Защищаемся от фишинга

Введение

Фишинговая атака - стандартная форма атаки, используемой киберпреступниками, чтобы одурачить пользователей, раскрыть чувствительные персональные данные или финансовую информацию, включая учетные данные. Как правило, каждую неделю появляются несколько новых фишинговых атак, предназначающихся для пользователей Интернет. Поэтому для онлайновых пользователей необходимо понять, что такое фишинговая атака и как лучше всего защититься от таких атак.

Что такое фишинговая атака?

Фишинговая атака включает использование веб-сайта, созданного злоумышленниками, похожего на веб-сайты известных организаций, такие как финансовые или правительственные учреждения и имеет целью мошенничество или кражу персональных данных жертвы. У фишинговой атаки есть два основных этапа:

- **Phishing-атака с использованием электронной почты**: атакующий посылает спам (письмо по электронной почте) тысячам адресов электронной почты, симулируя подлинное письмо от законной организации. Электронное письмо составлено таким образом, чтобы убедить пользователя щелкнуть по ссылке в нем. Если пользователь щелкнет по ссылке, то компьютер пользователя соединится с фишинговым веб-сайтом.
- **Phishing веб-сайт:** phishing веб-сайт создается, чтобы содержать поля, информация в которые будет вводиться пользователем (такие как имя пользователя и пароль). Если пользователь заполнит эти поля, информация будет получена атакующим. Если преступники в состоянии убедить пользователя, что их электронная почта и веб-сайт законны, они могут обмануть пользователей для получения имен и паролей (или другой уязвимой информации).

1. Лучший способ не стать жертвой фишинговой атаки состоит в том, чтобы обнаружить и/или блокировать phishing сообщения электронной почты (первая стадия атаки).
    1.1. Используйте антиспамовый фильтр, чтобы блокировать электронную почту, содержащую спам.
        1.1.1. Фишинговые атаки обычно полагаются на пользователя, получающего и щелкающего по ссылке в фишинговом сообщении электронной почты. Блокируя и фильтруя электронную почту, содержащую спам, пользователи, с меньшей вероятностью, будут читать, доверять или щелкать по таким ссылкам, особенно, если сообщение будет блокировано или отмечено как подозрительное спам-фильтром.
    1.2.Измените настройки своего программного обеспечения, чтобы получать предупреждение, в случае если получаемое письмо может быть отнесено к категории спам.

1.2.1. Спам-фильтры, хотя очень полезны и настоятельно рекомендованы, все же не всегда эффективны и некоторое количество спама все еще может быть доставлено в ваш ящик.

2. Обнаружение phishing веб-сайта может быть сделано одним из двух способов. Вместе с тем необходимо учесть, что ни один способ не является абсолютно надеженым, следовательно, рекомендуется, чтобы использовались оба для получения лучших результатов.
   2.1. Пользователи могут сконфигурировать свой веб-браузер, чтобы помочь обнаружить phishing сайты. Учтите, **всегда есть задержка между тем, когда вышла новая атака и когда обновлены технологии, чтобы обнаружить новую атаку.**
3. В современных браузерах, есть опции, которые могут быть активированы, чтобы помочь обнаружить фишинговые веб-сайты. Включение этих функций вряд ли окажет значимое влияние на скорость Интернет-соединения.

Что сделать, если вы встречаетесь с phishing электронной почтой или веб-сайтом.

Если Вы получаете фишинговое письмо, просто удалите его. Не отвечайте на адрес электронной почты и не щелкайте по ссылкам в нем.

Распознавание phishing электронных писем и веб-сайтов.

Технологии безопасности, описанные выше, очень полезны, чтобы помочь пользователям защитить себя от фишинговых атак. Однако в случае если не сработали по какой-то причине технологии безопасности, необходимо пользователю включить свой здравый смысл, чтобы не быть обманутым. В данном разделе попробуем описать некоторые из характеристик фишинговых сообщение и веб-сайтов, которые помогут распознать их, не полагаясь на технологии. Несмотря на обилие различных примеров фишинговых писем и веб-сайтов, у всех них есть общие характеристики.

