



New Netcraft Toolbar Blocks Phishing, Analyzes Web Sites

December 30, 2004

By Larry Seltzer

A new, free browser add-in from English Internet services firm Netcraft Ltd. fights phishing attacks and helps users investigate sites they visit.

eWEEK.com tested [the new tool bar](#), available initially only for Internet Explorer on Windows 2000 and Windows XP, and liked what we saw. All but one phishing link we visited was interrupted by a popup from the tool bar (click here to see a sample) and we used the built-in link to report the one site that the tool bar didn't block.

Once installed, the tool bar exists as an IE Explorer Bar, much like the Google tool bar, and coexisted well with other Explorer bars in our tests. (See the image of the tool bar below and click the image to see it within a browser window.)

The tool bar has two buttons, both of which have links to other services by Netcraft, many of them free. The Netcraft button exposes other security functions, such as reporting a phishing site unknown to the tool bar and reporting false positives from the tool bar, as well as many statistical reports, such as which countries and hosting services have the most phishing sites.

For insights on security coverage around the Web, check out eWEEK.com Security Center Editor Larry Seltzer's [Weblog](#).

Netcraft is most famous for [its Web server survey](#), reporting which Web server software is most in use on the Internet. For this and other research, the company scans the Internet regularly and has built up a large database of sites and what is running on them. This data plays a key role in the function of the tool bar.

RELATED LINKS

[New Browser Hole is a Phisherman's Delight](#)

[Industry Leaders Build 'PhishNet' to Stop Identify Theft](#)

[Finance CSOs: Feds Are No Help with Phishing](#)

[Pop-up Loophole Opens Browsers to Phishing Attacks](#)

[Scammers Exploit DomainKeys Anti-phishing Weapon](#)

Beyond the two buttons, the rest of the tool bar displays information about the site being viewed in the browser. First is the date the site was first observed by Netcraft. There is also a ranking of the site by number of visits, presumably by users through the Netcraft site and software. Finally, the tool bar reports the hosting service or netblock owner.

Netcraft tracks phishing sites in its database and uses that data to block sites when users visit them. The company also uses some heuristic techniques to block practices often used by phishers to deceive users, such as including '<script>' tags in a URL and other known attacks.

Even when the tool bar misses a phishing site, or some other type of Web-based fraud, the information in the tool bar could provide valuable clues about the legitimacy of the site. For instance, the site we visited that the tool bar didn't flag—purporting to be yet another Paypal log-in—was listed as a "New Site" (never seen before by Netcraft) and on a netblock owned by "Comite Gestor da Internet no Brasil." Just in case you're curious, the netblock for [www.paypal.com](#) is owned by "eBay, Inc."

For more on fighting phishing attacks, read Larry Seltzer's column ["Spotting Phish and Phighting Back."](#)

According to Netcraft, the company has received a great many requests for a Mozilla/Firefox version of the tool bar and is at work on it, but gave no dates for delivery.

Now that we have the tool bar running we expect to be using it frequently. Users who are nervous about fraud on the Internet can feel much better about the browsing experience by running the Netcraft Toolbar.

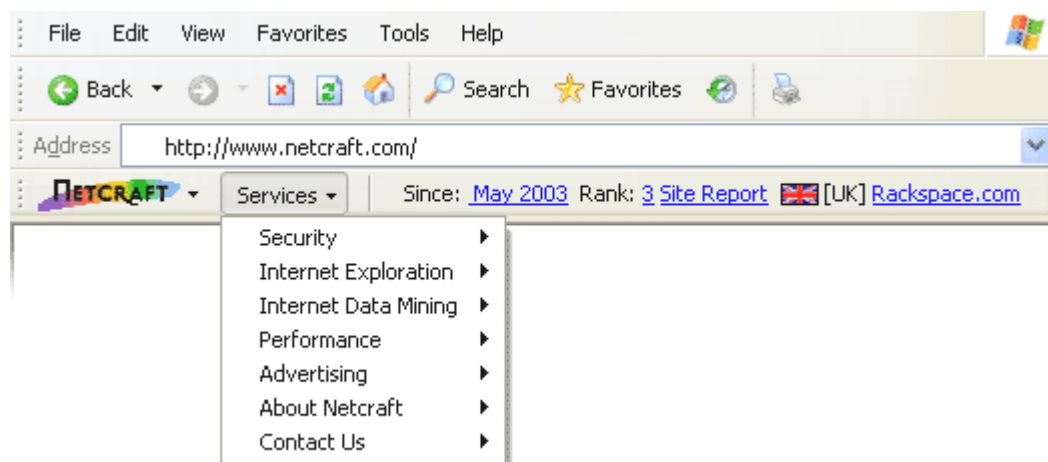
Check out eWEEK.com's Security Center for the latest security news, reviews and analysis.

