Microsoft anti-phishing software raises Internet privacy concerns

Mike Ingram
17 September 2005

A phishing filter developed by Microsoft and to be included in the next release of the Windows operating system has raised concern amongst privacy advocates.

The filter software is to be included in Internet Explorer 7 but has been released early as an extension to existing versions of the Windows web browser.

Phishing is the term given to the use of fake web sites in order to steal the identities of users. Phishing fraud normally starts with computer users receiving emails appearing to be from banks, credit card companies, or sites such as eBay and PayPal, requesting account updates. Links are provided to web sites that seem legitimate but in fact store the information, to be used for illegal activity. Unwary users are duped into giving up their Social Security, credit card and bank account information.

The increase in phishing attacks has prompted a new genre of software known as anti-phishing tools. Most of these come as extensions to the web browser, most commonly Internet Explorer. Two such tools are CallingID, and SpoofGuard from Dan Boneh and John Mitchell of the Stanford Security Lab. Netcraft also provides a toolbar for Internet Explorer and Firefox, which assists users in identifying phishing sites.

Anti-phishing software uses a combination of different methods in an attempt to spot spoof sites. Domain analysis is used to verify domain registrations using a number of criteria and from a number of sources. Session analysis is used to determine if a site uses properly encrypted communications and spot other telltale signs of a spoof site. Most of these programs are known as client-side, in that they operate on the user's own computer without sending data to a server.

Microsoft's anti-phishing software is controversial in that it sends a user's browsing activity to Microsoft servers for comparison against lists of sites know to be either good or bad. According to the Microsoft web site:

"Phishing Filter is a feature in Internet Explorer 7.0 that helps determine whether a Web site is legitimate or a so-called phishing Web site." Internet Explorer 7.0 is only available to a select group of developers and is not expected for general release within the next year. The phishing filter software is to be made available as an extension to existing versions of Internet Explorer over the next few weeks. The web site specifies three checks designed to help protect users from phishing scams:

"1. It compares the addresses of web sites that a user attempts to visit to the addresses of sites that have been reported as legitimate. This list is stored on the user's computer.

"2. It analyzes sites that a user attempts to visit by checking those sites for characteristics common to phishing sites.

"3. If the user chooses, Phishing Filter sends the addresses of web sites that a user attempts to visit to Microsoft to be checked against a frequently updated list of reported phishing sites."

It is this last point that has come in for the most criticism. Privacy campaigners argue that this allows Microsoft to track Internet use. Kevin Bankston, a lawyer and Internet privacy expert with the San Francisco-based Electronic Frontier Foundation, has said this is potentially "a wholesale handing over of one's privacy to Microsoft. I would say, right now, definitely don't use this. If you're careful, you don't need this."

As the software becomes integrated into the next generation of Microsoft Windows, however, users will have little option but to use it. While the sending of information to Microsoft is optional, many users will not realize the significance of what they are doing.

The problem of Internet security is a serious one, which needs to be addressed at many levels. Technology can assist in this and some of the new client-side anti-phishing software does seem to be effective. In the case of Microsoft's server based solution, however, too many questions arise for this to be considered a legitimate response to the problem.

Microsoft has, of course, insisted that it has no intention of tracking a user's web browsing activity and says it does not store the information sent by the phishing filter. "We don't store that information," Greg Sullivan, Microsoft Windows group product manager, said. "There is no server event log, no data base, no hosted event file."

Kevin Bankston told the Australian publication the *Age* that the information may be too valuable for Microsoft to ignore in the longer term. "There are clear financial imperatives for them to choose to make use of this information in the future and start logging it," he said. "It is not hard to imagine the gold that could be mined out of that information."

In fact, decisions as to the retention of such information may not be left to Microsoft at all. In the aftermath of the terrorist attacks of September 11, 2001, and those in London in July this year, there have been increasing demands by security forces internationally for broader access to electronic data and for Internet Service Providers to be required to log certain data.

There is also a question of the freedom of the Internet as a means of mass dissemination of information, open to all. Microsoft proposes to maintain a "white list" of sites deemed legitimate. Officials say the list of approved sites, which Microsoft calls "the list of highly trafficked legitimate web sites," will number in the "tens of thousands." The list is being provided by Nielsen NetRatings, which measures Internet traffic. ICANN, the Internet Corporation for Assigned Names And Numbers, reported in August that there are 43 million active registered domain names worldwide, meaning that only a tiny percentage of sites will make it to the Microsoft list.

Michael Aldridge, a product planner with Microsoft's technology care and safety group, told the *Age* the company would not be vetting which web sites are contained on the list. "It is based ... purely on traffic. We make no judgments on content."

For inexperienced users, the prospect of error messages to the effect that their identity may be stolen if they proceed to a selected site could prove intimidating enough to have them avoid the site all together. There is a very real danger that the phishing filter will have the effect of creating a two-tier Internet, with sites designated as safe or not, supposedly on the basis of the number of people visiting them on a list controlled by the world's largest software corporation.