Финансовые мошенничества в Интернете и в сфере дистанционного банковского обслуживания

Развитие современных технологий оказывает влияние и на криминальную сферу: если раньше на благосостояние граждан посягали лишь карманные и квартирные воры, то теперь, с развитием онлайн-банкинга, на охоту вышли такие «продвинутые» преступники, как фишеры, скиммеры и организаторы разнообразных мошеннических схем в Интернете.

Так, мошеннические операции с пластиковыми картами уже не первый год являются проблемой российской банковской сферы. Большая доля незаконных списаний происходит с помощью скимминга, то есть считывания при помощи специального устройства данных с магнитной полосы карты: в России, по подсчетам компании Visa, доля скимминга в общем объеме мошеннических операций с картами этой системы достигает 49%. А еще 51% приходится на другие виды мошенничеств, имеющих целью завладеть данными банковских карт и паролями от кабинетов в системах интернет-банкинга.

При этом отечественный рынок банковских карт еще очень далек от насыщения: по разным данным, в России на одного человека приходится от 1 до 1,7 карты, и это один из самых низких показателей в Европе. В то же время, согласно исследованию НИУ «Высшая школа экономики», в США на одного человека в среднем приходится 3,69 карты. То есть поле для мошеннических операций будет только увеличиваться, если в процессе использования пластиковых карт и онлайн-банкинга их владельцы не обучатся правилам безопасности и не вооружатся четким пониманием рисков утраты денежных средств при столкновении с многообразными мошенниками и аферистами, действующими в Сети.

В 2014 году вступила в силу 9 статья Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе», обязывающая банк компенсировать владельцу карты незаконно списанные с нее средства. Однако на практике вернуть их клиентам удается не всегда: например, если клиент вовремя не уведомил банк о несанкционированной операции, вероятность возврата средств невелика.

Поэтому правила безопасности и противодействия злоупотреблениям с пластиковыми картами и в сфере онлайн-банкинга, а также понимание гражданами рисков, сопутствующих активному присутствию в сетевых сервисах, становятся все более актуальными.

Ответственность банка за электронные платежи, не санкционированные владельцем счета (карты)

Обязана ли кредитная организация информировать клиентов о совершении операций с использованием электронного средства платежа, в том числе платежных карт? Возможно ли взимание с клиентов платы за подобное информирование?

В соответствии с частью 4 статьи 9 закона «О национальной платежной системе» оператор по переводу денежных средств обязан информировать клиента о совершении каждой операции с использованием электронного средства платежа (далее – ЭСП) путем направления клиенту соответствующего уведомления в порядке, установленном договором с клиентом.

Исполнение кредитной организацией законодательно установленной обязанности не может быть обусловлено уплатой клиентом вознаграждения за предоставление информации, в связи с чем в договоре должен быть предусмотрен способ бесплатного информирования клиента в соответствии со статьей 9 закона «О национальной платежной системе». Дополнительно кредитной организацией могут оказываться клиенту (при его согласии) платные услуги по его информированию о совершении операций с использованием ЭСП. Это значит, что банк вправе взимать плату за sms-информирование клиента, а бесплатно информировать его об совершенных операциях по электронной почте. [*Официальный сайт Банка России, раздел* ***«Национальная платежная система»–«Регулирование в национальной платежной системе»–«Вопросы и ответы»–«Ответы на вопросы, связанные с применением отдельных норм Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе»*** *(часть 1)*]

Как законодательство регулирует использование «личного кабинета» в рамках онлайн-банкинга или иных аналогичных интернет-сервисов?

Закон «О национальной платежной системе» не ограничивает возможные способы информирования клиентов о совершенных операциях с использованием ЭСП, предусматривая при этом направление оператором по переводу денежных средств клиенту соответствующего уведомления в порядке, установленном договором с клиентом.

При использовании «личного кабинета» или иного аналогичного интернет-сервиса в целях соблюдения требований статьи 9 закона «О национальной платежной системе» должно обеспечиваться извещение клиента о возможности ознакомления с предоставленной оператором по переводу денежных средств информацией о совершении операций с использованием ЭСП. [*Официальный сайт Банка России, раздел* ***«Национальная платежная система»–«Регулирование в национальной платежной системе»–«Вопросы и ответы»–«Ответы на вопросы по применению статьи 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе»***]

Вправе ли кредитная организация – оператор по переводу денежных средств при возникновении подозрения о совершении мошеннических операций с использованием принадлежащей клиенту пластиковой карты по собственной инициативе приостановить или прекратить использование электронного средства платежа, если соответствующая возможность предусмотрена договором?

