В чью пользу банковский счет?

16 копеек – много ли это? С одной стороны, для покупателя это повод сказать «сдачи не надо», а продавцу, к примеру, округлить стоимость товара. С другой стороны, даже такую незначительную, казалось бы, сумму не хочется дарить преступникам. Именно 16 копеек с каждой 1000 рублей смогли похитить кибермошенники со счетов россиян в 2017 году.

Киберпреступность развивается вслед за расширением сферы безналичных расчетов. Ежегодно количество и объем операций с использованием пластиковых карт растут на 25-30 процентов. Но это не значит, что потери увеличиваются пропорционально. В Банке России действует Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ). По данным ФинЦЕРТа, год от года благодаря слаженным действиям множества структур, а еще повышения бдительности самих граждан потери снижаются. В 2015 году они составили 1,150 млрд рублей, в 2016м – 1,08 млрд. В 2017 году преступникам не удалось взять рубеж в миллиард рублей, их незаконная добыча – 961,3 миллиона. И если сейчас показатель 16 копеек на тысячу рублей, то ранее он был почти в два раза выше – 28 копеек. Снижается и средняя сумма одной несанкционированной операции. В прошлом году она составила 3 тысячи рублей, что на 17 процентов меньше, чем годом ранее.

Технические данные или психологический расчёт?

Схемы обмана постоянно обновляются. Раз в три-четыре месяца мошенники меняют направление деятельности, хотя цель остается той же – похищение чужих средств. Основной источник несанкционированных операций – это Интернет. По данным компании InfoWatch, специализирующейся на информационной безопасности, в прошлом году объем утечек информации вырос более чем в четыре раза. 86% украденных данных — личная и финансовая информация, в частности реквизиты пластиковых карт.

Еще одна тенденция последнего времени – персонифицированный подход. Сегодня преступники получают информацию о конкретном человеке, например, через социальные сети. Как зовут кошку, когда родился человек, какой была девичья фамилия матери – все эти данные люди нередко используют в качестве пароля и при этом не стараются их скрыть.

Данные, а вслед за ними и деньги, могут быть похищены, стоит лишь на несколько секунд выпустить карту из рук, к примеру, расплачиваясь в кафе. Злоумышленник может сфотографировать или запомнить нужные сведения (номер, трехзначный код), а затем воспользоваться чужим счетом для оплаты собственных нужд.

По-прежнему часто мошенники используют навыки социальной инженерии. Звонок или СМС-сообщение от родственника, оповещение якобы от банка, предложение получить компенсацию – «легенд» в арсенале преступников немало, и каждая из них, как показывает практика, весьма действенна. Способ защиты здесь один – быть начеку и многократно перепроверять информацию.

Основы самообороны от киберпреступников

В электронные кошельки киберпреступнику залезть так же просто, как карманнику в обычное портмоне. И остановить его может только бдительность. Есть простые, но действенные рекомендации.

Во-первых, никогда не следует сообщать посторонним PIN-код карты. При вводе кода в банкомате или терминале клавиатуру лучше прикрывать рукой, даже если рядом никого нет: современные мошенники не подглядывают из-за плеча, а укрепляют миниатюрную камеру над устройством. Также PIN-код нельзя вводить при оплате покупок через Интернет. Кроме того, каждый может самостоятельно изменить код. Если делать это регулярно, защищенность повышается.

Во-вторых, для оплаты товаров и услуг лучше завести отдельную карту и вносить на нее лишь сумму, необходимую для совершения предстоящей покупки. Касается это и платежей на кассах, и дистанционных. А при оплате в сети интернет всегда стоит перепроверить адрес магазина. Нередко мошенники создают клоны популярных ресурсов, меняя всего один символ. А деньги в этом случае уже пойдут не по назначению, а в карман злоумышленника.

