

## **Microsoft Phishing Filter: A New Approach to Building Trust in E-Commerce Content**

The recent flurry of media coverage around identity theft and what is being called “the new scam of phishing,” in which online thieves attempt to use computers to gain illegal access to personal information, sometimes obscures the fact that these scams are not new but actually predate computers. In the pre-PC era (and sometimes even today), scam artists pretending to be bank employees or other similar seemingly trustworthy people would telephone unsuspecting consumers and convince some of them to give the caller private information, much to the consumer’s eventual dismay.

Phishing is bigger. Its emergence in online communications media allows scammers to reach many more people than ever before and at lower cost, whether through spam, e-mail and instant message scams; faked Web pages; or other online avenues. Media outlets have reported that phishing-related scams have resulted in more than \$2 billion in fraudulent bank and financial charges to date.

But although the media usually (and appropriately) focus on phishing’s consumer impact, there is an equally important topic that needs to be explored: the huge impact phishing has on legitimate Web site owners. Any solution that attempts to approach phishing in a holistic way needs to focus on both consumer and business audiences to help create a trustworthy e-commerce system in which all parties are protected and aware of potential hazards.

### **A Variety of Approaches**

To that end, Microsoft Corp. is taking a multipronged approach to combat phishing. This includes promoting effective legislation and working with law enforcement to enforce those laws, encouraging best practices by both Internet service providers (ISPs) and consumers to build awareness of potential phishing attempts, and developing and promoting innovative technology solutions that help protect users against phishing.

Microsoft has already made a number of investments in anti-phishing technology, including adding new functionality to its SmartScreen™ technology spam-filtering process to check for specific characteristics common to phishing scam e-mail. In MSN® Hotmail®, when SmartScreen detects a phishing e-mail, it will take appropriate action by either deleting the message outright or sending it to the user’s junk mail folder and disabling potentially dangerous content in the message, such as Internet hyperlinks. This helps protect users even if they are looking at messages in their junk mail folder.

But phishers commonly use both fraudulent e-mail and Web sites to commit their scams. Therefore, in addition to the innovations Microsoft continues to develop for e-mail, the company is enhancing the

Internet browsing and the MSN Search Toolbar experience to help better protect people from fraudulent Web sites and the potential for personal data theft via phishing.

The focus of this white paper is to describe the basic workings of a new capability, the Microsoft® Phishing Filter, that will be included in the upcoming release of Internet Explorer 7 in Windows Vista™ (currently in beta), and is now included in the Microsoft Phishing Filter Add-in for MSN Search Toolbar, giving MSN Search Toolbar users with Windows® XP Service Pack 2 (SP2) the chance to experience this new form of protection. The Microsoft Phishing Filter will not only help provide consumers with a dynamic system of warning and protection against potential phishing attacks, but — more important — it will also benefit legitimate ISPs and Web commerce site developers that want to defend against their brands being “spoofed” to propagate scams while not causing their legitimate outreach to customers to be confusing or misinterpreted by filtering software.

### **Machine and Mind Working Together**

Microsoft Phishing Filter software proactively blocks Web sites and cautions users about both reported and suspected phishing Web sites through the Internet browsing experience with Internet Explorer 7 for Windows XP SP2 and in the next-generation Windows Vista client operating system, formerly code-named “Longhorn.” It is also available to MSN Search Toolbar users who install the new Microsoft Phishing Filter Add-in. Based in part on techniques and key learning from Microsoft’s prior experience in e-mail filtering, the Microsoft Phishing Filter uses a combination of dynamic reputation services from the industry and machine-learning heuristics to help deliver a robust solution to phishing for the browser:

- The Phishing Filter will provide a broad level of anti-phishing capabilities that identify and combat a greater number of potential threats.
- It will deliver a clear and distinctive way for consumers and e-commerce service providers to assess whether a particular Web site is either a reported phishing site or a site that might pose potential problems.
- It will provide ISPs and Web service providers with a mechanism to clarify suspicious or unknown content and rectify any disputes over content or intent.

