Защита интернет-банкинга

Нашу жизнь сегодня уже сложно себе представить без Интернета. В частности, использования Сети для осуществления электронных платежей

Владимир Безмалый

В последнее время российские пользователи все активнее осваивают покупки в Интернете и все чаще пользуются системами онлайн-банкинга. По данным «Лаборатории Касперского», на сегодня 53% российских интернет-пользователей совершают покупки онлайн и 35% удаленно работают с банковскими счетами. Это означает, что в будущем нас ждет еще больше «банковских» троянцев и попыток кражи финансовой информации.

Уже сейчас пользователи довольно часто сталкиваются с киберугрозами при осуществлении онлайн-транзакций. Так, 26% респондентов признались, что в результате открытия почтового вложения их компьютер был инфицирован, а 11% вводили личные или финансовые данные на подозрительных веб-страницах. Даже соблюдая все правила интернет-безопасности, далеко не всегда достаточно полагаться на собственные силы, лучше использовать специальные защитные технологии.

Однако стоит отметить, что далеко не все пользователи услуг интернет-банкинга представляют себе уровень угроз, с которыми они могут столкнуться. Перечислим правила, которые рекомендуется соблюдать пользователям при совершении интернет-платежей и управлении своими средствами.

1. Используйте лицензионное программное обеспечение, полученное из надежных источников. Помните о том, что нелицензионное программное обеспечение и программы, загруженные из сомнительных источников, могут содержать вредоносные компоненты, специально сформированные закладки и т. д., предназначенные для хищения ваших паролей и номеров карт.
2. Регулярно обновляйте программное обеспечение. Помните, что в обновлении нуждается не только операционная система и офисные программы, а вообще все прикладное программное обеспечение, установленное на вашем компьютере. Для обновления операционной системы и других продуктов Microsoft используйте режим автоматического обновления. Для обновления стороннего клиентского программного обеспечения можно, например, использовать продукт компании Secunia — Personal Software Inspector. Эту бесплатную программу можно загрузить по адресу http://secunia.com/vulnerability_scanning/personal/.

ИЛЛЮСТРАЦИЯ ©DAVIDEVISON — FOTOLIA.COM

3. Для защиты своего компьютера используйте антивирус и сетевой экран, а также средства, предоставляемые операционной системой. Не забудьте установить пароль на вашу учетную запись. По информации европейских банков, до 90% случаев нанесения ущерба вызваны внедрением троянцев. Поэтому не забывайте вовремя обновлять антивирусное программное обеспечение!
4. Используйте защищенное соединение. При использовании общедоступных сетей необходимо применять SSL-соединение.
5. Проверяйте подлинность банковской интернет-страницы.
6. Выбирайте для аутентификации сложные пароли либо используйте системы многофакторной аутентификации.
7. Контролируйте операции, производимые по вашему счету
8. Будьте внимательны! Не реагируйте на фишинговые письма.

Однако, даже если вы и будете выполнять все эти рекомендации, дополнительные технические средства защиты не помешают. Ведь всего за первые месяцы 2012 года «Лаборатория Касперского» обнаружила более 15 тыс. новых троянцев, нацеленных на кражу банковских данных. География их распространения охватывает практически весь мир, наиболее «популярными» странами являются Россия, Бразилия и Китай. На фоне общего количества угроз 15 тыс. — это не очень много, но для того, чтобы потерять все деньги на банковском счете, достаточно одного случая заражения.

Следует учесть, что банки и другие финансовые организации не меньше своих клиентов заинтересованы в сохранении конфиденциальности информации, для этого они используют собственные средства защиты от злоумышленников (двойная аутентификация, система одноразовых динамических SMS-паролей, дополнительный список одноразовых паролей или аппаратный ключ, защищенное протоколом SSL-соединение и т. д.). Однако перечисленные средства не являются панацеей: троянец может перехватить платежный пароль пользователя или подделать сертификат подлинности сайта, мобильная версия Zeus, известная как Zeus-in-the-Mobile, может перехватить SMS с одноразовым кодом, а затем передать его злоумышленникам. Поэтому пользователю не стоит надеяться на банк, лучше с помощью собственного защитного компонента усилить предлагаемые им возможности. И в первую очередь для обеспечения безопасности банковской информации и системы в целом нужен качественный антивирус, входящий в продукт уровня Internet Security. Помимо антивируса необходимы средства поиска уязвимостей, проверка подлинности ссылок, блокировки зловредных веб-сценариев и всплывающих окон, защита данных от перехвата, а также виртуальная клавиатура для борьбы с кейлоггерами.