В соответствии с частью 1 статьи 9 закона «О национальной платежной системе» использование электронного средства платежа осуществляется на основании договора об использовании электронного средства платежа, заключенного оператором по переводу денежных средств с клиентом.

Таким образом, в силу части 9 статьи 9 указанного закона возможность приостановления или прекращения использования электронного средства платежа по инициативе оператора по переводу денежных средств при осуществлении мошеннических действий третьих лиц может быть предусмотрена в таком договоре в качестве элемента порядка использования электронного средства платежа. [*Официальный сайт Банка России, раздел* ***«Национальная платежная система»–«Регулирование в национальной платежной системе»–«Вопросы и ответы»–«Ответы на вопросы, связанные с применением отдельных норм Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе»*** *(часть 1)*]

Обязана ли кредитная организация – оператор по переводу денежных средств компенсировать клиенту потери, если операции с картой были совершены после ее фактической утраты клиентом и без его согласия? Или банк несет ответственность за списание денежных средств с карты только с момента, как клиент заявил об утрате карты в банк?

Требование о безусловном возмещении оператором по переводу денежных средств клиенту суммы операции, совершенной без его согласия после направления оператору по переводу денежных средств уведомления, предусмотренного частью 11 статьи 9 закона «О национальной платежной системе», установлено частью 12 указанной статьи.

Порядок уведомления клиентом кредитной организации, предусмотренный пунктом 11 статьи 9 закона «О национальной платежной системе», может быть конкретизирован в заключаемом между ними договоре в зависимости от используемого электронного средства платежа и сроков уведомления кредитной организацией клиента о совершенных операциях.

Частью 15 статьи 9 указанного закона установлено, что если оператор по переводу денежных средств исполняет обязанность по уведомлению клиента- физического лица о совершенной операции в соответствии с частью 4 указанной статьи и клиент – физическое лицо направил оператору по переводу денежных средств уведомление в соответствии с частью 11 данной статьи, оператор по переводу денежных средств должен возместить клиенту сумму указанной операции, совершенной без согласия клиента до момента направления клиентом-физическим лицом уведомления. При этом в указанном случае оператор по переводу денежных средств обязан

возместить сумму операции, совершенной без согласия клиента, если не докажет, что клиент нарушил порядок использования электронного средства платежа, что повлекло совершение операции без согласия клиента – физического лица. [*Официальный сайт Банка России, раздел* ***«Национальная платежная система» – «Регулирование в национальной платежной системе»–«Вопросы и ответы»–«Ответы на вопросы, связанные с применением отдельных норм Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе»*** *(часть 1)*]

Защита персональных данных держателей карт

Как действовать владельцу банковской карты, если ему пришло sms-сообщение или электронное письмо с информацией о ее блокировке от имени «Центрального банка»?

Банк России периодически получает информацию о фактах совершения мошеннических действий посредством sms-сообщений или email-рассылок с использованием его имени. В частности, мошенники направляют посредством sms-сообщений и email-рассылок в адрес клиентов различных кредитных организаций ложные сообщения о блокировке банковской карты клиента и предложения перезвонить по указанным в сообщениях телефонным номерам. В качестве отправителей сообщений, как правило, указываются: «Центробанк России», CentroBank, «Служба безопасности Банка России», то есть наименования, ассоциирующиеся с названием Центрального банка Российской Федерации (Банка России).

У граждан, обращающихся по указанным в сообщениях телефонным номерам, злоумышленники пытаются выяснить номера якобы заблокированных банковских карт, PIN-коды, количество денежных средств, размещенных на карточных счетах, персональные данные владельца карты и другую конфиденциальную информацию.

Центральный банк Российской Федерации никакого отношения к указанным sms-сообщениям и email-рассылкам не имеет. Подобные действия Банк России расценивает как мошенничество, осуществляемое с использованием имени Центрального банка Российской Федерации.