Because Internet Explorer is the world’s most popular browser, providing this anti-phishing functionality for it will give a broad range of users of Windows access to a powerful set of anti-phishing capabilities and help enable legitimate Web service providers reaffirm the value of their brands. Microsoft hopes that the dynamic protection provided by the Phishing Filter in Internet Explorer 7 and the add-in for MSN Search Toolbar will give customers greater confidence in the security and validity of the e-commerce sites they visit.

## How the Phishing Filter Works in Internet Explorer 7

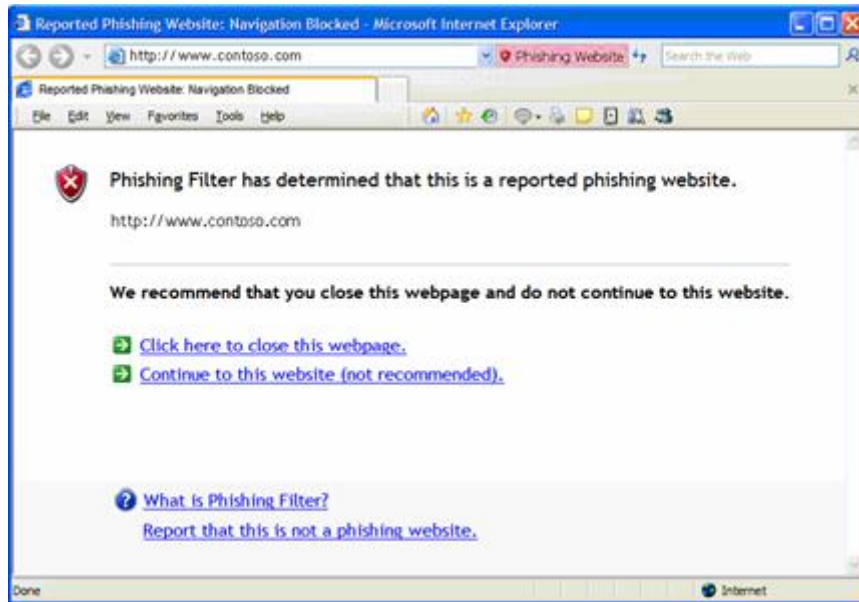
The Microsoft Phishing Filter is integrated into Internet Explorer 7, but stays in the background until a user visits a Web site that looks suspicious. The user must opt in to the feature to activate the dynamic protection it offers with an online reputation service, which is used to verify the sites being visited by consumers. When a user encounters a Web site that looks suspicious, Internet Explorer 7 launches a dialog box asking the user to opt in.

If the automatic option is chosen, by selecting yes, the Phishing Filter will work quietly in the background and will alert users about suspected or reported phishing Web sites through a two-stage warning system as follows:

- **The first level of warning (yellow)** signals to users that if the Phishing Filter detects a Web site which contains characteristics similar to a phishing site, Internet Explorer 7 will display next to the address bar a yellow button labeled “Suspicious Website.” Clicking on the yellow button reveals a warning that users have landed on a suspected phishing Web site and recommends that they avoid entering any personal information on the site.



- **The second level of warning (red)** automatically blocks users from a Web site if it has been confirmed as a reported phishing site and displays a red button labeled “Phishing Website.” When users land on a such a site (based on an online list of sites that are updated several times every hour), Internet Explorer 7 signals the threat level (in red) and automatically navigates them away from that site to a new page. This warning page offers users the option to close the Web page immediately or proceed at their own risk to the site.