Следует учесть, что сегодня у злоумышленников наиболее распространены три подхода:

- заражение компьютера жертвы троянской программой;
- использование методов социальной инженерии;
- технологические атаки (снифинг, подмена DNS/Proxy-серверов, подмена сертификатов и т. д.).

Исходя из этого можно сделать вывод, что существуют три основные проблемы защиты от финансового мошенничества:

- недостаточно надежная идентификация сайтов;
- отсутствие доверенного соединения между клиентами и онлайн-сервисами;
- отсутствие гарантий того, что программное обеспечение на компьютере клиента не содержит уязвимых мест, которые могут использоваться злоумышленниками для атаки.

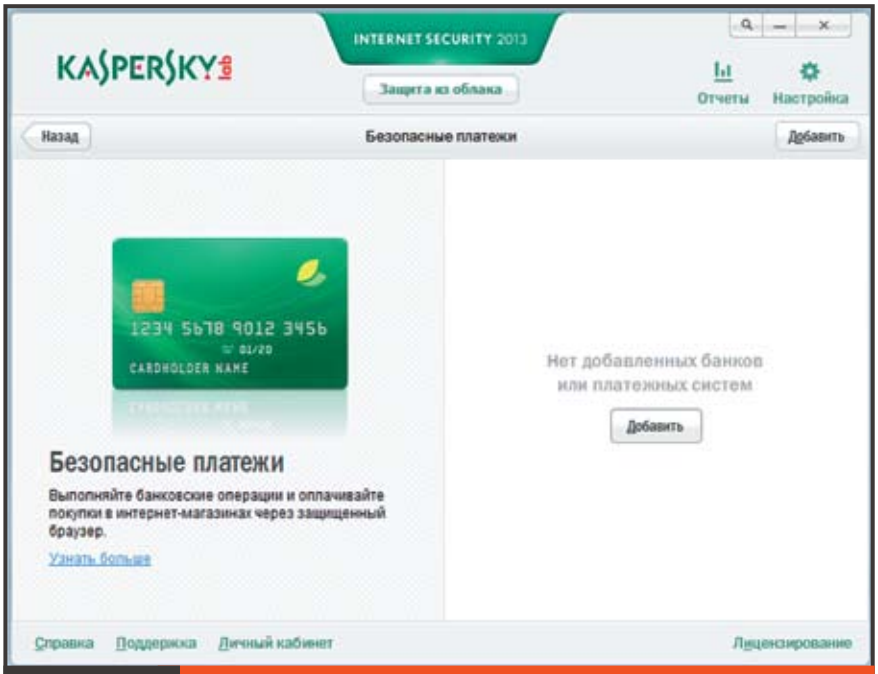
Безусловно, некоторые из этих проблем уже решаются продуктами класса Internet Security. В частности, защиту от фишинга предоставляют сегодня многие производители (качество такой защиты — это отдельный вопрос). Однако стоит учесть, что в большинстве продуктов такого класса некоторые из необходимых ступеней защиты отсутствуют.

Как уходят деньги?

Простейшим способом сбора финансовой информации является массовая рассылка фишинговых сообщений якобы от имени администрации банка. В письме злоумышленники могут прямо потребовать прислать им данные под выдуманным предлогом или же, что встречается значительно чаще, пройти по ссылке на официальный сайт банка.

Согласно исследованию «Лаборатории Касперского», подобную корреспонденцию получали до четверти (23%) пользователей по всему миру. Дальнейшие события зависят от способностей киберпреступников. Например, они могут создать копию официального сайта банка и разместить ее на домене, схожем по написанию с банковским. Пользователь проходит по ссылке и, думая, что находится на настоящем сайте, вводит свои данные в стандартную форму, откуда они попадают к злоумышленникам. Другой вариант: ссылка ведет на сторонний ресурс, где пользователю быстро загружают вредоносное программное обеспечение, используя сценарий или уязвимость в браузере, а затем перенаправляют на реальный сайт банка. Согласно исследованию «Лаборатории Касперского», подобная корреспонденция появлялась в почтовых ящиках 23% пользователей по всему миру. При получении сомнительной корреспонденции нужно внимательно посмотреть на адрес отправителя и ссылку, по которой предлагается пройти. И, конечно, помнить о том, что банки и другие финансовые организации никогда не присылают подобные письма. А в случае каких-либо сомнений лучше потратить минуту времени и позвонить в банк, переходить по предложенной ссылке ни в коем случае нельзя.