Сегодня в роли кошелька нередко выступает мобильный телефон. Платежные сервисы, мобильный банк – все это создано для удобства пользователя, но порой удобны они и для преступника. Стоит мошеннику заполучить аппарат без пароля, как он получает доступ ко всему счету. «Кроме того, такие приложения могут быть уязвимы для вирусов, - напоминает управляющий Отделения Рязань ГУ Банка России по Центральному федеральному округу Сергей Кузнецов. – Не следует забывать о лицензированном антивирусном программном обеспечении. А вот чего не надо делать, так это открывать или скачивать сомнительные файлы и устанавливать приложения из непроверенных источников».

Что со счета упало, то пропало?

Если получено сообщение о списании средств с карты, но при этом никаких операций держатель карты не совершал, в первую очередь ему необходимо лишить злоумышленника возможности управлять деньгами. Для этого следует связаться с банком, в котором открыт счет, и заблокировать карту. Телефоны горячей линии обычно указаны на самой карте, на официальном сайте банка или в договоре обслуживания. Затем следует написать заявление в правоохранительные органы, а из банка запросить выписку по счету и подать заявление о несогласии с операцией. Если спорная операция была совершена на территории Российской Федерации, такие заявления рассматриваются банком в течение 30 дней. Для международных операций срок рассмотрения 60 дней. На возмещение ущерба можно рассчитывать, если банк не докажет, что держатель карты нарушил условия ее использования, в том числе меры безопасности, и обратился в банк не позднее дня, следующего за днем получения уведомления о совершении операции. Но это не касается проблем с электронным кошельком и прочими неперсонифицированными платежными средствами.

«Остап Бендер знал 400 способов отъема денег у населения. Сегодняшние мошенники мало уступают литературному прототипу, - считает управляющий Отделения Рязань Сергей Кузнецов. - Они крадут пароли, списывают деньги со счета человека без его ведома, обещают огромные проценты по вкладам... И жертвой может стать любой. Банк России старается работать на опережение. Но в первую очередь все зависит от самого человека: окажется он начеку, сможет ли защитить свои сбережения. Если вооружиться знаниями, эту задачу решить под силу каждому».

Смена мобильного номера может обернуться потерей средств

Современные технологии позволяют получать дистанционный доступ к банковским услугам. Один из распространенных сервисов – мобильный банкинг. В этом случае счет карты соотносится с конкретным номером мобильного телефона. Держатель счета может отслеживать изменение баланса, переводить деньги другим людям и так далее.

При этом мобильный банк привязан не к конкретному физическому лицу, а именно к номеру телефона. Граждане меняют сотового оператора или избавляются от старых номеров, но не сообщают об этом в банк, хотя по истечении определенного срока номер возвращается в базу и может быть продан снова. Новый владелец будет получать СМС о движении средств, предложения кредитного учреждения и прочие сервисные сообщения. Но главное, что он получит доступ к счету и возможность перевести с него деньги.

«Если ваш номер телефона изменился, следует сразу сообщить об этом в банк, где находится привязанный к мобильному сервису счет, это поможет сохранить средства, - напоминает управляющий Отделением Рязань ГУ Банка России по ЦФО Сергей Кузнецов. – В том случае, если вы приобрели СИМ-карту и стали получать сообщения о движении средств по незнакомому вам счету, также необходимо уведомить кредитное учреждение. Попытка перевести деньги на свой счет уголовно наказуема. Так, молодому рязанцу, который воспользовался подобной ситуацией и присвоил себе 7100 рублей, теперь грозит до шести лет лишения свободы».

Мошенники маскируют телефонные номера под номера банков

Телефонные мошенники стали использовать для похищения средств виртуальные автоматические телефонные станции, которые работают на основе существующей сети. Злоумышленники меняют номер своей АТС на действующий номер кредитных организаций. Затем они звонят клиентам банка и пытаются под разными предлогами выяснить конфиденциальную информацию: номер и срок действия платежной карты, трехзначный CVV-код и одноразовый пароль.

