Владимир БЕЗМАЛЫЙ

Антифишинг: ответный удар. Часть 1. Браузеры на страже

Сегодня сложно найти активного пользователя Интернета, который ни разу не слышал бы о фишинговых письмах и атаках. Как правило, такими хитростями мошенники завлекают жертву на фальшивый сайт для сбора информации (личные данные, сведения о платежной карте и т.д.) с целью последующего незаконного ее использования. К сожалению, подобные киберпреступления вряд ли будут пресечены в ближайшие годы.

Но существует ряд инструментов для борьбы с упомянутой напастью. О некоторых из них я и расскажу в предлагаемой вашему вниманию статье.

Что такое фишинг?

Об этом уже было сказано немало (например, см. статью «Фишинг, вишинг, фарминг...», «Мир ПК», №12/06, с. 82). Напомню, что фишинг (phishing) — вид интернет-мошенничества, заключающийся в рассылке электронных сообщений с целью кражи конфиденциальной информации (как правило, финансового характера). Фишинг-сообщения составляются таким образом, чтобы максимально походить на информационные письма от банковских структур или компаний с известными брендами. Письма содержат ссылку на заведомо ложный веб-ресурс, специально подготовленный злоумышленниками и являющийся копией сайта организации, от имени которой отправлено письмо. На данном фальшивом сайте пользователю предлагается ввести, например, номер своей кредитной карты и другую конфиденциальную информацию.

Антифишинговый фильтр в Internet Explorer 7

В IE 7 антифишинговый фильтр включает следующие технологии:

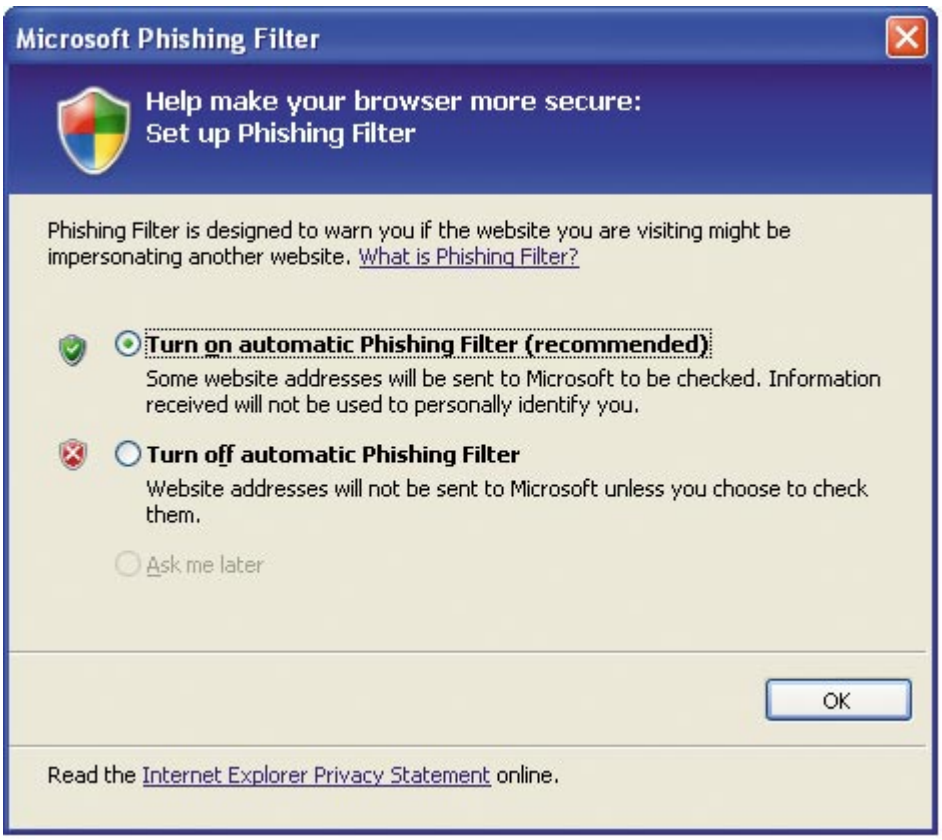
- Встроенный фильтр. Проводит сканирование посещаемых веб-страниц в поисках признаков, характерных для мошеннических узлов или фишинг-атак. Если пользователь загружает такую страницу, то получает предупреждение.

- Интерактивная служба. Содержит обновляемую информацию о «вредных» узлах. Очень часто фишинг-узлы появляются на срок 24—48 ч, поэтому чрезвычайно важным является процесс своевременного обновления.

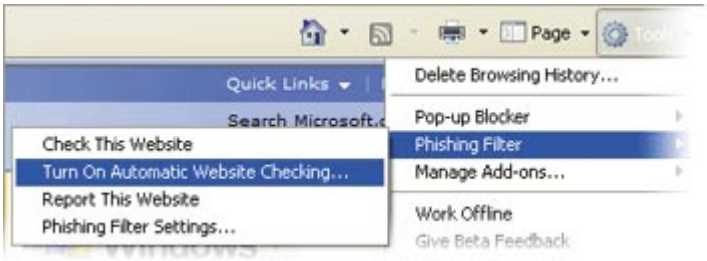
Встроенное средство (антифишинговый фильтр) позволяет получать предупреждение о подозрительных узлах. При этом пользователь может сам передать сведения о любом потенциально опасном узле в корпорацию Microsoft для последующей проверки. Затем подтвержденная информация добавляется в соответствующую базу данных для защиты компьютеров, использующих Internet Explorer с панелью управления Windows Live.