Copyright (c) 2004 Ziff Davis Media Inc. All Rights Reserved.



Site Search

Netcraft Toolbar



- **Protect your savings from Phishing attacks.**
- **See the hosting location of every site you visit.**
- **Help defend the Internet community from fraudsters.**

The Toolbar community is effectively a giant neighbourhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against [phishing](#) frauds. Once the first recipients of a phishing mail have reported the target URL, it is blocked for community members as they subsequently access the URL. Widely disseminated attacks (people constructing phishing attacks send literally millions of electronic mails in the expectation that some will reach customers of the bank) simply mean that the phishing attack will be reported and blocked sooner.

The Toolbar also:

- Traps suspicious URLs containing characters which have no common purpose other than to deceive.
- Enforces display of browser navigational controls (toolbar & address bar) in all windows, to defend against pop up windows which attempt to hide the navigational controls.
- Clearly displays sites' hosting location, including country, helping you to evaluate fraudulent urls (e.g. the real citibank.com or barclays.co.uk sites are unlikely to be hosted in the former Soviet Union).

Please [download and try out](#) the toolbar.

Information about licencing a branded version of the Toolbar for your own organisation is also [available](#).

Download Netcraft Toolbar

System requirements: Internet Explorer on Windows 2000/XP



Site Search

Netcraft Toolbar Help Pages



Toolbar Questions

What is the Netcraft Toolbar?

I use the Google Toolbar. Can I use the Netcraft Toolbar as well?

What if I find a URL that I cannot report?

How do I visit a site that has been blocked?

Will Netcraft know which pages I visit?

What does it mean when the toolbar says "New Site"?

What do I do when the display of the toolbar/address bar has gone all "weird"?

I don't use Microsoft Internet Explorer. Can I still use the Netcraft Toolbar?

General Questions

What is phishing?

Who are Netcraft?

I have a question that is not answered here. Who do I send it to?

What is the Netcraft Toolbar?

The Netcraft anti-phishing system consists of a user interface implemented as a **toolbar** (a small program that is active whenever the user is browsing the web using Microsoft Internet Explorer) and central servers, able to respond quickly to large numbers of requests as each user moves around the web. The central servers are managed by Netcraft and hold the information about URLs and sites provided by the the Toolbar community and Netcraft.

I use the Google Toolbar. Can I use the Netcraft Toolbar as well?

Yes. Several people at Netcraft use both the Google and Netcraft Toolbars simultaneously and it seems to be fine.

What if I find a Phishing URL that I cannot report?

There are a number of situations where you will not be able to report a URL directly using the toolbar, including, but not limited to:

- The page contains malicious Javascript, preventing normal browser operation.
- The URL is in a popup window that has been blocked.

- The page redirects to another location.

If you encounter a URL which you cannot report, please send the entire phishing mail message as a MIME attachment to scam@netcraft.com and we will investigate.

How do I visit a site that has been blocked?

If you are absolutely sure you want to visit a site that has been blocked, you can hold down the "Ctrl" key to bypass the toolbar's blocking behaviour. You may experience this when using FTP sites which require authentication (using the "File -> Login As..." menu option in the browser). If you hold down the "Ctrl" key while clicking the "Log On" button then you will be able to browse the FTP site correctly.

Will Netcraft know which pages I visit?

No - Netcraft have no way of knowing which pages you visit when using the Toolbar. In order to provide a defence against phishing URLs we construct and transmit a secure [hash](#) of each URL browsed from the Toolbar to a central server. The server compares this hash with a list of hashes of previously reported phishing URLs and instructs the Toolbar to block the page if it finds a match. There is no other case in which we can determine the URL of the page you have visited from the hash which we receive. We do, however, collect the names of the web sites visited by our users in order to provide popularity ranking information and contextual reports for the site being browsed.

In order to protect the privacy of organizations' internal networks the Netcraft Toolbar does not transmit information about sites on RFC 1918 private networks.

What does it mean when the toolbar says "New Site"?

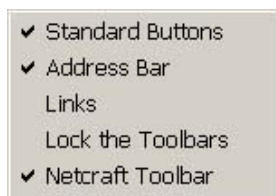


"New Site" means the site you are currently visiting has not been seen before by the [Netcraft Web Server Survey](#). This indicates that the site is very new and should be considered less trustworthy than other sites. Since most phishing sites spring up overnight and disappear just as quickly, you should be extremely suspicious if you see this when visiting what you believe to be a trustworthy site.

What do I do when the toolbar/address bar is displayed incorrectly?

The display of the toolbar, address bar and other elements of the browser can sometimes become confused and may overlap or be otherwise obscured. This can be fixed by:

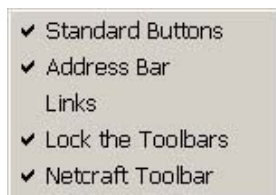
1. Right-click on the toolbar area and ensure that the menu option "Lock the Toolbars" does not have a tick next to it. This may require selecting the option to toggle it off.