«Если вам поступил звонок из кредитной организации и собеседник просит сообщить сведения по карте, лучшим выходом будет положить трубку и перезвонить в банк по официальному номеру, который указан на платежной карте, – советует управляющий Отделением Рязань ГУ Банка России по ЦФО Сергей Кузнецов. – Реальным сотрудникам банка такие сведения, как ваш код и пароль, не нужны».

Следует помнить, что на возмещение можно рассчитывать только в том случае, если держатель карты не нарушал условия ее использования, в том числе соблюдал меры по безопасности, и обратился в банк не позднее дня, следующего за днем получения от банка уведомления о совершении операции. Если кража денег с карты стала следствием собственной неосмотрительности клиента, сообщившего преступникам свои персональные данные, банк не обязан возвращать утраченные средства.

Как не открыть доступ мошенникам к банковской карте?

Жительница п. Александро-Невский лишилась 7,5 тысяч рублей после звонка лжесотрудника банка. Собеседник представился сотрудником службы безопасности кредитного учреждения и сообщил, что счёт якобы атаковали хакеры. Под предлогом защиты денежных средств мужчина попросил назвать все данные карты. Рязанка назвала не только их, также пароль, который пришел на номер телефона, и сумму на счете. По данным полиции, разговор продолжался 26 минут.

«Преступники в последнее время часто маскируются под сотрудников банка. Они выясняют имена и отчества клиентов, иногда даже подключают виртуальную АТС и формируют клон номера кредитного учреждения, - говорит управляющий Отделением Рязань ГУ Банка России по ЦФО Сергей Кузнецов. – Следует помнить, что настоящие сотрудники не запрашивают персональных данных, пин-код, код безопасности и прочие сведения, которые позволяют получить доступ к счету. Если вам поступил такой звонок, скорее всего, это мошенники».

Чтобы не лишиться средств, необходимо соблюдать простые правила кибергигиены. У звонившего нужно уточнить его ФИО и должность. Если он настоятельно требует назвать личные данные держателя карты и ее реквизиты (CVC/CVV-код, коды из СМС, пин-код), следует завершить разговор и перезвонить по официальному номеру банка, указанному на сайте или же на платежной карте. При этом необходимо самостоятельно набрать номер, а не перезванивать на тот, с которого поступил звонок ранее. Это позволит избежать ситуации, когда через виртуальную АТС клиент вновь попадет к мошенникам. Если в СМС, полученном вроде бы из банка, содержится ссылка, безопаснее будет по ней также не переходить, чтобы не получить вирус или не попасть на фишинговый сайт.

Клиенты микрофинансовых компаний дополнительно защищены

Процентная ставка по краткосрочным потребительским займам теперь не может превышать 1% в день. Вступили в силу соответствующие изменения в законодательство. Ранее ставка была ограничена 1,5%.

Также устанавливается новое единое ограничение предельной задолженности для договоров сроком не более года. С 01 июля 2019 года задолженность не может превышать сумму самого долга более чем в 2 раза. То есть если потребитель взял 3000 рублей, максимальная сумма, которую он будет должен кредитору, - 9000 (3000 основного долга плюс начисленные проценты и иные платежи). Это условие должно находиться на первой странице договора, перед таблицей, содержащей индивидуальные условия.

Изменения коснулись и полной стоимости потребительского кредита (займа). На момент заключения договора она не может в процентах годовых более чем на треть превышать наименьшую из двух величин: рассчитанное Банком России на квартал среднерыночное значение полной стоимости потребительского кредита (займа) или 365 процентов годовых.

Кроме того, с 01 июля 2019 года микрофинансовые организации (МФО) обязаны размещать на договорах QR-коды. Считав код, клиент сможет узнать наименование МФО, ее номер в реестре и контактные данные, а также получить ссылки на официальный сайт компании, сайт саморегулируемой организации, куда МФО входит, в том числе на страницу для подачи жалоб, сайты Банка России и Федеральной службы судебных приставов.