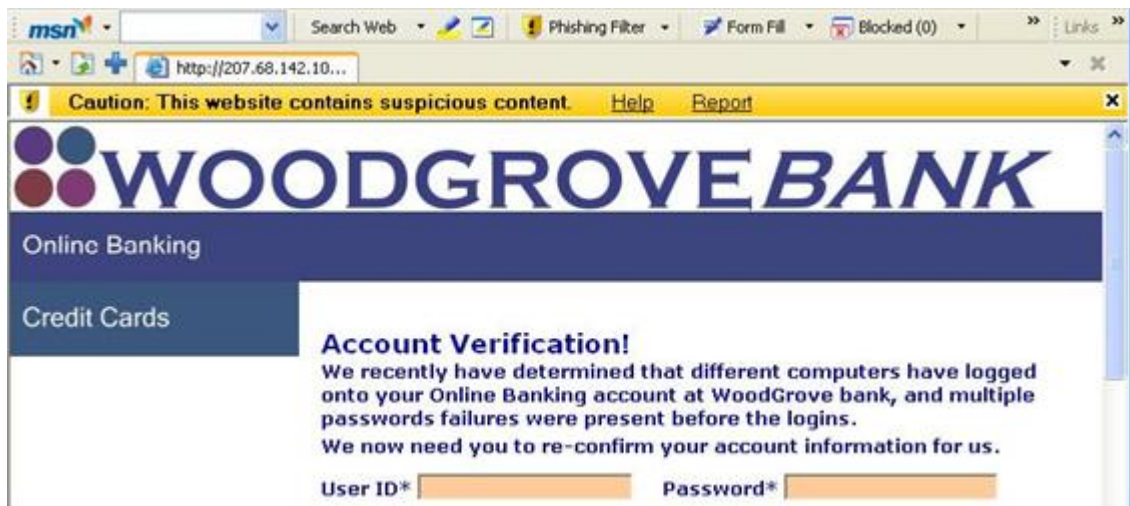
Users can also choose to opt out of Phishing Filter or use it on a case-by-case basis (based on selected Web sites). In the case-by-case scenario, users will see a small shield in the status bar each time they encounter a Web site that needs to be verified further.

### How the Microsoft Phishing Filter Works in MSN Search Toolbar

The Microsoft Phishing Filter capability is integrated into MSN Search Toolbar through an optional add-in for Windows XP SP2 users that can be downloaded from <http://add-ins.msn.com>. It is similar to the experience in Internet Explorer 7 with some slight differences. It is an opt-in experience as well, but users opt-in when they download and install the Microsoft Phishing Filter Add-in for MSN Search Toolbar. This will activate the dynamic protection with the online reputation service, used to verify the Web sites being visited by consumers.

The Microsoft Phishing Filter Add-in for MSN Search Toolbar also warns users in a similar way to Internet Explorer 7, but with subtle differences. It, too, works quietly in the background and alerts users about suspected or reported phishing Web sites through a two-stage warning system:

- **The first level of warning Warn (yellow bar)** signals to users that the Phishing Filter detects a Web site that contains characteristics similar to a phishing site. MSN Search Toolbar will display a yellow warning bar and a yellow Phishing Filter button on the toolbar labeled "Suspicious Website." Users can click the **Help** link for more information and will be informed that the Web site may be legitimate, but they still should not submit any personal or financial data to it unless they are certain it is trustworthy. They can also click the **Report** link in the yellow bar to report it for further analysis and verification.



- **The second level of warning Block (red bar)** automatically blocks MSN Search Toolbar users from a Web site if it has been confirmed as a reported phishing site and displays a red warning bar *“This website has been blocked for your safety.”* When users land on such a site (based on an online list of sites that is updated several times every hour), the Phishing Filter Add-in for MSN Search Toolbar signals the block warning above the Web site (in red) and automatically blocks the ability to enter data on that page.