Фишинговые электронные письма обычно содержат следующие характеристики:

- Сообщение электронной почты подразумевает, что оно написано известной организацией
- Доменное имя поля "От" сообщения электронной почты, возможно, не противоречит доменному имени законной организации. Некоторые фишинговые электронные письма изменяют поле "От" и вставляют доменное имя, принадлежащее законной организации. Следовательно, только просмотр поля "От" не всегда дает уверенность, что это мошенническое сообщение.
- Текст сообщения включает ссылку на сайт
- Цель сообщения электронной почты состоит в том, чтобы заинтересовать читателя щелкнуть по ссылке и войти в систему или ввести другие персональные данные.

У фишинговых веб-сайтов обычно бывают следующие характеристики:

- Веб-сайт похож на веб-сайт известной организации

- Некоторые поля на веб-странице, возможно, будут отличаться от страницы реального сайта. URL (в адресной панели) отличается от URL законной организации. В адресной строке обычно не используется https, в то время как обычно использовалось бы для страницы входа в систему (вместо этого используется http), недопустимый цифровой сертификат или самоподписанный цифровой сертификат.

Примеры фишинговых писем содержатся в архиве рабочей группы Anti-Phishing: http://www.antiphishing.org/phishing archive/phishing archive.html
В данной статье мы с вами рассмотрим возможные варианты фишинговых фильтров и протестируем их на коллекции фишинговых ссылок

Тест антифишинговых фильтров

Несмотря на то, что Internet Explorer 9.0 показывает прекрасные результаты в борьбе с фишингом и вредоносными ссылками, все же многие сегодня используют и другие браузеры, да и Internet Explorer более младших версий все еще не редкость. Как быть в этом случае?
В этом случае вам на помощь могут прийти программы-плагины, которые выполняют те же функции антифишинговых фильтров или антивирусное ПО, в котором реализованы подобные функции.
Протестируем некоторые из программ, выполняющих подобные функции.
Тест проводился на ПК HP G72.
В ходе теста был создан образ ОС Windows 7 SP1 Ultimate Rus. По окончании тестирования каждого продукта проводилось восстановление системы из образа.
Тестовая коллекция включает 31 вредоносную ссылку.
В тесте принимали участие Internet Explorer 9.0, Firefox 4.01, Google Chrome 12.0.742.100, Opera 11.11, Safari 5.
Для создания равных условий встроенные антифишинговые фильтры в браузерах были отключены.

WOT

Аспиранты Timo Ala-Kleemola и Sami Tolvanen начали разрабатывать первую версию, WOT в начале ноября 2005.
С 2007 процветающее WOT сообщество дало оценки репутации более чем 25 миллионам сайтов. Данный продукт был рекомендован PC World, The Kim Komando Show, PC Welt, CNET и многими другими.
Данный продукт представляет собой сервис репутаций. Для данного сервиса существуют версии под Internet Explorer, Firefox, Google Chrome, Opers и Safari.
Результат тестирования приведен в таблице 1
Табл 1 Тестирование WOT

Internet Explorer 9.0	Firefox 4.01	Google Chrome 12.0.742.100	Opera 11.11	Safari 5
67.74%	61,29%	58,06%	54,84%	48,39%