При получении подобного рода sms-сообщений и email-рассылок гражданину необходимо незамедлительно обращаться в подразделения кредитной организации, выдавшей ему банковскую карту, чтобы удостовериться в полученной информации. Делать это следует по тому телефону, который написан на оборотной стороне карты. Обращаясь же по телефону, указанному в сообщении, существует большая вероятность столкнуться с мошенниками. [*Пресс-релиз Банка России от 24 августа 2012 года – Официальный сайт Банка России, раздел* ***«Пресс-релизы»***]

Какие инструменты есть у Банка России для борьбы с финансовыми мошенничествами?

В связи ростом случаев мошенничества с банковскими картами Банк России обнародовал Указание от 14.08.2014 № 3361-У «О внесении изменений в Положение Банка России № 382-П от 9 июня 2012 года «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (далее – Указание № 3361-У), регламентирующее порядок защиты информации при осуществлении переводов денежных средств.

Этот нормативный документ вступил в силу 16 марта 2015 года.

В соответствии с Указанием № 3361-У банки должны информировать граждан о появлении в Сети ложных (фальсифицированных) ресурсов и программных обеспечений, имитирующих программный интерфейс интернет-банкинга кредитных организаций.

Также, согласно Указанию № 3361-У, банки должны размещать на лицевой панели банкоматов и терминалов или в непосредственной близости от них свое наименование, идентификатор устройства, телефонные номера и адреса электронной почты для связи клиентов с кредитной организацией. Кроме того, на банкоматах должен быть приведен алгоритм действий клиента в случае нарушения работы банкомата либо при выявлении нарушений защиты информации.

Наконец, один из пунктов обязывает банки с 1 июля 2015 года выдавать карты только с микропроцессором (чипом). Данные таких карт невозможно скопировать, что существенно затрудняет действия скиммеров. [*Указание от 14.08.2014 № 3361-У «О внесении изменений в Положение Банка России № 382-П от 9 июня 2012 года «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»*]

Какими тактиками пользуются злоумышленники, чтобы получить доступ к данным о банковской карте?

Одним из самых распространенных методов мошенничества является фишинг, когда мошенники получают доступ к конфиденциальным данным вкладчика от него самого. Злоумышленники используют несколько основных тактик.

Вариант первый – «звонок из банка» с просьбой о погашении задолженности по кредиту. Абонент предсказуемо отрицает наличие задолженности и кредита, тогда «представители банка» просят его уточнить данные своей карты – номер, PIN-код и дату выдачи, «чтобы больше не беспокоить по этому поводу». Если клиент сообщит все свои данные, мошенники без особого труда снимут средства с карты, изготовив ее фальшивый аналог.

Вариант второй – рассылка электронного письма, в котором от имени одного из крупных розничных банков сообщается о якобы последних новациях в его системе безопасности. Преступники могут знать, что адресаты являются держателями карт именно этого банка, а могут и не знать — рассылка делается в широкий список адресов, и среди них, скорее всего, найдется какое-то количество клиентов соответствующего банка. Для отвода глаз запрашиваются некоторые сведения (вплоть до потребительских предпочтений), но самое главное — номер карты и PIN-код (еще могут поинтересоваться ответом на «контрольный вопрос»). К письму прикрепляется ссылка, якобы ведущая на сайт банка-эмитента карты. Но этот сайт – подделка, имитирующая логотип и дизайн сайта банка, которым пользуется выбранный мошенниками клиент. После заполнения этой анкеты персональные данные клиента, а значит, и электронные средства, доступные по его карте, станут добычей мошенников.

Вариант третий – злоумышленники по электронной почте или на аккаунт в соцсети присылают код, который рекомендуют вставить в строку браузера, либо ссылку, по которой они предлагают пройти. Код или ссылка якобы позволят видеть закрытые записи в блогах поп-звезд или популярных актеров или получить доступ к будто бы существующей базе обо всех гражданах Российской Федерации. Но на самом деле это фишинговая программа, скачивающая с вашего компьютера и пересылающая преступникам файлы cookies, которые отражают маршрут заходов выбранной ими жертвы в различные сервисы. В том числе, возможно, и пароль к личному кабинету в системе банка, которым пользуется этот гражданин.

Что делать, чтобы не стать жертвой «фишинга»?

Прежде всего нельзя допускать, чтобы данные вашей карты попадали к третьим лицам, тем более незнакомым. Запомните: банки и операторы платежных систем никогда не присылают писем и не звонят клиентам с просьбой предоставить им данные о счете, PIN-код или иные персональные данные — вся необходимая информация у банка и так имеется. Банк просит клиента лично заехать в офис или, если это vip-клиент, присылает к нему курьера. И еще – стоит взять себе за правило с ходу стирать пришедшие на ваш электронный адрес сообщения, содержащие непонятные вам коды.