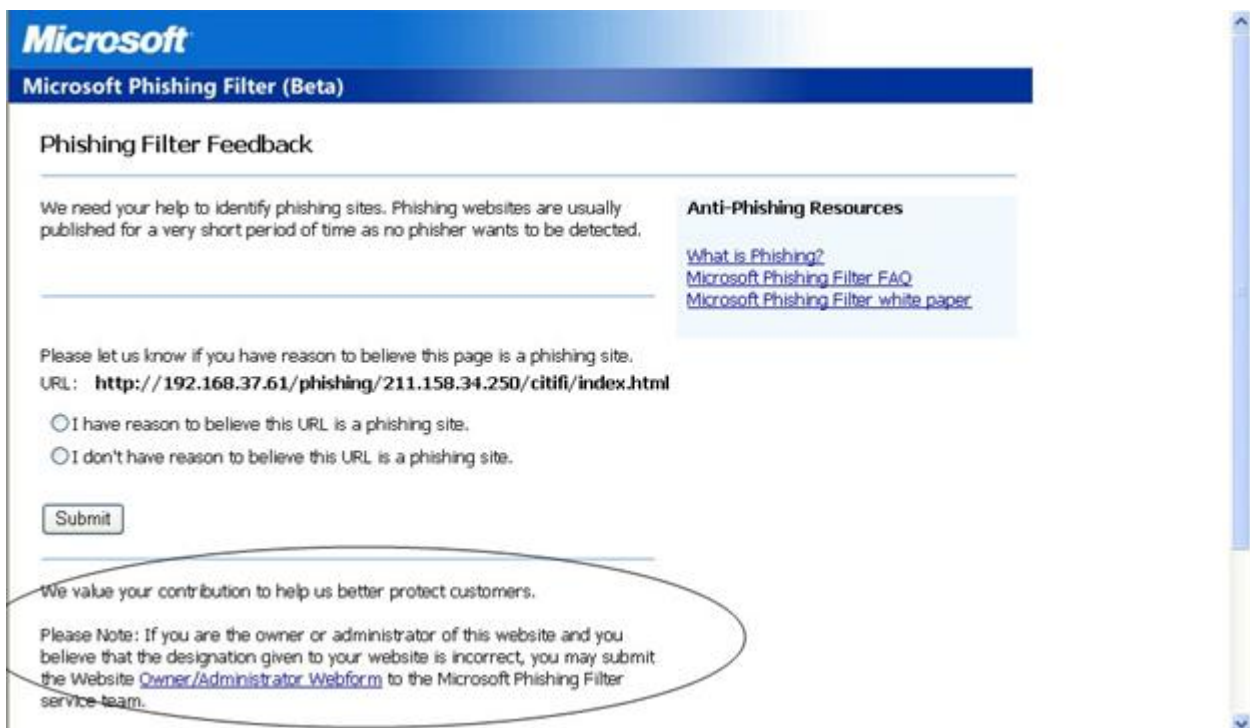


This MSN Search Toolbar experience is slightly different from the Internet Explorer 7 experience, which navigates users away to a warning page, but both offer users the option to proceed at their own risk and unblock access to the Web page.

In both experiences, if a user knows a Web site is not a phishing Web site and it is being blocked, the user can click **Report** in the red bar to report the page as a legitimate site for further analysis and verification by the Microsoft Phishing Filter service.

## Protecting Legitimate Commerce

Because the yellow warning in the MS Phishing Filter reflects a “maybe,” rather than a “proven,” phishing label, Microsoft believes it is vital that any Web service provider whose site falls into that category has a clear and simple path to resolve any questions. Microsoft has built such a path directly into the Microsoft Phishing Filter user interfaces both in Internet Explorer 7 and the add-in for MSN Search Toolbar. Site owners can launch a webform that will prompt them for information about their business and their site. For Internet Explorer 7, this webform can be launched through the Tools à Phishing Filter à “Report This Website” menu options in the browser, or from the UI that comes from pressing the yellow or red button in the UI or from the blocked page itself. This UI is also accessible by right clicking on the status bar on the lower-right corner of the Internet Explorer 7 window. In the MSN Search Toolbar Add-in, the webform is accessible by clicking on the **Report** link in either of the two warning bars or by clicking on the Phishing Filter button on the MSN Search Toolbar itself and selecting **Report This Website**.



**Microsoft**  
Microsoft Phishing Filter (Beta)

### Phishing Filter Feedback

We need your help to identify phishing sites. Phishing websites are usually published for a very short period of time as no phisher wants to be detected.

Please let us know if you have reason to believe this page is a phishing site.  
URL: **http://192.168.37.61/phishing/211.158.34.250/citifi/index.html**

I have reason to believe this URL is a phishing site.  
 I don't have reason to believe this URL is a phishing site.

We value your contribution to help us better protect customers.

Please Note: If you are the owner or administrator of this website and you believe that the designation given to your website is incorrect, you may submit the Website [Owner/Administrator Webform](#) to the Microsoft Phishing Filter service team.

**Anti-Phishing Resources**  
[What is Phishing?](#)  
[Microsoft Phishing Filter FAQ](#)  
[Microsoft Phishing Filter white paper](#)

Once that information is sent, a team of experts at Microsoft will look at the data and decide if there's a genuine mistake on the part of the filter: a false positive. In communicating with the site owner, the team can either move the site into the “clean” category or assign it red-warning status if the initial diagnosis was correct. The overarching goal of this review process is to ensure that every legitimate site owner and Web service provider is able to conduct e-commerce with their customers, with both parties protected against outside phishing attempts.

