

Anti-Phishing Toolbar Comparison Check List

	A	B	C	D	E	F	G	H	I	J
Solution	Watch for Phishing	Authenticated White List	Protect Against Pharming	Protect Against Man in the Middle Attacks	Validated Company Name	Enhanced User Features Allow for Personal Site Approval	Supports IE 6, IE 7, Firefox, Netscape	Supports Windows 95, 98, ME, 2000, XP, Vista, Fedora, Mac	Free	Invades Privacy
TraceAssure	♦	♦	♦	♦	♦	♦	♦	♦	♦	-
PhishTank SiteChecker	♦	-	-	-	-	-	-	-	♦	♦
Netcraft	♦	-	-	-	-	-	-	-	♦	♦
Petname	♦	-	-	-	-	♦	-	-	♦	-
iTrustPage	♦	-	-	-	-	-	-	-	♦	♦
FirePhish	♦	-	-	-	-	-	-	-	♦	-
TrustBar	♦	-	-	-	-	♦	-	-	♦	-
SiteAdvisor	♦	♦	-	-	-	-	-	-		-

TraceSecurity has made every effort to validate this information is 100% accurate.
 If you feel there is a mistake in this diagram please report it to support@tracesecurity.com

A) Watch for Phishing

Phishing attacks continue to rise and the sophistication of these attacks makes it extremely difficult for the average user to detect. Browsers such as Internet Explorer 7 and Firefox 2 have attempted to reduce the risk by incorporating anti-phishing technology but tests have shown these solutions have had little effect on protecting against phishing attacks. Because of this, a number of solutions have been created to resolve the phishing crisis. The effectiveness of these new solutions also has been questionable and due to most solutions being based on a “blacklist” approach, they tend to be reactive, only becoming aware of issues after numerous users have already become victim. Because of this, it is important to look for a solution that is not based on the blacklist (Reactive) approach but instead uses a “white list” (Proactive) methodology.

B) Authenticated White List

A white list is based on only approving what can be validated. A simple way to think of this is deciding to have a party where you only want people you trust. So you make a list of trusted people and then when each person shows up at the door, you look at the list and see if they are on it. If they are then they can come in. If not they are sent packing. Now let's compare this same scenario using a blacklist. In this case you would be required to make a list of every single person you did not trust. When each person came to the door you would review the list and if they were not on it, then they would be allowed in. This of course means that if you forgot to put someone on the list they would be allowed in. Or if you had never heard of a person before, they would also be allowed in. Basically the only people blocked would be people you had already had past experience with that you now knew couldn't be trusted. This is why the blacklist approach has failed and why every day more and more people fall victim to phishing attacks. With the white list, you can be 100% certain that if the site comes back as authenticated, then you are safe to visit it. If on the other hand it comes back unknown, then you are clear that the site could be risky and you should use caution. TraceAssure is the only solution on the market that not only uses a white list but ties that back to a cross comparison with IP and Domain information to eliminate not only Phishing attacks but also Pharming and Man in the Middle.

C) Protect against Pharming Attacks

Many people are not aware of pharming attacks and therefore are susceptible to these types of attacks. Pharming attacks can come in several different forms but ultimately the end user will input a real URL but be redirected to a malicious site. For example, if you were to enter the URL www.tracesecurity.com into your web browser, you would assume that when the page was displayed, it would be the website of TraceSecurity. However, if a hacker is able to modify the DNS settings for that domain, they could simply send you somewhere else. This becomes a major threat when you are doing online banking or transactions as you could inadvertently submit confidential information to malicious sites without ever having any idea. A simple way to understand DNS is to think of a hotel address. If you told someone that you were staying at the Hilton in Downtown Baton Rouge and needed someone to pick you up, you could simply tell them where you were staying and assume they could find you. The reason they could find you is because they could lookup the address based on the name of the hotel and the area you were staying. DNS basically allows for the same lookup. When

you give the URL www.tracesecurity.com, you are basically giving the name and location but are not giving the real address. DNS will in turn take that information and translates it into what is known as an IP address. An IP Address may look like 172.16.0.1. Most people never see these addresses and would have a very difficult time remembering them. Now, if a malicious person could modify the DNS so when the URL lookup was made, a different IP address was resolved, this would mean that your computer would no longer go to the site you typed in but instead to another site that may impersonate the real site. Ultimately what is important to understand is that Pharming attacks do happen and TraceAssure is designed to protect you while other tools can't.

D) Protect against Man in the Middle Attacks

A man in the middle attack basically means that while you are visiting a web site, everything you do is being monitored and or recorded by another site. Remember when you were a kid and you decided you were not talking to your sister so whenever she asked you a question, instead of answering her, you would tell your mom and your mom would in turn relay it back to her. Man in the middle attacks would be similar to that only it's not your mom in the middle and you have no idea that it's taking place. Most often this attack is used in conjunction with a Pharming attack. The user enters in a URL and instead of going to the real site; they first pass through the malicious site, that site then in turns records the data that is passed and then connects to the real site. By staying in the middle, the malicious site gets to watch all information you send to the web site and all information that is returned from that web site. While this will generally go unnoticed by the end user, TraceAssure will detect and warn you if this is taking place when you attempt to visit authenticated web sites.

E) Validated Company Name

Often times companies are unable to get URLs that match their company name. Therefore they must become creative and use URLs that are either similar or in some cases are just completely different from their real company name. This makes it extremely difficult for the average user to have any guarantee that the site they are visiting is truly the company they thought they were visiting. TraceAssure takes the guesswork out by displaying the real company name each time you visit an approved or authenticated web site. This additional information is not just an automated guess by the software but has actually been validated by the Security Staff of TraceSecurity. Giving this extra information is yet another way that TraceAssure is designed to help users easily avoid security threats.

F) Enhanced User Features Allow for Personal Site Approval

Because there are billions of web sites that people can visit, obviously not every site will be approved or authenticated by TraceAssure. In many cases for example a user may be browsing what is known as an Intranet. This is a web site located on a companies internal network and not accessible to people on the Internet. In these cases a user may be approved even though TraceSecurity engineers haven't or can't approve it through normal channels. With the click of a button the user can make the approval themselves allowing for future ease of mind when browsing the same site.

G) Supports IE 6, IE 7, Firefox, Netscape

TraceAssure was developed to run in Internet Explorer 6, Internet Explorer 7, Firefox 1, Firefox 2 and Netscape 9. Supporting so many different platforms is extremely rare for any tool and shows the commitment dedicated by TraceSecurity to protect all users on all platforms.

H) Supports Windows 2000, XP, Vista, Fedora, Mac

TraceAssure will run in browsers on numerous operating systems. Approved operating systems are Fedora 2, 3 and 4, Mac OSX, Windows 95, Windows 98, Windows ME, Windows 2000, Windows XP and now Microsoft's Vista!

I) Free

No tool comes close to the complete solution offered by TraceAssure and best of all, TraceAssure is 100% free!

J) Invades Privacy

TraceAssure was designed with privacy in mind. Therefore absolutely none of your data is collected or monitored by TraceSecurity. In fact the only information that is ever passed from a users PC to the TraceSecurity network is the version number of the toolbar when a database update is requested. Surprisingly though, a number of other solutions do invade your privacy. Each tool is different in how much data is being monitored but often times they will track every single web page you visit and in some cases capture other usage information off of your computer. Some tools will even cause major browsing delays when they silently connect to another web site; first where they monitor the page you are going to and then let you continue each time you visit any web page. Security should not require your privacy to be invaded and at TraceSecurity we have found that not only can we offer you a higher level of protection, we can do it without becoming big brother. Simply put TraceAssure will protect your privacy, not invade it.