Клиентам банков рекомендуется немедленно прекращать любую финансовую интернет-операцию, если возникли малейшие подозрения, что она проходит нештатно, и тут же обращаться к специалистам банка. Необходимо также как можно чаще проверять выписки со своего счета, для чего из соображений безопасности желательно подключить услугу sms-информирования о совершенных операциях. [*Общие рекомендации по обеспечению безопасной работы в Интернет. «Управление «К» предупреждает: будьте осторожны и внимательны!», Министерство внутренних дел Российской Федерации. Электронное издание. 2012*]

Может ли владелец платежной карты добровольно передать ее другому лицу?

Передавать платежную карту другим лицам, в том числе родственникам, не следует. В отличие от находящихся на карточном счете средств, сама карта является собственностью банка, а не клиента. Пользоваться ей может только тот человек, чьи фамилия и имя указаны на карте. Передача карты другим лицам и сообщение им PIN-кода — это нарушение порядка использования электронных средств платежа, устанавливаемых банками-эмитентами и международными платежными системами. При выявлении такой передачи банк в дальнейшем вправе отказать владельцу карты в возмещении денежных средств по совершенным несанкционированным операциям.

Банк России в пресс-релизе от 14.07.2014 предупредил о распространении сделок по продаже владельцами кредитных карт неустановленным лицам. Эти неизвестные лица, в свою очередь, размещают объявления о приобретении платежных карт или обращаются непосредственно к владельцам с предложением продать карты.

Банк России предупреждает, что, во-первых, сам факт передачи карты представляет собой нарушение правил использования электронных средств платежа, во-вторых, владелец карты рискует быть привлеченным к ответственности как соучастник в случае, если его карта будет использована при совершении противоправных действий. [*Памятка «О мерах безопасного использования банковских карт» (Приложение к письму Банка России от 02.10.2009 № 120-Т); Пресс-релиз Банка России от 14.07.2014*]

Как отличить настоящий интернет-сайт банка от поддельного?

При подключении к банковскому серверу или иной веб-странице, на которой необходимо ввести конфиденциальные сведения, надо убедиться, что открылась именно нужная страницы и что адрес, отображаемый в браузере, правильный. Если URL-адрес состоит из случайного набора букв и чисел или выглядит подозрительно, следует прекратить сеанс. Можно потратить несколько секунд и напечатать адрес (URL) сайта самостоятельно.

Далее надо убедиться, что сеанс происходит в защищенном режиме (SSL): если соединение безопасное, то URL-адрес страницы будет начинаться с букв «https», а в адресной строке или строке состояния браузера будет отображаться небольшой значок замка. Щелкнув по значку замка, можно увидеть информацию о сертификате подлинности, который был выдан данному сайту. Сертификат должен быть действующим. Если его статус отличен от «This certificate is OK» или «Этот сертификат действителен», следует выйти из системы и обратиться в банк.

Банк России в памятке «О мерах безопасного использования банковских карт» рекомендует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг и обязательно убеждаться в правильности адресов Интернет-сайтов, на которых предполагается совершить покупки, так как похожие адреса могут использоваться для противоправных действий. [*Памятка «О мерах безопасного использования банковских карт» (Приложение к письму Банка России от 02.10.2009 № 120-Т)*]

Как через поддельные интернет-сайты осуществляются финансовые мошенничества?

Расширение числа госуслуг, предоставляемых гражданам через сеть Интернет, вызвало к жизни новый вид мошенничества, основанный на эксплуатации доверия к государству. Речь идет, к примеру, о мошеннических сайтах, собирающих деньги за якобы официальную информацию о долгах граждан.

Некоторые из сайтов имеют дизайн, схожий с официальным ресурсом Федеральной службы судебных приставов (далее - ФССП) и сервисом «Банк данных исполнительных производств». Мошеннические сайты «рекламируются» через ссылки в популярных социальных сетях и демонстрируют посетителям символику Федеральной службы судебных приставов Российской Федерации и изображение российского флага. Введя свои данные, пользователь «узнает», что в отношении него проводится проверка, либо ему закрыт выезд за рубеж, либо на его имущество вот-вот будет наложен арест. Чтобы узнать детали, он должен отправить платное sms-сообщение на некий номер. В должниках оказываются абсолютно все посетители и кто-то тут же расстается с какой-то суммой денег.