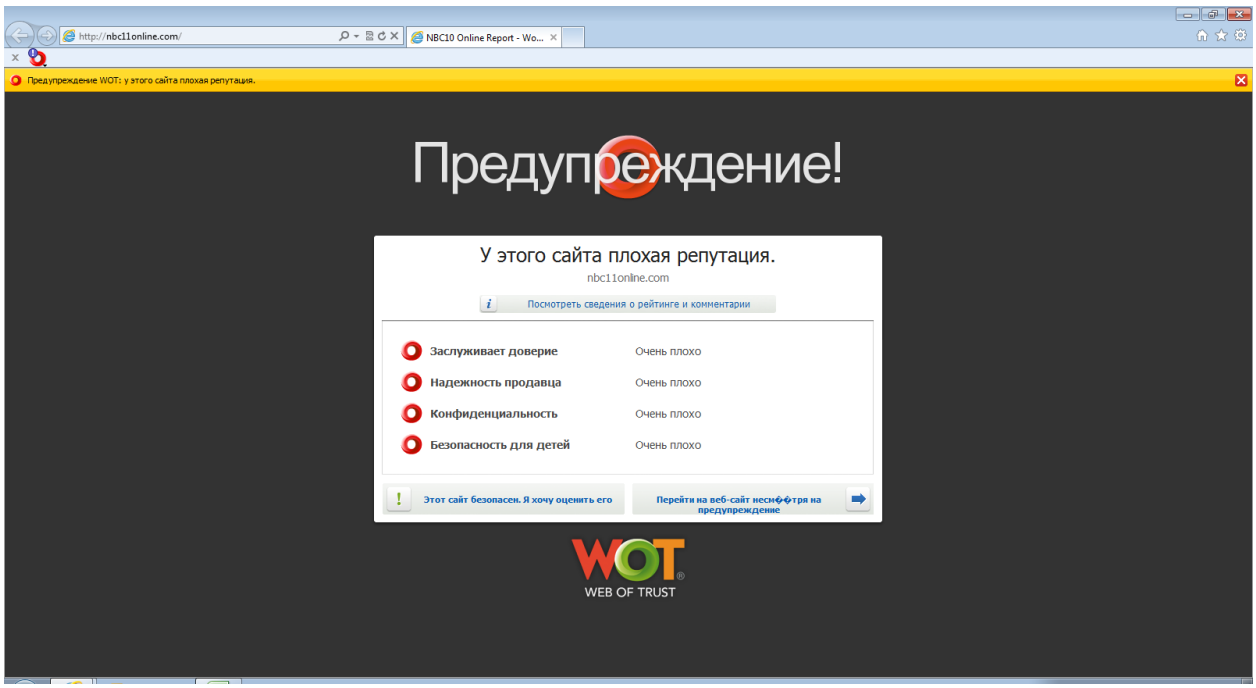

Рисунок 1 Срабатывание предупреждения WOT в Internet Explorer 9.0

McAfee SiteAdvisor

Решения McAfee SiteAdvisor Enterprise — надежный друг, который защитит вас во время работы в Интернете, не мешая ей.

Легкое выявление угроз. Благодаря наглядной системе с цветовым кодированием решения SiteAdvisor Enterprise предоставляют дополнительный уровень защиты на персональном компьютере. Чтобы получить дополнительную информацию по оцененному сайту, щелкните кнопку SiteAdvisor Enterprise в обозревателе или в сообщении, которое появляется, когда вы наводите курсор на результат поиска. Вы узнаете о тестах электронной почты, тестах загрузок, ссылках, связанных веб-сайтах и навязчивых действиях.

Непрерывный анализ Интернета. SiteAdvisor Enterprise непрерывно исследует Интернет с помощью интеллектуальных роботов или виртуальных компьютеров, которые загружают сайты и сканируют их на предмет вредоносных программ. Роботы даже заполняют регистрационные формы, чтобы определить, приводит ли регистрация к отправке нежелательной почты. Если сайт содержит вредоносный код или другую подозрительную активность, решения SiteAdvisor отмечает сайт «красным» как рискованный.

McAfee Global Threat Intelligence (GTI) — это комплексная «облачная» служба сбора сведений об угрозах. Уже интегрированная в продукты безопасности McAfee, она круглосуточно работает в реальном времени, чтобы защитить клиентов от киберугроз по всем направлениям, включая файлы, Интернет, сообщения и сеть. McAfee GTI предлагает самый широкий диапазон данных об угрозах, наиболее надежную корреляцию данных и наиболее комплексную в отрасли интеграцию продуктов. Сеть GTI компании McAfee позволяет поддерживаемым продуктам оценивать угрозы в реальном времени по нескольким направлениям, что ускоряет процесс выявления угроз и улучшает коэффициент перехвата. SiteAdvisor использует службу оценки веб-репутаций и службу веб-категоризации McAfee GTI для выявления сайтов, которые используются вредоносными программами, заражены ими и имеют неприемлемое содержимое.

