

Microsoft Phishing Filter Feature in Internet Explorer 7 and Windows Live Toolbar

Privacy Assessment Report

Presented by Jefferson Wells

July 28, 2006

This report is intended to be used in its full and original content. Any use of this information not in its full and original content is prohibited without the express written consent of Jefferson Wells management.

Table of Contents

EXECUTIVE SUMMARY.....	3
OVERALL CONCLUSION.....	4
FUNCTIONAL OVERVIEW	5
ASSESSMENT APPROACH.....	7
SCOPE.....	9
ASSESSMENT RESULTS	10

EXECUTIVE SUMMARY

The following report details the assessment performed on the Microsoft Phishing Filter in Internet Explorer 7 Beta 3 and Windows Live Toolbar including the Phish Detective as delivered with the OneCare Advisor toolbar component. The Windows Live Policy and Privacy Team defined the scope of the engagement and the assertions to be included in the review. Jefferson Wells planned and performed the documentation reviews, interviews of key personnel and testing to validate the technical design and processes related to the identified assertions.

Jefferson Wells delivers professional services in the areas of technology risk management, internal audit, tax and finance and accounting. Jefferson Wells Technology Risk Management group specializes in Information Technology assessments, security assessments, business continuity management and privacy reviews.

The objective of the analysis was to determine the validity of the assertions for the Microsoft Phishing Filter in IE 7 and Windows Live Toolbar including the Phish Detective. The assertions tested were identified as appropriate statements that, when tested and validated, would assess the transmission and/or collection of personal information when using the Phishing Filter feature. Jefferson Wells used the Microsoft definition for personal information in performing the review. The Microsoft Online Privacy Statement definition of personal information, also referred to as personally identifiable information (PII) in this report is:

“Personally Identifiable Information means any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains, or from which identification or contact information of an individual person can be derived. Some examples of PII include first and last name, address, and e-mail address.”

The review consisted of an assessment of the Microsoft Phishing Filter, which was limited to the end-user Windows Live Toolbar OneCare Advisor component for Internet Explorer 6 Phishing Filter and Phish Detective features and Internet Explorer 7 Beta 3 Phishing Filter feature, URL Reputation Web Service, Phish Detective back end service and caution logging.

The following assertions were used by Jefferson Wells in conducting the privacy assessment:

- 1) The Phishing Filter client does not transmit any personally identifiable information without explicit user consent.
- 2) URL information transmitted automatically by the Phishing Filter client cannot be traced back to the user's personal information including IP Address.

- 3) HTTP and HTTPS URLs transmitted for rating by the Phishing Filter client are limited to the domain and path only. All other information in the URL is stripped.
- 4) The Phishing filter client only transmits URLs in the following scenarios.
 - (a) When the user wants to manually provide feedback on a URL.
 - (b) When the URL is not found in the Phishing Filter local dat files.
 - (c) When the Phishing client heuristics determine a site as suspicious.
 - (d) When the Phish Detective is enabled and the feature determines a password has been reused on different websites.
- 5) Transmission of any and all URL information by the Phishing Filter client is over SSL on the Internet.
- 6) When the Phish Detective is turned off, it is not inspecting web pages or transmitting URL's to Microsoft for grading.

For assertion 1, the definition for “explicit user consent” is based on Microsoft’s Privacy Standard for Development, which requires that the user take or have the ability to take an explicit action before data is collected or transferred.

OVERALL CONCLUSION

As of July 28th, 2006 and based on the assertions identified and the testing performed Jefferson Wells found that all assertions were valid. Based on Jefferson Wells testing, the assertions noted have been validated for the versions noted in the “Scope” section of this report. A matrix with the assertions and results by assertion is provided in the “Assessment Results” section of the report.

FUNCTIONAL OVERVIEW

The Microsoft Phishing Filter service, as tested, consists of components installed on the user's local workstation and on Microsoft servers, collectively referred to as the URL Reputation Web Service (URS).

Browser DAT and URL Local Cache

When a user enters a web address in the Browser Technology, (Internet Explorer 7 or Internet Explorer 6 with the Windows Live Toolbar and OneCare Advisor component including Phishing Filter, the Phishing Filter first checks the local .DAT file and cache for a match to a previously rated site. The URL to be checked is limited to the domain and path (i.e. http://domain.com/path) with the query string data removed. If a match is identified, the user either continues to the site, is presented a "warn experience", or is presented a "block experience" based on the matched site's rating. If a match is not identified, the Phishing Filter contacts the URS to identify a rating for the attempted URL.

URL Reputation Web Server

When the Browser DAT file and URL Local Cache do not contain the ratings for the URL, the client attempts to match the stripped URL to a list of rated URLs stored on the URL Reputation Web Server hosted by MSN. If a URS match is identified, the user either continues to the site, is presented a "warn experience", or is presented a "block experience" based on the on the matched site's rating provided by the URS. If a match is not identified, the URS returns a rating of "Unknown" to the Phishing Filter.

Heuristic Analysis and URL Verification

After the content is loaded on the client, the page is subjected to a heuristic analysis by the Phishing Filter. If the heuristic analysis determines that the website may be a Phishing site, also known as a caution, the Phishing Filter connects with the URS to identify if a match exists with the stripped URL to determine the rating of the currently loaded site, which may be different than the originally matched URL. Based on the heuristic analysis and the URL verification, the user is either presented a "warn experience", presented a "block experience", or continues as normal depending on the rating returned by the Phishing Filter.

Caution Logging

A process for logging all caution events of suspected phishing sites displayed to the user in Internet Explorer 7 and the Windows Live Toolbar Phishing Filter component to help identify phishing sites earlier and to help identify and mitigate falsely identified phishing sites.