2. Once the toolbars are unlocked, a "grab bar" will appear to the left of each browser element that can be moved. Click on these and drag the bars to arrange them as you wish.



3. Right-click again on the toolbar area and select "Lock the Toolbars" to prevent them from being accidentally moved after you have arranged them.



I don't use Microsoft Internet Explorer. Can I still use the Netcraft Toolbar?

Not presently. We intend to make the Netcraft Toolbar functionality available in other browsers and on other operating systems. Please [let us know](#) the browser and operating system that you use, as this will help prioritize development.

What is phishing?

Phishing is a name derived from the notion of "fishing for information", and "phreaking", which was an eighties term used for people who hacked phone networks and systems to gain access to free calls, or control over parts of the telephony system. It is a simple concept, which is to try to trick people into disclosing their bank account details, so that the attacker may then log in to the person's Internet bank and withdraw their savings.

Organisations which are not banks, but which have accounts that allow the customer to administer money or other tokens of value are also affected; this includes credit card companies, credit unions, exchanges, and some Internet retail sites. Amazon, Paypal, Visa, and Ebay are some non-bank sites that have been attacked to date.

Phishing is a highly scalable and attractive opportunity for fraudsters; many people in the civilised world now have Internet enabled bank accounts, and under normal circumstances they offer a more pleasant and convenient user experience than visiting a bank branch or telephoning a bank call centre. Many businesses also have Internet enabled bank accounts, and a very significant amount of wealth is accessible via web based banking systems, typically protected by a username and password and other textual tokens supplied over the web by the account holder.

The technology required to construct a phishing fraud is minimal. Conventionally, the fraudster constructs an html mail message with forged mail headers indicating that the mail has come from the bank, and asks for the recipient to confirm their bank account username and password. To make the request appear more authentic, the mail usually links to a web server that opens a new window with the bank's own site (not a copy, but the actual site), and asks for the account details in a separate window, hosted on the attacker's server.

- Hosted at a company that is paid to ignore complaints about the scam; unscrupulous hosting locations in Asia and the former Soviet Union sell "bullet proof hosting" as a service, meaning that they will endeavour to keep the site running despite requests to close it down from outside of their own jurisdiction. A server involved in an attack on Barclays was hosted in Moscow and stayed up for at least a week after the phishing attack first started.
- Hosted on a machine that the attacker has broken into, without the owner's knowledge.
- Hosted at a bona fide web hosting company; phishing sites hosted at reasonably reputable hosting companies will be taken down quickly once complaints arrive.

There are no publicly available dependable statistics on how many of a bank's customers receiving phishing mails respond to them, but the fact that the largest UK banks have taken their entire banking sites offline during some phishing attacks indicates that the fraudsters are enjoying a non-trivial degree of success. There has been speculation that phishing may drive Internet banking off the Internet until the banks re-engineer their systems to require an additional level of security that cannot be compromised in this fashion, such as a one-time password generated by a SecureID card or equivalent operation.

Who are Netcraft?

Netcraft is an Internet services company based in Bath, England. Netcraft is funded through retained profit and derives its revenue in the following ways:

- Providing network security services, including application testing and automated penetration testing.
- Providing research data and analysis on many aspects of the Internet. Netcraft has explored the Internet since 1995 and is a respected authority on the market share of web servers, operating systems, hosting providers, ISPs, encrypted transactions, electronic commerce, scripting languages and content technologies on the Internet.

Netcraft has a cosmopolitan client list, spread through the UK, the USA, mainland Europe, the Middle East, Asia Pacific and Latin America. Clients include Aegon, American Express, AMP, Britannic, British Telecom, Cable & Wireless, Capita, Credit Suisse, Dell, Deloitte & Touche, Energis, Elsevier Science, GCHQ, Hewlett Packard, IBM, Intel, Interland, John Lewis, Lloyds of London, Macromedia, Microsoft, Morgan Stanley, Northern Rock, Oracle, Rackspace, Securicor, Sun Microsystems, Verisign, Virgin, Visa, and Vodafone.

<http://www.oreillynet.com/pub/wlg/3605>

"I've thought for a long time that Netcraft represents a real revolution in market research. Firms like Gartner can tell you what they think people are going to do. Folks like Netcraft can tell you what people are actually doing." Tim O'Reilly, August 2003.

<http://www.linuxworld.com/story/33855.htm>

"It's no surprise that someone of the caliber of Bob Metcalfe, inventor of Ethernet and co-founder of 3com, should have called [Netcraft](#) 'cool'." Linuxworld, July 2003.

I have a question that is not answered here. Who do I send it to?

Please send it to toolbar@netcraft.com.

COPYRIGHT © NETCRAFT LTD. 2004-5