По этому поводу ФССП делала официальное заявление о том, что все ее сервисы, во-первых, предоставляются на официальном сайте, во-вторых, бесплатны.

Другой пример подобного рода — это «услуги» по оплате штрафов за нарушение правил дорожного движения. Некоторые автовладельцы в Московской области, получавшие по почте протоколы об административных нарушениях на дорогах, стали жертвами махинаторов, организовавших поддельный Интернет-сервис по оплате штрафов за нарушение ПДД — не зная того, что оплата штрафов возможна через портал «Госуслуги», сайт регионального ГИБДД, а также через платежные системы на основании номера и даты документа.

Режим безопасности электронных платежей

Как защитить свои финансовые средства при совершении покупок через интернет?

Для обеспечения безопасного онлайн-банкинга используются такие методы, как двухфакторная аутентификация и протоколы шифрования.

Двухфакторная аутентификация предполагает поэтапный доступ к онлайн-банку: сначала пользователь с компьютера вводит логин и пароль, затем для подтверждения входа в систему и проведения операций вводит дополнительные одноразовые коды. Эти коды пользователь может получить несколькими способами.

Во-первых, он может взять распечатку со списком паролей в банкомате обслуживающего банка, и при работе с онлайн-банком ему потребуется ввести неиспользованный пароль, указанный сервером. Поскольку квитанция с одноразовыми кодами может попасть в чужие руки, некоторые кредитные организации устанавливают ограничения на сумму операции, совершаемой по такому одноразовому коду.

Во-вторых, одноразовые коды могут генерироваться криптокалькулятором — специальным криптографическим устройством, которое клиент получает в банке при открытии счета и подключении услуги онлайн-банкинга.

В-третьих, одноразовые коды могут создаваться сервером банка под каждую операцию клиента и отправляться на его мобильный телефон в виде sms-сообщения.

На стадии идентификации пользователя в системе большинство банков предлагает многофакторную модель с вводом, помимо логина и пароля, дополнительного кода. При этом банк может использовать различные способы выдачи одноразовых кодов. Самым популярным является отправка sms-сообщения с паролем — она применяется в 91% систем онлайн-банкинга. В 44% систем используется сгенерированный пароль, в 32% систем — пароль из предоставленного клиенту списка.

Для похищения денег с банковского счета злоумышленник должен не только узнать пару «логин-пароль», но и получить доступ к одноразовым кодам. Если телефон, на который Ваш банк отправляет sms-сообщения с кодами, потерян или украден, нужно немедленно обратиться к оператору сотовой связи и заблокировать sim-карту. Предоставленный банком список кодов надо также тщательно хранить — он «стоит» не меньше, чем PIN-коды банковских карт. Если список потерян или украден, следует немедленно аннулировать все неиспользованные одноразовые коды. [*«Функциональность в ущерб безопасности. Как банку защититься от инсайдеров». – Банковское обозрение (Москва) № 7, 01.07.2014*]

Как настроить свой компьютер, чтобы произведенные с него онлайн-платежи были безопасными?

Можно выделить отдельный компьютер исключительно для онлайн-банкинга и покупок через Интернет, но такая возможность имеется не всегда, и сама по себе не гарантирует полной защиты. Используется ли компьютер только для финансовых операций в Интернет или для других нужд, он в любом случае должен быть «чистым»: легальное программное обеспечение, никаких вредоносных и сомнительных по происхождению программ. Необходимо регулярно выполнять антивирусную проверку, устанавливать обновления операционной системы, применять дополнительные защитные программы.

Эти и другие требования изложены, в частности, в разделе 7.5. «Общие требования по обеспечению информационной безопасности средствами антивирусной защиты» Стандарта Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», введенного с 1 июня 2014 года. В соответствии с пунктами 7.5.1-7.5.7 Стандарта, на всех автоматизированных рабочих местах должна применяться антивирусная защита, функционирующая в автоматическом режиме (включая установку обновлений антивирусного программного обеспечения и его сигнатур). Должна производиться антивирусная фильтрация всего электронного почтового трафика; в случае установки или изменения программного обеспечения должна выполняться антивирусная проверка с использованием актуальных обновлений.