## Behind the Scenes

As with any potential security issue, smart phishers will continually try new ways to bypass security software in the hope of reaching unsuspecting computer users. To approach the phishing problem in a holistic manner, while continuing to drive to develop technology innovations such as SmartScreen and the Microsoft Phishing Filter, Microsoft will also focus on consumer outreach, industry collaboration and dissemination of best practices.

### ***Consumer Outreach***

Given the social engineering aspect employed in scams such as phishing, technology alone cannot alleviate the problem. Organizations such as Microsoft must continue to help consumers better understand how to protect themselves from online threats and scams, and they must do so in a way that doesn't require consumers to be computer-security experts, but does provide them with enough information to know they should at least exercise the same caution interacting online as they do when meeting strangers on the street. Microsoft and MSN already offer a number of online resources to help educate consumers about online safety issues such as phishing, including <http://safety.msn.com/phishing> and <http://www.microsoft.com/athome/security/email/phishing.msp>. Addressing the issue of phishing directly within the browsing experience, in addition to making other security investments in Internet Explorer 7, should go a long way toward helping raise consumers' confidence that they can help protect themselves online.

### ***Industry Collaboration***

Microsoft continues to work with a number of industry stakeholders to help stop the proliferation of phishing scams. For example, the Microsoft Phishing Filter uses information provided through online anti-phishing aggregation services that provide data to the online reputation service, which is then used to inform the filtering process in Internet Explorer 7. The Microsoft Phishing Filter will use multiple data providers when the service is final. The goal is to have as wide a variety of industry data sources as possible. The data sources for this service will only get richer once new data providers come online over the coming months. In addition, Microsoft is updating its key ISP and Web commerce partners about the Phishing Filter's capabilities and encourages a continuation of data-sharing about proven and potential phishing sites. Microsoft, as an active sponsor and steering-committee member in the Anti-Phishing Working Group, as well as a founding member of Digital PhishNet, will be able to share knowledge gained from the Phishing Filter with broader industry and law-enforcement audiences.

## **Best Practices**

Although there are obviously many aspects of filtering technologies that cannot be publicly disclosed, Microsoft is encouraging legitimate Web service providers (many of which are small businesses without the IT resources of larger providers) to follow some simple rules that can help avoid the “yellow warning button”:

- **Certification.** If Web site owners intend to ask users for personal information, they should have secure sockets layer (SSL) certification.
- **Security.** Legitimate Web site owners should continually make sure their sites are as secure as possible from outside attacks by maintaining up-to-date firewalls and installing all necessary security updates.
- **Cross-site scripting attacks.** All Web site owners should be protecting themselves by using anti-cross-site scripting attack tools.

**External content.** If a Web site intends to post external or third-party content, it is recommended that the content be secure and from a known and trusted source.

## **What's Next**

Microsoft, along with other key technology companies, is committed to helping protect Internet users worldwide against phishing scams, as well as preventing spam and phishing before they begin to impact computer networks. From developing robust detection systems to supporting legislation that assigns severe legal penalties for those who send deceptive and unwanted e-mail, Microsoft realizes the necessity for a broad industry effort to help contain both spam and phishing.

The battle clearly will be ongoing, as purveyors of spam and phishing e-mail will continue to exploit and prey on unsuspecting computer users. With capabilities such as the anti-phishing features in Internet Explorer 7 and the MSN Search Toolbar, Microsoft will continue to work to provide innovative technology solutions that help combat spam and phishing for the benefit of consumers and legitimate e-commerce vendors alike.

#####

The information contained in this document represents the current view of Microsoft Corp. on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of Microsoft.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

© 2005 Microsoft Corp. All rights reserved.

Microsoft, SmartScreen, MSN, Hotmail, Vista and Windows are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

**For more information, press only:**

Rapid Response Team, Waggener Edstrom, (503) 443-7070, [rrt@wagged.com](mailto:rrt@wagged.com)