Внимание! *Данный продукт может быть использован только с браузерами Internet Explorer и Firefox*

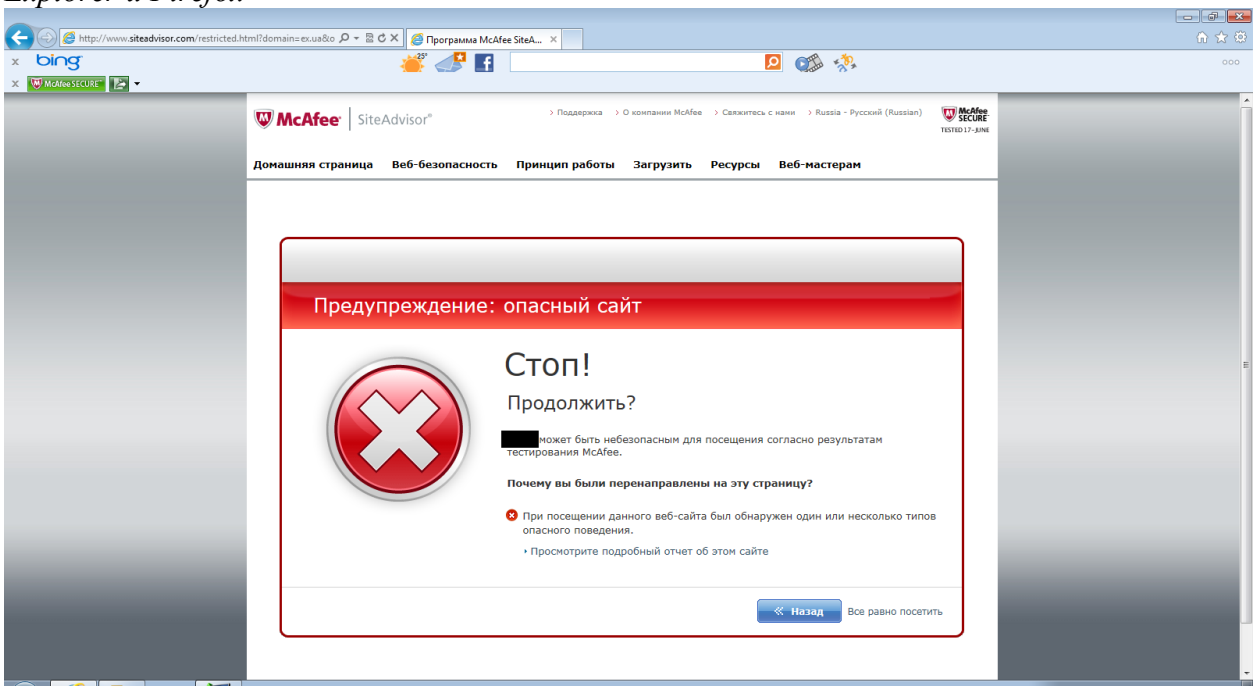

Рисунок 2 Предупреждение: Опасный сайт!