Несмотря на то что данный способ давно описан в соответствующей



Экран 1 Безопасные платежи

литературе и не является чем-то новым для пользователей, ввиду легкости и дешевизны осуществления он применяется до сих пор.

В качестве примера можно привести банковский троянец Trojan-Banker.MSIL.MultiPhishing.gen, который эксперты «Лаборатории Касперского» обнаружили в январе 2012 года. Он специализируется на похищении данных для авторизации на сайтах Santander, HSBC Bank UK, Metro Bank, Bank Of Scotland, Lloyds TSB, Barclays и других банков. Попав на компьютер жертвы, троянец никак себя не проявляет, пока пользователь не зайдет на сервис онлайн-банкинга одного из перечисленных финансовых учреждений. Дождавшись желаемого момента, троянец демонстрирует пользователю окно, имитирующее форму авторизации соответствующего банка. Если пользователь не заподозрит подвоха и введет в нее свои данные, вся информация будет незамедлительно отправлена владельцам троянца. Trojan-Banker.MSIL.MultiPhishing.gen действует по всему миру, но большая часть срабатываний приходится на Великобританию.

Вместе с тем не стоит забывать о технических средствах, предназначенных для хищения данных авторизации в момент их ввода пользователем, а также создания снимков экрана. Это так называемые кейлоггеры. Кроме того, популярность приобрели троянские программы, предназначенные для хищения паролей из менеджера паролей браузера.

Другие вредоносные программы могут во время работы пользователя подменять сайт банка сайтом злоумышленников (путем манипуляций с DNS) или модифицировать загруженные в браузере веб-страницы реального сайта, например добавляя в них собственные поля. Так поступал знаменитый универсальный (то есть выкрадывающий всевозможную личную информацию) троянец Zeus, заразивший 3,5 млн компьютеров только в США. Один из его наследников, троянец Trojan-Spy.Win32.Carberp, проникает в систему, используя известные уязвимости, и затем крадет деньги с банковских счетов физических и юридических лиц. Местом обитания троянца являются преимущественно Россия и страны СНГ.

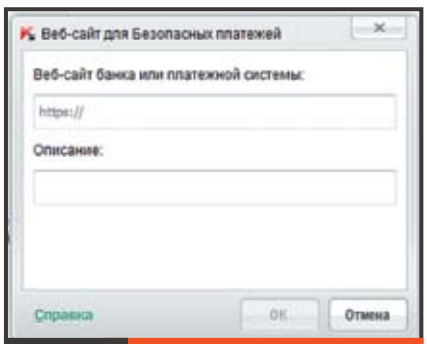
Банковская защита от мошенников

Безусловно, банки и другие финансовые организации не менее своих клиентов заинтересованы в сохранении конфиденциальности информации, а потому всегда использовали и будут использовать собственные средства защиты. Например, системы разовых паролей или двойную аутентификацию, которая предусматривает два пароля: один для входа в систему и просмотра баланса и другой — для проведения платежей. Некоторые организации предусматривают специальное программное обеспечение для операций онлайн-банкинга. Увы, данные средства не являются панацеей.

В первую очередь для обеспечения безопасности банковской информации и системы в целом нужен качественный антивирус, входящий в продукт уровня Internet Security. Он должен защитить компьютер от вредоносных программ, в том числе с помощью проактивных технологий. Также необходим веб-фильтр или аналогичное решение, способное обеспечить безопасность пользователя во время онлайн-серфинга, а также виртуальная клавиатура — для обхода кейлоггеров.

В новой линейке Kaspersky Internet Security для защиты финансовой и другой важной информации во время проведения платежных операций предусмотрена технология «Безопасные платежи» (экран 1), включающая три ключевых компонента защиты:

- база доверенных адресов платежных и банковских систем;
- сервис проверки сертификатов, позволяющий убедиться в подлинности веб-сайта;



Экран 2 Веб-сайт для безопасных платежей

- проверка компьютера пользователя на наличие уязвимостей. В данном случае проверяется наличие уязвимостей определенного типа, влияющих на безопасность онлайн-банкинга (к примеру, уязвимости класса повышения привилегий). В случае обнаружения «дыр» пользователю будет предложено устранить их в автоматическом режиме.

Следует учесть, что пользователь может сам добавить в список доверенных любой банк, платежную систему или интернет-магазин. Для этого достаточно нажать кнопку «Добавить» и в появившемся окне (экран 2) ввести соответствующий адрес и описание.

Настройка данного модуля не требуется. По умолчанию он уже готов к работе. Единственное действие, которое вы можете выполнить при настройке, — ввести доверенные адреса.

