House
P.O Box 438
Road Town
Tortola
British Virgin Islands

However a quick look at the SiteHound Site Information reveals both the Registrant (Site Owner) and Registrar (Site Location) are located in China

fire trust
SITEHOUND

URL ACCESS
PROTECTION

chkuntiondefun.com

SITE OWNER (REGISTRANT)

SITE LOCATION (REGISTRAR)

China

China

Site Owner: Dima li
IP Address: 61.188.39.212
Country: CHINA (CN)

Country: CHINA (CN)

Reporting a website


You can report a website through to us by pressing the “Report this site” button from the SiteHound toolbar

Doing so will open a new browser window in which the website you were currently visiting will be presented for reporting. You can also alter this URL should you need to.

Select which category(s) you feel the website belongs, and enter as much information that you can about the person(s) involved, general information about the website, or details relating to the scam, then simply press Submit. We will review your submission and should it be accepted, add it to the list of bad websites. The details you entered into the comments area will also be available to other registered users.

No personally identifiable information however will be included, unless you enter this yourself, however we would strongly advise to never enter any personal details into these fields.

Example :

**REPORT URL** URL User ID: 25649859

Category (required) (Click question mark button for category definition.)

| | | |
|-------------------------------------|---|---|
| <input type="checkbox"/> Adult ? | <input type="checkbox"/> Spyware ? | <input type="checkbox"/> Spamvertising ? |
| <input type="checkbox"/> Phishing ? | <input type="checkbox"/> Possible Scam or Fraud ? | <input checked="" type="checkbox"/> Misleading or False Advertising ? |
| <input type="checkbox"/> Pharming ? | <input type="checkbox"/> Rogue or Suspect Product ? | <input type="checkbox"/> Adware ? |
| | <input type="checkbox"/> Malware or Virus ? | |

Site Information

Company/Individual involved:

Also known as:

Contact details:

General/Site info:

Technical/Further info:

Updating SiteHound

Updating SiteHound Manually

You will be reminded in the **SiteHound Status** field should the database of bad websites be out of date, and need to be updated.

To do this manually, from your browser go **SiteHound >> Options >>** and select **Update Now**

This will download all the changes to the database of bad websites, since you last update.

For any reason, should you wish to download the entire database of bad websites again, from your browser go **SiteHound >> Options >>** and select **Full Update**

Updating SiteHound Automatically

Registered users will enjoy the benefit of automatic updates to SiteHound's database of bad websites. Should the SiteHound database become out of date, SiteHound will update itself automatically if the browser is open, or when you next open your browser.

You can also update manually as well if you prefer. To change the automatic update settings, from your browser go **SiteHound >> Options >>** you will see the settings for changing this here.

Using the Whitelist

The Whitelist allows you to protect websites from being blocked by SiteHound, though if you believe a website is being blocked in error contact sitehound@firetrust.com and let us know.

However if there is a website you access frequently that SiteHound does legitimately block, you can add this to your whitelist.

To do this either access the website from your browser and select **SiteHound >> Add to Whitelist**.

OR

From your browser select **SiteHound >> Options >>** select the **Whitelist** tab at the top >> enter in the website you wish to whitelist e.g. sitehound.com >> then click the **Add** button.

Password protecting SiteHound

SiteHound allows you to create a password to protect blocked sites. This option means that in order to enter a website blocked by SiteHound, you will need to enter the password.

To create a password

Open your browser and select **Options >> Personal Options** from the SiteHound toolbar >> check the the **Create Password** box >> Enter a password under **New Password** >> Enter the password again under **Retype Password** >> Click **Apply**

You can then select **Password protect blocked sites so that the password will be required in order to enter a website blocked by SiteHound**

Click **Apply >> OK**

Note : Please keep a copy of this password for safekeeping or choose a password you are likely to remember

Unblocking Adult sites

To stop SiteHound from blocking Adult websites.

Open your browser.

Click **Options > Personal Options** from the SiteHound toolbar.

If you have **already enabled** the Password Protect feature **simply remove the check mark from Block Adult Sites**.

You will then be asked to enter your current password in order to activate this feature.

Enter your password and then click **Apply**.

If you have not already enabled the Password Protect feature, then see the section above.

Getting Help

The online help can be accessed by pressing the **Help** button from the SiteHound toolbar or you can access it directly from <http://www.sitehound.com/support/help/>

The user supported forum for SiteHound and other Firetrust programs can be seen here <http://www.firetrust.com/forums/>

Otherwise feel free to send us an email to sitehound@firetrust.com

Also try to be as descriptive as possible in your email, as this will enable us to answer your question without first having to ask you more questions.