«Все изменения направлены на защиту прав потребителей финансовых услуг. Но важно помнить, что организации, которые нелегально работают на рынке, как правило, не соблюдают требования закона, - говорит управляющий Отделением Рязань ГУ Банка России по ЦФО Сергей Кузнецов. – Поэтому, прежде чем оформить заем, следует проверить, есть ли МФО в реестре, состоит ли она в саморегулируемой организации. Нелегальные кредиторы нередко игнорируют максимально установленный процент или превышают возможные штрафы и пени».

«Раздолжнители»: разовый долг может превратиться в два

«Замучили кредиторы, коллекторы не дают спокойно жить», - так или примерно так начинается призыв фирм, которые еще называют себя «раздолжнителями». Они предлагают списать долги перед банком или микрофинансовой организацией (МФО). Но существует ли законный способ это сделать?

Такие организации бывают двух типов. Одни – откровенные мошенники. Другие действительно оказывают юридические услуги, но нередко человек мог обойтись без сторонней помощи. Рассмотрим эти варианты.

Помощники с большой дороги

«Нередко организации, позиционирующие себя как «раздолжнители», работают по принципу «финансовой пирамиды», - предостерегает управляющий Отделением Рязань ГУ Банка России по ЦФО Сергей Кузнецов. – Они обещают решить вопрос с действующими кредитами, берут деньги за свои услуги и исчезают. А гражданин остается не только с тем долгом, что у него был, но и с новыми штрафами и пени.

Схема здесь простая: человеку говорят, что за помощь он должен заплатить, к примеру, 20-30% от общей суммы кредита. Затем даже может быть составлен договор, где будет прописана обязанность снять с вас кредит. Это, кстати, вполне можно рассматривать как мошенничество. Но данный факт не слишком заботит подобные организации, ведь пока клиент поймет, что «посредники» не договорились с кредитором, те смогут свернуть деятельность. Иногда фирмы, чтобы сформировать репутацию, какое-то время действительно гасят долги обратившихся, но чаще всего это происходит за счет средств новых клиентов.

Заканчиваются подобные случаи стандартно: какое-то время (обычно не очень продолжительное) человек на самом деле не получает сообщений от банка или МФО. Но затем они понимают, что долг никто не возвращает, и выставляют дополнительные штрафы на остаток.

Еще одна разновидность мастеров обещаний – «инвесторы». Они говорят, что средства, которые вы им заплатите за работу, будут вложены в некие «доходные инструменты». Что это за финансовые инструменты, на какой доход может рассчитывать человек, никто не поясняет. Чаще всего это оказывается инвестиция в «Поле чудес в Стране дураков», то есть деньги, которые просто идут в карман мошеннику.

Кому я должен, я все прощу!

Если для большинства участников рынка понятие «банкрот» - часть ночного кошмара, то «раздолжнители» уверяют, что это настоящее спасение для попавшего в кредитную яму гражданина. По закону человек, который понимает, что более он неплатежеспособен, имеет право начать процедуру банкротства. Исключение лишь для тех, кто задолжал алименты или нанес вред жизни или здоровью другого лица. В этих случаях проститься с долгом не удастся. Казалось бы, сплошные плюсы (о которых как раз и рассказывают «раздолжнители»): единственную квартиру забрать не имеют права, с кредиторами и коллекторами больше не нужно общаться, проценты, штрафы и пени не начисляются.

Но в банкротстве есть и минусы, о которых клиент может не догадываться, а сотрудники фирмы о них умолчат. Во-первых, банкротство портит деловую репутацию и кредитную историю. Никто не может гарантировать, что в будущем вам не потребуется кредит или заём, но с банкротством в прошлом кредиторы могут и отказать: никто не хочет потенциально расстаться с деньгами, если вы захотите повторить процедуру. Кстати, сделать это можно не чаще одного раза в пять лет.