При первом входе на соответствующий сайт достаточно ответить на вопрос «хотите ли вы запустить сессию в защищенном режиме?», после чего при всех дальнейших операциях с этими адресами автоматически будет запускаться специальная защищенная сессия браузера.

Что происходит при запуске защищенного режима браузера?

1. Автоматически задействуется ряд антифишинговых технологий, включая проверку репутации сайта в «облачной» системе KSN и эвристический анализатор сайтов. Таким образом, даже если злоумышленники заманили пользователя письмом якобы от его банка и заставили перейти на поддельный сайт, защита распознает атаку, предупредит и заблокирует. Спуфинг (подмена адресов сайтов) также блокируется.
2. KIS проводит валидацию цифровых сертификатов (согласно базе данных KSN) для установления действительно доверительного, защищенного соединения с сайтом и предотвращения использования поддельных сертификатов.
3. Каждый раз при запуске проводится экспресс-сканирование операционной системы для выявления критических уязвимостей, которые могут использоваться злоумышленниками для атаки на компьютер и обхода стандартной защиты. Если уязвимости найдены, система выводит предупреждение и предлагает запустить модуль обновления Windows для установки обновлений.

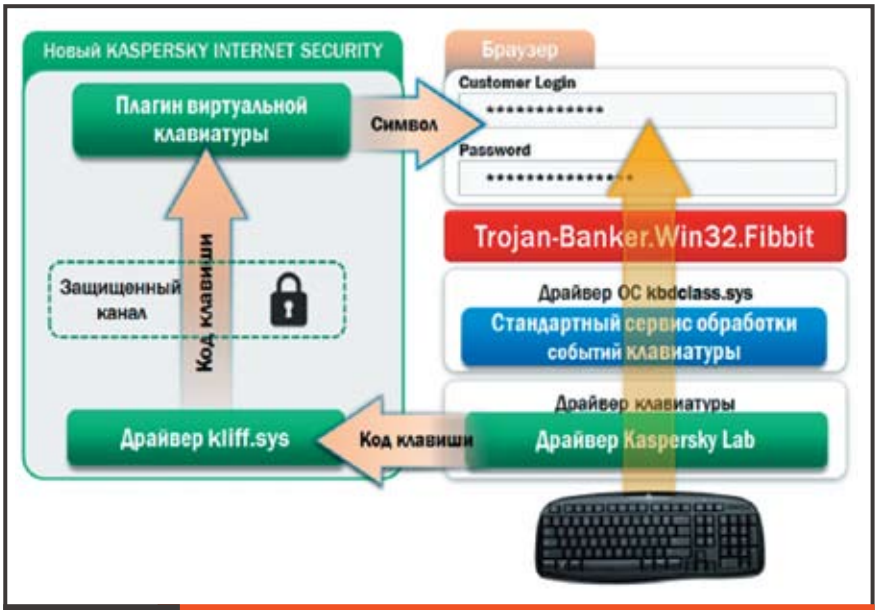


Рисунок Схема работы KIS

Защищенный режим браузера включает расширенный режим контроля программ (HIPS) специально для веб-сайтов, защищает вводимые с клавиатуры символы при помощи виртуальной клавиатуры и новой технологии «Безопасная клавиатура», защищающей от клавиатурных перехватчиков (кейлоггеров) на уровне драйвера операционной системы (см. рисунок).

Таким образом создается интегрированная, многоуровневая защита для борьбы с финансовым мошенничеством и специализированными вредоносными программами. Защита синхронизирует все необходимые компоненты продукта (в том числе автоматическую защиту Automatic Exploit Prevention для блокировки как известных, так и неизвестных атак через уязвимые места) для безопасной работы с «денежными» онлайн-сервисами.

Вместе с тем следует учесть, что не нужно каждый раз вручную включать специальный защищенный режим — это происходит автоматически, причем браузер сигнализирует об активации режима подсветкой окна. Технология не требует настройки: пользователю выводятся только предупреждения о блокированных атаках.

И наконец, самый главный вопрос. А зачем вообще все это нужно? Ведь уже сегодня нормальные банки используют многофакторную аутентификацию, одноразовые пароли, SMS-оповещения, защищенные соединения, политику оценки и аудита паролей, даже иногда попадаются сервисы с виртуальными клавиатурами. Да затем, что киберпреступность не будет стоять на месте, угрозы, увы, развиваются непредсказуемо. А значит, дополнительный уровень защиты лишним не будет!

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor