Как банку удержать клиентов своих цифровых каналов

Денис КАЛЕМБЕРГ, генеральный директор SafeTech — компании-резидента Инновационного центра «Сколково»

Специально для «ЧД»

В последние годы мы наблюдаем очень интенсивный процесс цифровизации взаимодействия между гражданами, бизнесом и государством. Наиболее ярко инновации заметны в банковской отрасли, где практически любые операции уже можно совершать удаленно, буквально движением пальца по экрану смартфона, и тем самым существенно экономить время.

Но есть и обратная сторона медали. Новые технологии несут в себе новые угрозы. И дистанционный банкинг — не исключение. За последнее время резко выросло количество краж со счетов клиентов с использованием заражения вредоносным ПО компьютеров, смартфонов, перехвата и выведывания мошенниками SMS-кодов. И банкам приходится балансировать на тонкой нити между удобством, мобильностью и безопасностью своих цифровых каналов, чтобы клиенты не ушли к конкурентам, потому что «система неудобная», и при этом не лишились своих денег. Ведь виновным в данном случае также останется тот, кто предоставил некачественную услугу.

При этом решать проблему одной «серебряной пулей» не получится, лучше разбить клиентскую базу на несколько категорий, проанализировать их основные сценарии работы, используемые каналы, необходимый уровень мобильности и предложить набор средств защиты, который будет минимизировать риски клиента, не меняя алгоритмов его работы.

Самым простым вариантом сегментирования я бы назвал разбивку клиентов на традиционных пользователей Интернет-банкинга — а это средние и крупные компании, имеющие выделенного бухгалтера, работающего за стационарным компьютером (назовем их «классиками»), и современных молодых предпринимателей и физических лиц, которые привыкли к тому, что все их коммуникации происходят «на бегу», через смартфон, и поэтому предпочитающие взаимодействовать с банком через приложение мобильного банкинга (они у нас будут «современниками»).

В этом случае, основные риски «классиков» — заражение рабочей станции вредоносным ПО, которое позволит злоумышленнику удаленно управлять компьютером жертвы и подписывать платежи в Интернет-банке, если ключи электронной подписи хранятся на флэш-карте или на подключенном к компьютеру USB-токене, а также автоматически подменять реквизиты и суммы подписываемых платежных поручений на заранее предустановленные мошенником шаблоны. На сегодняшний день наиболее адекватным способом защиты от таких атак является использование аппаратных решений класса «доверенный экран», которые отображают реквизиты платежей, идущих на подпись (например, в USB-токен), и не пропускают их до тех пор, пока пользователь не нажмет кнопку на корпусе устройства.

Что касается «современников», то в силу активного использования ими мобильных решений, банки в основном отправляют для подтверждения платежей SMS или PUSH-коды, что не выдерживает никакой критики с точки зрения уровня защиты. Эти коды элементарно перехватываются на всех этапах жизненного цикла: в канале передачи, на фишинговом сайте либо в мобильном устройстве. Кроме того, их довольно легко узнать у клиента, представившись сотрудником службы безопасности банка и попросив сообщить код для отмены якобы мошеннического платежа.

НОВЫЕ ТЕХНОЛОГИИ НЕСУТ В СЕБЕ НОВЫЕ УГРОЗЫ. И ДИСТАНЦИОННЫЙ БАНКИНГ — НЕ ИСКЛЮЧЕНИЕ

Для этой категории клиентов банки начали применять более совершенную технологию подтверждения: «мобильную» электронную подпись, которая генерируется непосредственно в смартфоне клиента, позволяет подписывать его электронные действия в любых цифровых каналах с контролем авторства и целостности. Что интересно, в данном типе решений удалось повысить одновременно как уровень безопасности, так и удобство работы клиентов, ведь последним теперь не надо ждать прихода SMS с кодом и вводить его вручную. Документ сразу отобразится на экране смартфона и необходимо только нажать кнопку «подтвердить».

Таким образом, банки, которые заботятся о безопасности и удобстве работы своих клиентов, сегодня имеют возможность выбрать решения для любой категории пользователей. ◆

Фото из личного архива Дениса Калемберга