До завершения процедуры банкротства суд может запретить выезд за границу. Хотя неизвестно, будет ли, на что ехать: имуществом и деньгами станут распоряжаться

другие, а вы сможете тратить лишь установленную судом ограниченную сумму. Тем более будет, на что еще направить средства, ведь статус банкрота – не бесплатный. Нужно оплатить госпошлину, различные публикации, а также вознаграждение финансовому управляющему, которое составляет несколько десятков тысяч рублей, и его расходы. Так что порой выгоднее постепенно возвращать долг, чем соглашаться на призывы различных компаний «законно решить все проблемы через процедуру банкротства».

Реструктуризация долга – нужен ли посредник?

Пожалуй, наиболее комфортный для клиента способ, который предлагают всевозможные посредники, - это реструктуризация долга. Посыл фирм – человек без помощи грамотных юристов (которые, безусловно, работают именно в этой фирме) не сможет разобраться во всех тонкостях финансовых услуг и договориться с кредиторами. Реклама звучит красиво: «Вы сможете в разы снизить платежи или получить возможность для паузы в выплатах». Сотрудники рассказывают вдохновляющие истории, как некая клиентка отдавала по 40 тысяч рублей ежемесячно, а после их вмешательства сумма сократилась до 4 тысяч.

Действительно, банк или МФО могут пересмотреть график платежей или ежемесячную плату по кредиту. Но что за этим последует? Кредитор все равно планирует получить назад все выданные вам деньги. И если разовый платеж уменьшился, значит, увеличился срок погашения, а вслед за ним – переплата, ведь проценты будут начисляться на оставшуюся сумму, которая из-за небольших взносов будет меняться медленно.

«Не стоит забывать и о том, что бесплатно оказывать юридические услуги никто не будет, - говорит управляющий Отделением Рязань Сергей Кузнецов. – Коммерческий интерес подобных фирм напрямую зависит от величины долга: чем он больше, тем дороже обойдется помощь, которая нередко на самом деле не нужна».

Кредиторы заинтересованы в том, чтобы вернуть деньги. Именно поэтому начать лучше с диалога напрямую. Если вы благонадежный клиент, который внезапно попал в сложную ситуацию, можно попросить о рассрочке. Второй вариант – та самая реструктуризация, при которой пересматривают условия договора и уменьшают платежи. Чтобы банк или микрокредитная организация согласились на это, нужно подать письменное заявление и максимально подтвердить возникшие трудности (потерю работы, болезнь и т.д.). Худший вариант – скрываться и ждать, что про долг забудут.

Нужна ли помощь посредника там, где и сам гражданин может попробовать изменить ситуацию? Каждый решает сам. Главный же совет один: максимально ответственно относиться к обслуживанию кредита или займа. Тогда риск попасть в число злостных неплательщиков будет минимален, а обращение к «раздолжнителям» не потребуется.

Рязанцы могут стать биометрию в 33 отделениях банков

В Рязанской области работают 33 отделения 8 кредитных учреждений, где можно сдать биометрические данные. Биометрическое распознавание позволяет воспользоваться системой удаленной идентификации, которая призвана повысить доступность финансовых услуг. Многие операции (открытие счета, перевод средств и пр.) после сдачи биометрических данных можно совершать, не выходя из дома.

Процедура бесплатная и добровольная, осуществляется она только с согласия клиента, которому необходимо один раз лично обратиться в офис уполномоченного банка. Сотрудники кредитного учреждения запишут изображение лица и голос посетителя, проверят документы, а затем зарегистрируют человека в Единой биометрической системе. После прохождения процедуры начинает действовать механизм удаленной идентификации. Карту точек банковского обслуживания, где можно сдать биометрические персональные данные, можно найти на сайте Банка России.