Feedback Functionality

The Phishing Filter service also includes the ability to provide manual feedback on websites, to Microsoft, for review and rating to include in the URL Reputation Web Service. There are two functions within the feedback process:

1. A user can provide feedback to Microsoft on a site that they believe is or is not a phishing site.
2. A user, identifying themselves as a site owner or representative of the website, can also provide feedback on the website and is required to enter information to assist Microsoft with verifying ownership or representation of the website and communicate with while researching the validity of the feedback.

Phish Detective

A data collection system that sends the web addresses (*Uniform Resource Locator - URL*) of suspected phishing websites to Microsoft. When an end-user enters a password on a website, the Phishing Filter encrypts and stores it securely on your computer. When Phish Detective determines that you have reused a password on a different website, the addresses of both sites are sent to Microsoft to help identify fraudulent sites that are disguised as legitimate sites.

ASSESSMENT APPROACH

Jefferson Wells Technology Risk Management consultants followed a three-phase assessment approach to analyze the validity of Microsoft's privacy assertions. The phases included; Discovery, Validation of Assertions and Testing.

1. Discovery

Jefferson Wells conducted interviews with key Microsoft personnel to gain an understanding of the architecture, operational scope and privacy issues related to the Phishing Filter solution. Follow up interview and document requests were initiated from these initial interviews.

2. Validation of Assertions

Once a solid base of understanding was established, Jefferson Wells reviewed the original assertions with a focus on customer privacy and the published "Microsoft Online Privacy Statement". Jefferson Wells provided recommendations to Microsoft to alter the language of the assertions to be focused on the privacy of personal information and limit the testing to privacy related issues.

3. Testing

Jefferson Wells developed formal test plans in order to create a repeatable process to execute the testing. The formal test plans should also provide individuals, not directly involved in the testing, an understanding of the methodology used to validate the assertions and recreate the results assuming there have been no changes to the product since Jefferson Wells testing was completed. Jefferson Wells testing methods included:

1. Observing the behavior of the product under specified conditions
2. Collecting screen shots of evidentiary data
3. Extracting test data with Microsoft-provided test tools
4. Capturing and analyzing packets with a network "sniffer" while navigating to specified test URLs in a simulated end-user environment.

Testing by use of capturing and analyzing packets was executed on non-Microsoft owned equipment and networks. The testing was designed to closely mirror a typical end user's broadband environment. Test hard drives were formatted and clean installs of Microsoft Windows XP Professional with all service packs were completed prior to testing and when switching between Internet Explorer 6 with Windows Live Toolbar and Phishing Filter feature and Internet Explorer 7.

During the execution of the test plans, Jefferson Wells collected and cross referenced the appropriate evidence to the control matrices in order to determine the validity of the assertions included in this assessment.

SCOPE

Jefferson Wells' scope was to validate the following management assertions as determined by the Windows Live Policy and Privacy Team:

1. The Phishing Filter client does not transmit any personally identifiable information without explicit user consent.
2. URL information transmitted for rating by the Phishing Filter client cannot be traced back to the user's personal information including IP Address.
3. HTTP and HTTPS URLs transmitted for rating by the Phishing Filter client are limited to the domain and path only. All other information in the URL is stripped.
4. The Phishing filter client only transmits URLs in the following scenarios:
 - a. When the user wants to manually provide feedback on a URL.
 - b. When the URL is not found in the Phishing Filter local data files.
 - c. When the Phishing Filter client heuristics determine a site as suspicious.
 - d. When the Phish Detective is enabled and the feature determines a password has been reused on different websites.
5. Transmission of any and all URL information by the Phishing Filter Client is over SSL on the Internet.
6. When the Phish Detective is turned off, it is not inspecting web pages or transmitting URL's to Microsoft for Grading.

In order to complete the assessment, the Jefferson Wells review consisted of an evaluation of the Phishing Filter Service from the end-user client to the termination at the URS Web Service. The following areas were evaluated:

1. The client workstation with Internet Explorer 6 with Windows Live Toolbar and Phishing Filter and Phish Detective feature version 4.0.6613.0 as delivered with the OneCare Advisor toolbar component
2. The client workstation Internet Explorer 7 Beta 3 version 7.0.5450.4
3. URL Reputation Service and Network Topology Maps from MSN Networking
4. Phish Detective servers
5. Phishing Filter caution logging server feature

ASSESSMENT RESULTS

The assessment results that were subject to the testing of the following Phishing Filter features for all six assertions noted below. The components included:

1. The client workstation with Internet Explorer 6 with Windows Live Toolbar and Phishing Filter and Phish Detective feature version 4.0.6613.0 version as delivered with the OneCare Advisor toolbar component
2. The client workstation Internet Explorer 7 Beta 3 version 7.0.5450.4
3. URL Reputation Service and Network Topology Maps from MSN Networking
4. Phish Detective servers
5. Phishing Filter caution logging server feature

Assertion	Valid	Not valid
1) The Phishing Filter client does not transmit any personally identifiable information without explicit user consent.	X	
2) URL information transmitted for rating by the Phishing Filter client cannot be traced back to the user's personal information.	X	
3) HTTP and HTTPS URLs transmitted for rating by the Phishing Filter are limited to the domain and path only. All other information in the URL is stripped.	X	
4) The Phishing Filter client only transmits URLs in the following scenarios. <ol style="list-style-type: none"> a) When the user wants to manually provide feedback on a URL. b) When the URL is not found in the end users Phishing Filter local data files. c) When the Phishing Filter client heuristics determine a site as suspicious. d) When the Phish Detective is enabled and the feature determines a password has been reused on different websites. 	X	
5) Transmission of any and all URL information by the Phishing Filter Client is over SSL on the Internet.	X	
6) When the Phish Detective is turned off, it is not inspecting web pages or transmitting URL's to Microsoft for Grading.	X	