В настоящий момент функция антифишингового фильтра доступна в обозревателе Internet Explorer для ОС Windows XP SP2 и Windows Vista. Кроме того, она имеется в новой панели инструментов Windows Live (http://toolbar.live.com) для Internet Explorer 6 или старше.

Как воспользоваться защитными возможностями? После загрузки и установки Internet Explorer 7 можно включить функцию антифишинга.



Если при установке IE 7 вы не активировали данную защиту, то сможете сделать это позже. Для этого в меню Tools (Сервис) обозревателя IE 7 выберите пункт Phishing Filter (Антифишинг).



Фильтр распознает два типа «нехороших» узлов:

- веб-узлы, подозреваемые в атаках;
- веб-узлы, на которых фишинг-атаки уже происходили.

При посещении узла, подозреваемого в фишинг-атаках, фильтр выдает предупреждение в виде щита желтого цвета.

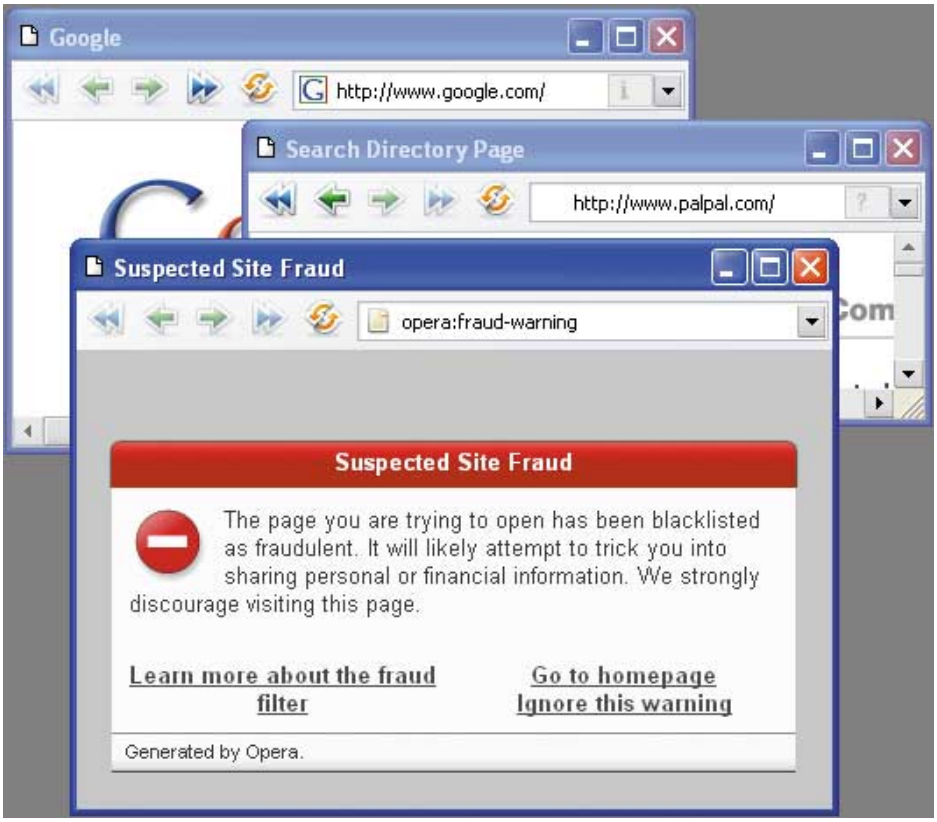
При попытке посетить веб-узел, на котором предпринимались атаки, фильтр выдает щит-предупреждение красного цвета и прекращает доступ к этому узлу. Ввод любых данных в любую форму на этом узле далее невозможен.

Можно настроить фишинг-фильтр на панели инструментов Windows Live.

После инсталяции новой панели инструментов Windows Live установите кнопку OneCare Advisor. Функция антифишинга при этом начинает работу аналогично IE 7.

Защита от фишинга в Opera 9.10

Защита от фишинга в Opera будет организована несколько по-иному, нежели в Firefox и IE. В Opera, когда вы набираете URL в адресной строке, браузер будет одновременно делать запрос к онлайновой базе данных Opera Software — для проверки легитимности сайта, который вы хотите посетить. Если сайт будет определен как подставной, пользователь увидит соответствующее предупреждение.



Впрочем, у пользователя остается возможность посетить данный сайт, если ему это действительно нужно.

В отличие от Firefox, который сличает адрес с хранящимися на ПК сведениями, Opera делает проверку в режиме реального времени, сверяясь с постоянно обновляемой базой. Это представляется мне более эффективным, так как фишинговые сайты-однодневки появляются внезапно и очень быстро исчезают. Opera получает данные о легитимности сайта из антифишинговой базы от компании GeoTrust (http://www.geotrust.com), которая специализируется на защите от мошенничества подобного рода.

* * *

Хочу заметить, что на самом деле проблема фишинга вряд ли когда-нибудь будет решена исключительно техническими средствами. Поэтому призываю всех читателей сто раз подумать, прежде чем реагировать на письма, в которых вас просят использовать какие-либо персональные данные. Кроме встроенных в браузеры методов антифишинговой защиты есть и другие, более серьезные, например одноразовые пароли. Но об этом — в следующей статье.

Об авторе

Владимир Федорович Безмалый — MVP, руководитель программы подготовки администраторов информационной безопасности Академии БМС Консалтинг, e-mail: Vladimir_Bezmaly@ec.bms-consulting.com.