В Управление Роспотребнадзора по Республике Алтай часто поступают обращения граждан о несанкционированном списании денежных средств с банковских карт мошенническим путем посредством услуги «Мобильный банк».

Российские банки стали предлагать своим клиентам услуги по управлению безналичными средствами и предоставлению информации. Все большую популярность приобретают системы мобильного банкинга – управления счетами посредством смс, равноценного по функционалу интернет-банкингу посредством компьютера.

Однако, популярность и расширение функционала сервиса имеют и обратную сторону медали – вместе с развитием мобильного банкинга растет число связанных с ним схем мошенничества. Пристальное внимание злоумышленников легко объяснимо. Мобильный банкинг наряду с информационными сервисами предоставляет возможность управления счетами клиента (переводы денежных средств между счетами, внутрибанковские переводы, переводы в другой банк, на телефоны и т.д.).

При открытии банковского счета, получении зарплатной карты, или оформлении кредита банки предлагают потребителям возможность подключения мобильного банка. Услуга подключается только на основании заявления потребителя и должна быть оформлена договором.

При заключении договоров, в том числе и на получение банковских карт, клиент должен внимательно изучить его условия. Банк в обязательном порядке прописывает информацию о необходимости его (банка) уведомления, в случае смены телефонного номера клиентом.

В обязанность банка входит: в случае поступления в службу помощи Банка сообщения об утрате мобильного телефона блокировать предоставление услуг «Мобильного банка». Одновременно, держатель банковской карты обязан в случае изменения его данных, указанных в заявлении (в том числе номера телефона) переоформить заявление.

Если имеет место факт утери мобильного телефона, сим-карта может попасть в руки постороннего человека. Нельзя забывать, что на Вашем номере подключен «мобильный банк», услугами которого очень быстро воспользуются мошенники. Поэтому необходимо немедленно! сообщать оператору связи о ситуации для блокировки сим- карты.

Другой случай когда абонент, приобретая сим- карту и указав ее номер в банке, забывает ею пользоваться. Если не пользоваться сим-картой более 90 дней, карта блокируется, а более 180 дней – оператор связи расторгает договор с абонентом в одностороннем порядке.

По истечении указанного срока неиспользования телефонного номера, оператор может заблокировать сим-карту и выпустить новую с тем же номером, а далее передать (продать) этот телефонный номер другому физическому лицу.

Таким образом, при поступлении СМС – сообщений по информации «Мобильного банка» о состоянии счета, новый пользователь будет иметь возможность технически оперировать счетом, не имея пароля, пин-кода и т.д..

Как же обезопасить свои сбережения?

Прежде всего, тщательно обдумайте: нужен ли вам мобильный банк вообще? Как часто вы совершаете банковские операции «на ходу» - на улице, на работе, на отдыхе? Можете ли вы отказаться от этих операций, например, класть деньги на телефон заранее - с домашнего компьютера, или через терминал, банкомат и прочие «физические» каналы? У подавляющего большинства людей нет жёсткой необходимости иметь «банк в кармане», это не более чем игрушка, дань моде, демонстрация «современности» и «приверженности прогрессу». Если по здравому размышлению вы поняли, что в состоянии обойтись без мобильного банка, угроза в существенной степени уменьшится.

1. Если у вас есть возможность и желание выбрать, в каком банке держать средства, выберите тот, где подключение дополнительных сервисов (и особенно мобильных) производится только по заявке клиента. И, соответственно, не подавайте такую заявку. Задайте этот вопрос сотруднику банка, если ответ будет «мы сами ничего не подключаем» - отлично, если «вы можете отключить то, что автоматически подключено» - хуже, но приемлемо, если сотрудник не готов ответить на ваш вопрос, это плохой банк.

2. Поинтересуйтесь в банке, есть ли у них возможность получать одноразовые пароли для операций со счётом не через смс, например, распечатывая одноразовые пароли в банкомате.

3. Спросите у сотрудника банка, все ли удалённые операции по счёту требуют двухфакторной аутентификации. Т.е. для проведения операции требуется введение двух паролей: постоянного, который вы держите в памяти, и одноразового, который получаете по смс или в банкомате. В мобильных банках часто бывает достаточно только одноразового пароля, приходящего в смс, но это очень слабая защита.