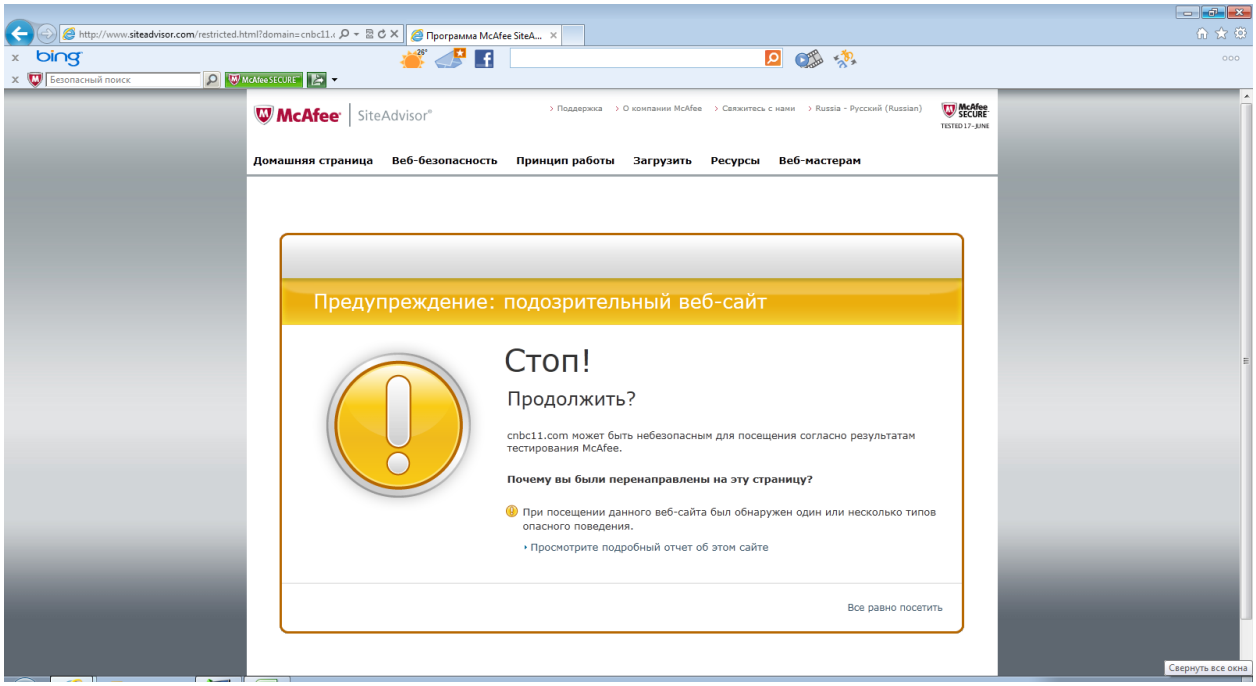

Рисунок 3 Предупреждение: подозрительный веб-сайт

Таблица 2Результат тестирования

Internet Explorer 9.0	Firefox 4.01
58.06%	58.06%

AVG LinkScanner Free

Данный продукт предназначен для защиты в режиме реального времени от интернет-угроз, таких как взломанные или зараженные веб-страницы.

Обеспечивается:

- Защита до перехода на зараженную веб-страницу
- Понятные рейтинги безопасности для результатов поиска в Google, MSN и Yahoo
- Совместимость с наиболее популярными продуктами для антивирусной защиты и обеспечения безопасности
- Анализ страниц, а не сайтов, благодаря чему не осуществляется блокировка всего сайта, если он содержит одну зараженную страницу
- Проверка веб-страниц в наиболее важный момент — в реальном времени перед переходом по ссылке
- Быстрая и простая установка и использование — малая нагрузка на системные ресурсы

Компонент LinkScanner встраивается в виде плагина **AVG Security Toolbar** в браузеры Internet Explorer или Mozilla Firefox.

Дополнительно http://free.avg.com/ru-ru/faq#ixzz1PtYHL1Pw

Таблица 3. Результат тестирования

Internet Explorer 9.0	Firefox 4.01
9,68%	9,68%

Panda Security Toolbar

Данный продукт (http://www.pandasecurity.com/toolbar/PandaSecurityToolbar.exe) представляет собой панель встраиваемую в браузеры Internet Explorer и Mozilla Firefox.