Ведущие производители антивирусных программ, наряду с традиционными продуктами, предлагают специализированные решения для защиты онлайновых платежей. Такие программные модули выполняют важные дополнительные функции: например, проверяют аутентичность запускаемого платежного сервиса для исключения его подмены фишинговым сайтом, обеспечивают запуск платежного сервиса в защищенном браузере, благодаря чему исключается как возможность вредоносного внешнего воздействия на компьютер пользователя, так и вредоносное воздействие из компьютера (если он все-таки заражен троянской программой) на операции пользователя в системе онлайн-банкинга; имеют встроенную виртуальную клавиатуру для ввода логина и пароля для защиты от вероятных клавиатурных перехватчиков.

В настойках обозревателя лучше сразу запретить автозаполнение форм и сохранение паролей (в Internet Explorer это делается в меню **«Сервис»** -> **«Свойства обозревателя»** -> **«Содержание»** -> **«Автозаполнение»**). [*Общие рекомендации по обеспечению безопасной работы в Интернет. «Управление «К» предупреждает: будьте осторожны и внимательны!», Министерство внутренних дел Российской Федерации. Электронное издание. 2012 «Защита электронных денег в Интернет. Советы по интернет-безопасности для защиты денег и кредитных карт». Лаборатория Касперского. Официальный сайт*]

Насколько рискованно использовать компьютер с многопользовательским доступом для входа в систему онлайн-банка?

Компьютеры с общим доступом (в интернет-кафе, аэропортах, клубах, гостиницах, библиотеках) для входа в систему онлайн-банка или покупок в интернет-магазинах использовать нежелательно. Эти компьютеры могут быть заражены шпионскими программами, и вводимые логины и пароли могут стать известны мошенникам. Не рекомендуется также подключать собственный компьютер, используемый для финансовых операций, к общедоступным сетям Wi-Fi во избежание перехвата трафика администратором сети или киберпреступниками. В случае, если возникает необходимость произвести те или иные действия с использованием собственного устройства, предпочтительно использовать сеть сотового оператора — вероятность злонамеренного вмешательства извне в этом случае ниже, нежели при использовании общедоступных сетей Wi-Fi в общественных местах.

Если финансовые операции выполняются с компьютера, подключенного к домашней сети Wi-Fi с выходом в Интернет, то, помимо защиты собственно компьютера, следует принять меры для защиты сети, чтобы минимизировать вероятность несанкционированного доступа извне и внедрения вредоносных программ. [*«Безопасность общедоступных Wi-Fi-сетей». Лаборатория Касперского. Официальный сайт*]

Какой пароль для входа в систему онлайн-банкинга может быть признан надежным?

Надежный пароль — это такой пароль, который трудно угадать, но легко запомнить. Пароль должен состоять по меньшей мере из 8 символов (чем длиннее, тем лучше), в нем должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы. Он не должен включать в себя легко вычисляемые сочетания, вроде имени и года рождения, последовательности букв qwerty или цифр 123456, слов user, admin и т.д.

Как наилучшим образом настроить мобильный телефон или смартфон для осуществления через него интернет-платежей?

Для получения sms-кодов из банка лучше использовать отдельный телефон, причем простой модели, без возможностей установки посторонних программ (чтобы исключить загрузку какой-либо вредоносной программы).

Если для получения sms-кодов используется основной телефон (смартфон) владельца, то желательно использовать блокировку экрана – так можно уменьшить риск при попадании телефона в руки киберпреступника — и шифрование важной информации.

Современные смартфоны нуждаются в такой же антивирусной защите, как домашний компьютер и ноутбук. Некоторые продукты для смартфонов, помимо антивирусных функций, имеют инструменты защиты на случай кражи, включая дистанционный доступ хозяина к потерянному или украденному смартфону с целью установления его местонахождения, блокировки и уничтожения данных.

При установке на смартфон новых программ надо обращать внимание на то, каких разрешений она требует, особенно на возможность доступа к sms-сообщениям. Если запрашиваемые новой программой разрешения вызывают подозрение или не соответствуют заявленной функции, лучше от нее отказаться. [*«Меры безопасности при использовании Мобильного приложения». Сберегательный банк. Официальный сайт. «Советы по безопасности смартфонов». Лаборатория Касперского. Официальный сайт*]