Особые ситуации требуют особого подхода

Интернет-банкинг, с одной стороны, очень удобен для потребителей, так как клиент может управлять своими счетами через браузер, а с другой - выгоден для банков, которые минимизируют затраты, перенося общение в Интернет. Все довольны. К сожалению, довольны и киберпреступники.

Популярность этого вида дистанционной работы с банковскими данными открывает новые возможности для кибермошенников - они могут завладеть финансовой информацией пользователя. Статистика неумолима: только похищенные данные владельцев кредитных карт приносят киберпреступникам (по разным оценкам) от 100 до 200 млрд долларов в год. Мы (Россия) также не стоим в стороне. По оценкам МВД, в прошлом году число преступлений, связанных с онлайн-банкингом, выросло в два раза, а в 2011 году, как отмечают эксперты, вновь увеличилось. Потери же составляют около 0,5 млрд рублей в год.

Поэтому один из главных вопросов, который волнует пользователя во время онлайн-банкинга - это сохранность его средств. Есть два варианта действий клиента: понадеяться на банковские механизмы аутентификации и поведенческого анализа или добавить к этим инструментам антивирусную защиту на своем компьютере.

Давайте рассмотрим защиту, которую предлагают банки. Программы для онлайн-банкинга, в том числе и банк-клиент в веб-интерфейсе, защищены только паролями и протоколом https, в лучшем случае - крипто-алгоритмом токена или смарт-карты. Честно говоря, они вообще не имеют никакой поведенческой защиты на уровне драйверов системы. Иллюзии о том, что «клиент работает с одним банком, который прекрасно знает, какие платежи соответствуют его профилю, какие - нет, и в состоянии обеспечить поведенческий контроль», рушатся о реальность под названием ZeuS.

Этот знаменитый банковский троян считывал с виртуальной клавиатуры пароль и логин доступа клиента, а затем подменял платежи. И был очень распространен. А еще существовал SpyEye и много других менее известных вредоносов, которые опустошали счета и карманы пользователей. Получается, что банки не в состоянии обеспечивать поведенческий контроль при проведении онлайн-операций на компьютере пользователя. Это могут делать только модули поведенческого контроля антивирусных

программ. Но большинство из них лишь решают вопрос поведенческой блокировки в целом и не специализируются на сценариях онлайн-банкинга.

Поэтому, когда меня спрашивают о необходимости «персональной» защиты компьютера в дополнение к банковской, я советую использовать и то и другое, причем это «другое» должно быть специализированным «банковским» антивирусом. Как говорится, «на бога надейся, а сам не плошай».

Однако даже при использовании проверенного онлайн-банкинга на защищенном компьютере, но через общественный WiFi, я бы не советовал заходить в «Личный кабинет» на сайте банка. Ведь неизвестно, каким образом обеспечивается безопасность на уровне роутера и линий коммуникаций с провайдером интернет-услуг. Настоятельно рекомендую всегда проверять защищенность беспроводной сети. Лучше всего, если она соответствует таким параметрам: тип безопасности WPA2, шифрование согласно алгоритму AES, случайный пароль не менее десяти, а лучше двадцати символов. При этом гарантировать, например, защищенность самого роутера вам никто не сможет. А через роутер злоумышленник легко получит доступ к паролю пользователя, а оттуда - и к информации, отправляемой по WiFi, в том числе и об онлайн-банкинге.

Подведем итог. Защита на стороне банка - лишь первый рубеж обороны против злоумышленников, пытающихся выкрасть ваши финансовые данные. В дополнение к ней необходимо защитить и сам компьютер. При этом не стоит надеяться на массовые антивирусы с «общими» поведенческими алгоритмами, следует использовать специальные «банковские» программы. И даже когда ваш компьютер надежно защищен, не забывайте, что «слабое звено» может оказаться вне вашей зоны контроля - на стороне раздающей бесплатный беспроводной интернет кофейни или чьего-то домашнего роутера, к которому вы подключились на улице.