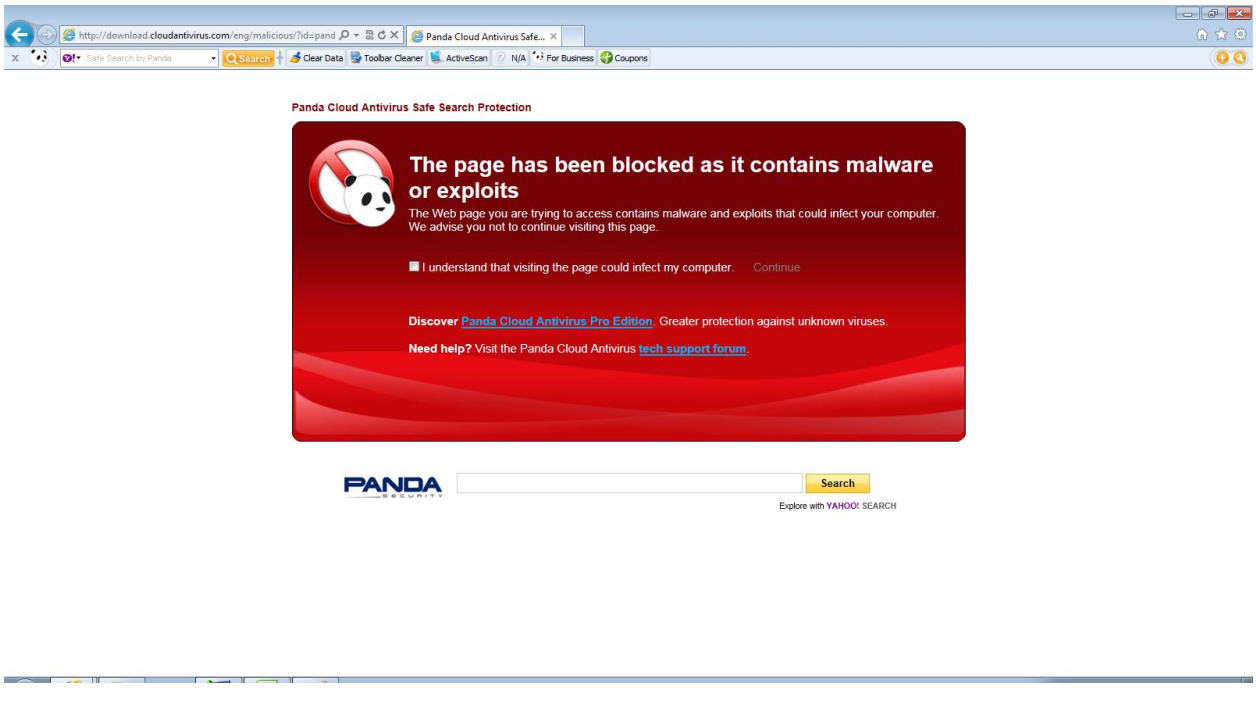

Рисунок 4 Предупреждение о вредоносном сайте

Таблица 4. Результат тестирования

Internet Explorer 9.0	Firefox 4.01
22.58%	16.13%

GData CloudSecurity

Компания G Data представила бесплатный плагин для браузеров G Data CloudSecurity, который блокирует фишинг-сайты или интернет-сайты, зараженные вредоносным кодом. Плагин работает с браузерами Mozilla Firefox, Internet Explorer.

С 4 апреля 2011 G Data CloudSecurity можно загрузить с веб-сайта компании G Data (http://www.free-cloudsecurity.com)

G Data CloudSecurity блокирует опасные интернет-сайты, предотвращая опасность заражения. Плагин совместим с любым антивирусным решением, и начинает работать сразу после установки. Данная программа не требует обновлений. С помощью плагина пользователи могут отправлять URL подозрительных сайтов в лабораторию. Эксперты лаборатории безопасности G Data проверяют их и добавляют в облако полученную информацию.

Рисунок 5 Вредоносный сайт

Таблица 5

Internet Explorer 9.0	Firefox 4.01
29.03%	29.03%

Avira Premium Security Suite

Данный продукт предназначен для защиты вашего ПК от вирусов, вредоносного и шпионского ПО и другого нежелательногоПО. В состав продукта входит и модуль по защите от фишинга.

Таблица 6

Internet Explorer 9.0	Firefox 4.01	Google Chrome 12.0.742.100	Opera 11.11	Safari 5
48,39%	48,39%	48,39%	48,39%	48,39%

Kaspersky Internet Security 2012

Данный продукт поступит на российский рынок в конце лета 2011 года, потому в тесте рассматривается англоязычная версия, продаваемая в Европе.