For general information see the **Useful Links:** section below

Glossary

Adware or advertising-supported software is any computer program or software package in which advertisements or other marketing material are included with or automatically loaded by the software and displayed or played back after installation, or in which information about the computer or its users activities is uploaded automatically when the user has not requested it. These applications often present banner ads in pop-up windows or through a bar that appears on a computer screen.

Malware is a software program or service developed for the purpose of causing harm to a computer system, or altering its behaviour for profiteering purposes.

Pharming is a new form of phishing attack (i.e. email based fraud) that employ malicious software and other techniques in an attempt to steal personal data from unsuspecting Internet users. These new forms of fraud dubbed "pharming" attacks combine malicious software with traditional email based phishing techniques to create scams that are more dangerous and more difficult to detect, even for experienced Internet users.

Phishing is a form of criminal activity, by attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message. The term phishing arises from the use of increasingly sophisticated lures to fish for users' financial information and passwords.

Spamvertising is a website advertising itself by sending unsolicited junk emails, or spam.

Since buying products or services from spammers only encourages them to send more, you should consider doing business with a different website instead.

Spyware consists of computer software that gathers and reports information about a computer user without the user's knowledge or consent.

Other ways to protect yourself

Unless you have been a victim, it's difficult to imagine having your identity stolen. Often we associate theft with the loss of a physical item, such as my prized XBOX 360, however with a few pieces of the right information someone can, unfortunately, imitate your person to achieve a goal, whether it be removing money from your bank, running fake auctions under your name, or using your identity to purchase products be it online or through credit services.

Protect your identity. Don't give your bank account numbers, credit card numbers or other personal information to anyone you don't know or haven't checked out. When dealing with people over the phone, do not give out any personal information unless you yourself initiated the call.

Do not accept unsolicited emails. Because email is a cheap and effective way to broadcast a message, it's become a common tool used by scam artists. You should also, when given the chance opt-out of third party information sharing

Be wary of "trusted" sources. Your bank will not send you an email in which they ask you to confirm any personal details, your bank should not call you to confirm your credit card or other bank card PIN numbers. When scammers attempt to make contact pretending to be a trusted source, they often do so with a false sense of urgency. If you notice this high pressure technique be wary. This policy can also extend to many other situations outside of the internet, so if you're being pressured into making decisions suddenly and without full and proper thought, you should take a cautious approach.

Be extremely suspicious of money orders. While it can be said that money orders are a legitimate tool for financial exchanges, fake money orders are a very common medium for fraud, particularly with auction fraud. A bank will often accept a money order, but then when it's discovered to be fraudulent, you are the one responsible for the amount. Money orders are not covered by the same limited liability laws that we enjoy with our credit cards. In fact the limited liability laws make credit cards far safer than money orders for transactions.

Check your bank account and credit card statements frequently. Be on the look out for purchases or transactions that you may not be familiar with.

Don't judge reliability by how professional a website looks. It's relatively easy and costs very little to create, register, and promote a website. Remember that people and companies you communicate through the internet with are not always what they seem.

If it sounds too good to be true, it probably is. Ask yourself

"How could I win a lottery prize if I haven't bought a ticket ?"

"How would Bill Gates share his fortune with me, if I forward this email ?"

"Why would the lost prince of the little known country of Scamartistan share his millions with me ?"

If you win something you should not pay anything to receive your prize. This technique is very common, and is also known as Advance Fee Fraud, or 419 Fraud. Eventually the scammer will reveal that in order for the arrangement to proceed a smaller amount of money is required to be paid first.

Be cautious of Internet Dating. Unfortunately scam artists have begun using Internet Dating sites to groom people over a longer period of time, eventually requesting money whether it be for travel (to be together) or for some other deeply emotional issue, such as a family member requiring medical attention.

Useful Links

Artists Against 419 – <http://www.aa419.org>

CARMA - <http://carmainc.org/>

CastleCops – <http://www.castlecops.com>

Calender of Updates - <http://www.dozleng.com/>

Federal Trade Commission Grand Scam Test - <http://www.ftc.gov/grandscam>

MalWare Removal - <http://www.malwareremoval.com/>

PayPal - https://www.paypal.com/cgi-bin/webscr?cmd=_vdc-security-spoof-outside

RipOffReport - <http://ripoffreport.com/>

Romance Scams - http://en.wikipedia.org/wiki/Romance_scam

ScamBusters - <http://www.scambusters.org>

SpyWareWarrior - <http://spywarewarrior.com/>

Subratam - <http://subratam.org/main/>

Feedback

For any feedback, suggestions or alterations regarding this document please send them through to sitehound@firetrust.com