Новые риски мобильного банкинга

Двухканальная или многоканальная защита позволит существенно снизить вероятность хищения средств со счетов пользователей мобильного банкинга или интернет-банкинга

текст Михаил Левашов, независимый эксперт, член правления АРСИБ, эксперт фонда «Сколково»

Недавно в массмедиа появилась сенсационная информация о том, что программа Siri, установленная на мобильных устройствах компании Apple, может быть использована в мобильном банкинге для кражи денег даже при заблокированном экране. В рамках статьи, опубликованной в одном из СМИ, приводятся комментарии представителей ряда известных банков, которые, как бы оправдываясь, рассказывают читателю о том, как они борются с подобными угрозами. Такая борьба в основном ограничивается лимитированием сумм и количества операций за определенный отрезок времени. То есть риски уменьшаются не за счет недопущения реализации угрозы, а за счет уменьшения сумм возможных потерь. Эти робкие попытки противодействия очередной новой угрозе, конечно, ограничивают возможности злоумышленников, но радикально ничего не меняют.

Мы уже обращали внимание читателей (например, в рамках круглого стола «Информационная безопасность в банковском секторе», проведенного NBJ в сентябре 2016 года и опубликованного в октябрьском номере журнала) на то, что защита любого мобильного банка, построенная на одном канале – том же устройстве, где находится сама программа, – имеет очень большой недостаток. Это устройство, если его использовать для работы в сети Интернет, в конечном счете может заразиться одной из действующих вирусных программ, похищающих деньги. И этот «зловред» на мобильном устройстве произведет все необходимые операции самостоятельно, причем в тайне от владельца гаджета. Оформит перечисление денег на нужный счет, получит и подтвердит его СМС-сообщением банка и несанкционированно переведет деньги.

Единственным радикальным способом избежать такого развития событий является реализация в мобильных банках принципа двухканальной или многоканальной защиты, заключающийся в том, что пользователь должен готовить перевод на одном устройстве, а подтверждать перевод с помощью другого. Например, готовить платеж на планшете (причем, на полноценном сайте интернет-банкинга), а СМС-подтверждение получать на мобильный телефон. Понятно, что для кражи денег злоумышленнику теперь нужно скомпрометировать оба устройства одновременно, так как компрометации одного из них будет недостаточно. Очевидно, что вероятность этого события на порядок меньше, чем компрометация только одного устройства. В идеале будет очень полезно присоединить еще и третий канал – например, банкомат, используемый для смены аутентификационных данных в мобильном банке. В этом случае при компрометации планшета злоумышленник не сможет заранее узнать ваш пароль.

Конечно, многие пользователи, даже, наверное, подавляющее большинство из них, не захотят пользоваться двумя устройствами мобильного банкинга. Это менее удобно и более накладно. Однако банк должен предусмотреть в своем интернет-банкинге или мобильном банкинге такую возможность для продвинутых пользователей. Причем она должна быть реализована в виде двух программ: для одного гаджета и для двух, без возможности перенастройки одной программы в другую. Это необходимо, для того чтобы исключить возможность в настройках одной программы менять параметр, регулирующий количество используемых в мобильном банкинге устройств. При этом банк должен четко и ясно предупреждать пользователей о существенных рисках использования одного устройства. В этом случае никакая Siri не будет страшна, какой бы исключительно приятный голос у нее ни был! NBJ