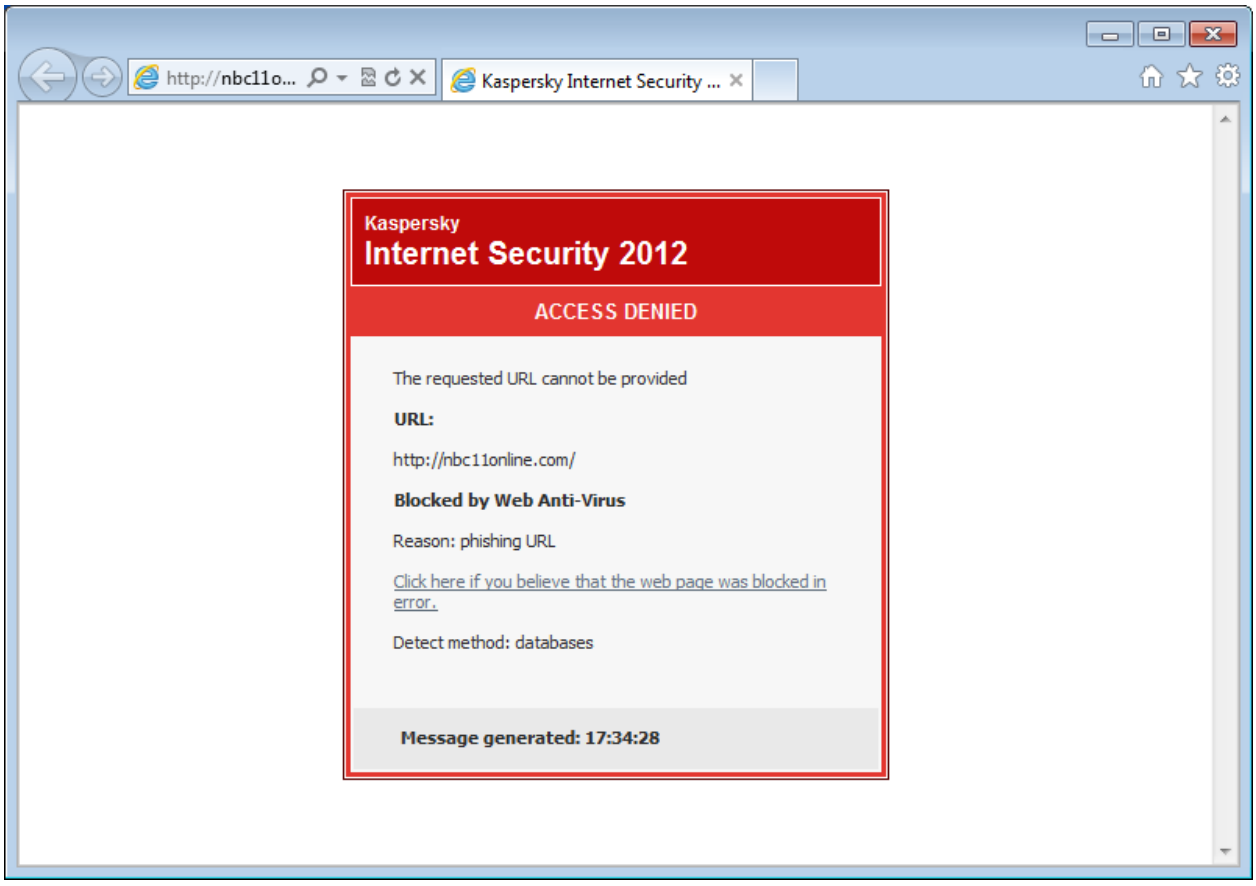

Рисунок 6 Блокирование вредоносного сайта

Результаты тестирования приведены в Таблице 7.

Таблица 7

Internet Explorer 9.0	Firefox 4.01	Google Chrome 12.0.742.100	Opera 11.11	Safari 5
96,77%	96,77	96,77	96,77	96,77

Kaspersky Internet Security 2011

Таблица 8

Internet Explorer 9.0	Firefox 4.01	Google Chrome 12.0.742.100	Opera 11.11	Safari 5
93,55%	93,55%	93,55%	93,55%	93,55%

Заключение

Исходя из результатов тестирования можно сделать два весьма интересных вывода:

1. Производители антифишинговых фильтров (плагинов) предпочитают сосредотачивать свои усилия на поддержке Internet Explorer и Firefox. Это вызывает удивление, так как с выходом Internet Explorer 9.0 пользователи данного браузера и так оказываются в выигрышном положении по сравнению с другими. IE9 блокирует в 2-3 раза больше, чем любой другой браузер.
2. Сравнивая антифишинговое ПО между собой несложно заметить большой отрыв антифишинговых фильтров, входящих в состав антивирусных продуктов.

Итого можно сделать вывод. На сегодняшний день наиболее предпочитаемая следующая связка – Internet Explorer 9.0 и Kaspersky Internet Security (2011, а после выхода новой версии 2012).