«Механизм удаленной идентификации защищен в соответствии с самыми высокими стандартами безопасности, - рассказывает управляющий Отделением Рязань ГУ Банка России по ЦФО Сергей Кузнецов. - Данные хранятся в двух независимых системах, никак друг с другом не связанных. Персональные данные (паспорт, СНИЛС и прочее) – в Единой системе идентификации и аутентификации, в которой зарегистрировано более 80 млн россиян, с ее помощью, к примеру, получают госуслуги. Биометрические данные находятся в единой биометрической системе, причем без привязки к персональным данным, что повышает уровень безопасности».

При проведении удаленной идентификации кредитные организации в случае необходимости вправе применять дополнительные меры по снижению рисков, например, запрашивать дополнительную информацию, что позволяет обеспечить дополнительный уровень надежности. Для дальнейших действий достаточно будет любого гаджета (смартфона, планшета, ноутбука) или стационарного компьютера с камерой и микрофоном.

С 1 июля строительные компании будут получать деньги дольщиков через счета эскроу.

Счет эскроу – это специальный счет для безопасного проведения сделки между покупателем и продавцом. Его еще называют условным, так как переход счета, а значит и денег на нем, происходит при выполнении определенного заранее условия, кроме того, всегда есть третья сторона – кроме продавца и покупателя это банк или нотариус. Причем можно продавать и покупать с помощью счетов эскроу не только жилье, а любое имущество.

Создание нового механизма финансирования жилищного строительства, замещающего средства граждан банковским кредитованием, входит в число задач национального проекта «Жилье и городская среда», в реализации которого участвует и Банк России. Наша задача – подготовить банковскую сферу к работе по новым условиям. Так, заранее были определены оптимальные процедуры взаимодействия уполномоченных банков и застройщиков. Эти рекомендации учитывают интересы обеих сторон. На наш взгляд, они помогут сделать переход на проектное финансирование объектов долевого жилищного строительства более прозрачным.

Прежде всего, застройщикам для бесперебойного финансирования уже запущенных проектов было рекомендовано в кратчайшие сроки направить в банк заявку на получение кредита, причем можно выбрать несколько банков, чтобы сравнить условия и выбрать оптимальные Главное – предоставить полный и достоверный пакет документов.

Уполномоченные банки со своей стороны должны предоставить застройщикам максимум информации для подготовки заявки: какие финансовые продукты готово предоставить кредитное учреждение, как должны быть оформлены материалы для получения заёмных средств, по какой ставке могут быть выданы средства. Рассмотрение документов от застройщика не должно затягиваться, ориентировочный срок – 45 рабочих дней.

Установлены жесткие требования для кредитных организаций. Во-первых, достаточно высокий кредитный рейтинг. Чем рейтинг ниже, тем меньше проектов сможет обслуживать банк. Также установлен лимит суммы задолженности по всем договорам о предоставлении целевых кредитов застройщикам – не более 20% величины капитала банка.

Список уполномоченных банков есть на сайте Банка России и обновляется ежемесячно. До недавнего времени их было 63, в мае постановление Правительства расширило их еще на 3 десятка. По данным на 1 июня 2019 года 19 банков, имеющих представительство в Рязанской области, имеют право открывать счета застройщикам и счета эскроу. Еще несколько кредитных учреждений имеют банкоматы в нашем регионе, представлены в списке и интернет-банки.

Проектное финансирование с использованием счетов эскроу теперь обязательно для всех реализуемых проектов многоквартирных домов. Исключения должны соответствовать установленным Правительством критериям. Оно вышло 22 апреля. Застройщики получили возможность достроить то, что начато по старой схеме финансирования, если степень готовности объекта составляет 30% и если застройщик уже заключил не менее 10% договоров долевого участия. Если строительство идет в рамках комплексного освоения территории, степень готовности должна быть не меньше 15%. Эта же норма распространяется на случаи, если идет возведение и последующая передача государству социальных объектов или инженерных сетей. Значения критериев и случаи их применения могут быть уточнены на основании соглашений между правительством страны и властями регионов.