Один из вариантов хорошей защиты - постоянные логин и пароль для доступа в интернет-банк в пассивном режиме (посмотреть состояние счетов) и одноразовые пароли для любой расходной операции. Плохо, если в качестве логина используется какая-то очевидная информация (номер телефона), логин должен быть уникальным и известным только вам (и банку). Пару логин/пароль или только пароль желательно периодически менять.

4. При заключении договора внимательно читайте текст, обращая особенное внимание на дополнительные бесплатные услуги. Это тяжело, скучно и занимает много времени. Однако помните, злоумышленники, подделывая сим-карты неоднократно уводили со счетов пострадавших сотни тысяч. Данная мысль должна вас взбодрить.

5. После того, как договор заключён, вы получили доступ в интернет-банк и имеете на руках карту (или карты), проверьте ещё раз, какие услуги у вас подключены: в кабинете клиента в интернет-банке (если эта информация там есть) и у сотрудника в отделении (не по телефону). Отключите те услуги, что «случайно» подключились после подписания договора, если они вам не нужны.

6. Если мобильный банк вам всё же нужен или вы не можете до конца быть уверенным в том, что его у вас нет, правильно организуйте хранение денег в банке.

6 а) Сбережения храните на **сберегательном счёте** (вкладе), к которому нет вообще никакого доступа, кроме как в отделении по предъявлении паспорта. Ни интернет-банка, ни мобильного банка, ничего. Он должен быть максимально гибким в плане пополнения и частичного снятия денег. Договор к этому счёту храните в надёжном месте.

6 б) У вас должен быть по крайней мере один **текущий счёт** без привязки к картам, с доступом к нему только через полноценный интернет-банк и в отделении. На этом счёте вы будете хранить основную сумму «оперативных» денег (в пределах одного-двух размеров месячных трат).

6 в) Третий счёт **привяжите к карте**, которой будете пользоваться в магазинах. Пополняйте его через интернет-банк с текущего счёта по мере необходимости, скажем, два-три раза в месяц или, если вы любите строгий распорядок - каждую неделю в один и тот же день.

6 г) И, наконец, заведите ещё одну карту, привязанную к **отдельному счёту**, и именно эту карту свяжите с мобильным банком, если он вам очень нужен (или от него невозможно отказаться). Этой же картой вы можете совершать интернет-платежи и вообще относиться к ней без особого уважения. Никогда не храните на этом счёте хоть какие-то значимые для вас деньги. Вы должны понимать, что карта, привязанная к этому счёту, рано или поздно будет скомпрометирована, и какой-нибудь плохой человек получит к ней доступ. Не надо его радовать приличной суммой, которую можно украсть. Пополняйте этот счёт только перед платежом и держите на нём «аварийный» остаток на случай, если придётся срочно положить денег на телефон для одного-двух звонков.

6 д) Обратите внимание: каждая карта должна быть привязана к отдельному счёту. Это же требование, кстати, относится и к «семейным» картам. Выпуская дополнительную карту к своему счёту (для жены или мужа, ребёнка, родителей и т.д.), вы немного экономите, но в разы увеличиваете опасность потерять все деньги со своего счёта.

7. Если вы активно пользуетесь банком на смартфоне или планшете через приложение (не смс или USSD), то подумайте о возможности отделить приложение от получения паролей для доступа в него. Проще говоря, желательно иметь отдельный телефон для получения смсок из банка и хранить его не рядом со смартфоном (в другом кармане, в сумке и т.п.). Если вы потеряете смартфон, и он попадёт в плохие руки, злоумышленник не сможет получить смску с паролем для доступа в банк.

На первый взгляд, получившаяся система кажется громоздкой и неудобной. Но на самом деле, переводы между заведенными счетами будут занимать несколько секунд. При этом через карточки и мобильный мошенники подобраться к вашим основным деньгам не смогут. Это не значит, что средства защищены на 100% (интернет-банк – так же может быть лазейкой для злоумышленников), но защита станет на порядок прочнее, чем при отсутствии такой системы.

Если Вами зафиксирован факт незаконного снятия денег с карты, подайте заявление в полицию по факту мошенничества.

За консультацией по вопросам защиты прав потребителей в сфере финансовых услуг можно обратиться на «горячую линию» Роспотребнадзора по Республике Алтай: (38822)64241, по будням с 9-00 до 18-00.