ПАМЯТКА О МЕРАХ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ ЭЛЕКТРОННОГО СРЕДСТВА ПЛАТЕЖА И СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ
АО БАНК «НАЦИОНАЛЬНЫЙ СТАНДАРТ»

Москва 2021

Содержание

1. Общие положения

Настоящая Памятка о мерах по безопасному использованию электронного средства платежа и систем дистанционного банковского обслуживания АО Банк «Национальный стандарт» (далее – Памятка) направлена на информирование АО Банк «Национальный стандарт» (далее – Банк) своих клиентов в соответствии с рекомендациями Банка России в рамках реализации комплекса мер по повышению финансовой грамотности населения и на основе анализа практики использования физическими лицами электронного средства платежа. Соблюдение рекомендаций, содержащихся в настоящей Памятке позволит предупредить несанкционированные операции с использованием электронных средств и способов платежа:

1. Проведение операций с банковской картой в банкомате.
2. Безналичная оплата банковской картой товаров и услуг.
3. Оплата банковской картой в сети интернет.
4. Использование систем дистанционного банковского обслуживания.

2. Основные понятия

CVV2/CVC2 - (англ. Card Verification Value 2/ Card Verification Code 2), ППК2 – (Проверочный параметр Карты 2) – трёхзначный или четырёхзначный цифровой код на обратной стороне карты (в конце панели образца подписи), который используется клиентом конфиденциально как способ удостоверения распоряжений по операциям с реквизитами карты в сети Интернет.

Банковская карта — эмитированная Банком расчетная карта международной платежной системы Visa International или MasterCard Worldwide, или расчетная банковская карта национальной платежной системы Мир, являющаяся электронным средством платежа, предоставляемая для совершения держателем карты операций, расчеты по которым осуществляются в соответствии с законодательством Российской Федерации, Правилами платежной системы, Правилами предоставления и обслуживания расчетных банковских карт АО Банк «Национальный стандарт». Под банковской картой понимается также дополнительная карта.

Электронная подпись (далее – ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Ключ ЭП – уникальная последовательность символов, которая в целях недопущения ее компрометации известна только владельцу электронной подписи и предназначена для создания электронной подписи в электронном документе.

Ключевые носители – USB-устройства «Рутокен», а также другие внешние носители информации, на которые записана ключевая информация в электронном виде, предназначенная для постановки электронной подписи на электронном документе владельцем электронной подписи.

Сервис «SMS-оповещение», предоставляется в рамках услуги обслуживания счетов с использованием системы дистанционного банковского обслуживания, а также с использованием банковской карты и (или) её реквизитов. Данный сервис предназначен для повышения качества обслуживания Ваших банковских счетов и безопасности проведения операций с использованием систем дистанционного банковского обслуживания, а также банковских карт. SMS-оповещение – это возможность контролировать состояние счета с помощью мобильного телефона.

Системы дистанционного банковского обслуживания «Банк-Клиент», «Банк-Клиент через Internet» (для юридических лиц) и «Интернет-Клиент» (для физических лиц) — совокупность аппаратно-программных средств и технологий, используемых Банком и Клиентом для осуществления дистанционного банковского обслуживания по телекоммуникационным каналам и сети Интернет.

Электронное средство платежа (далее – ЭСП) — средство и (или) способ, позволяющие Клиенту Банка составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств (USB-устройства «Рутокен», система дистанционного банковского обслуживания, электронные кошельки WebMoney и Яндекс.Деньги и пр.)

3. Общие рекомендации

Запрещается:

Отвечать на электронные письма, телефонные звонки или иные обращения, в которых от имени Банка предлагается предоставить персональные данные. Не рекомендуется переходить по ссылкам, указанным в электронных письмах (включая ссылки на сайт банка), т.к. такие ссылки могут вести на сайты-двойники.

Необходимо:

В целях информационного взаимодействия с Банком использовать только реквизиты средств связи (телефонов, факсов, web-сайтов, обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в Банке.

4. При использовании банковской карты

Запрещается:

Сообщать ПИН-код или данные Вашей банковской карты третьим лицам, в том числе родственникам, знакомым, работникам кредитной организации, кассирам и лицам, помогающим Вам в использовании карты.

Передавать банковскую карту для использования третьим лицам, в том числе родственникам.

Необходимо:

Запомнить ПИН-код или в случае, если это является затруднительным, хранить его отдельно от банковской карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте.

При получении банковской карты расписаться на её оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования её без Вашего согласия в случае её утраты.

Уделять особое внимание условиям хранения и использования банковской карты. Не подвергать банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегать попадания на нее влаги.

Иметь при себе контактные телефоны Банка в целях незамедлительной блокировки карты в случае получения информации (через SMS-оповещение или другим способом) о неправомерном списании средств. Телефон Банка указан на оборотной стороне банковской карты.

Набирать ПИН-код банковской карты таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН-кода прикрывайте клавиатуру рукой. Применение данных мер защитит от подсматривания Вашего ПИН-кода посторонними людьми, а также при наличии на банкомате установленной злоумышленниками видеокамеры.

Помнить, что в случае раскрытия ПИН-кода, данных банковской карты, а также утраты банковской карты существует риск кражи денежных средств. Если имеются предположения о раскрытии ПИН-кода или данных банковской карты, а также если банковская карта была утрачена, необходимо немедленно обратиться в Банк для блокировки банковской карты. До момента обращения в Банк Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета.

Рекомендуется:

С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковской карты установить суточный лимит на сумму операций по банковской карте, а также подключить электронную услугу оповещения о проведенных операциях (например, оповещение посредством SMS-сообщений или иным способом).

4.1. При совершении операций с банковской картой в устройстве самообслуживания (банкомате, терминале и пр.)

Необходимо:

Не использовать устройства, считывающие магнитную полосу/данные чипа банковской карты, которые требуют ввода ПИН-кода для доступа в помещение, где расположено устройство самообслуживания, и другие внешние устройства, которые считывают магнитную полосу карты. Данные устройства не являются легитимными.

Перед использованием устройства самообслуживания осмотреть его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН-кода и в месте (прорези), предназначенном для приема банковских карт (например, наличие неровно установленной клавиатуры набора ПИН-кода). При появлении подозрений о наличии дополнительных устройств на устройстве самообслуживания воздержитесь от его использования и сообщите о своих подозрениях по телефону, указанному на устройстве.

Не применять физическую силу, чтобы вставить банковскую карту в устройство самообслуживания. Если банковская карта не вставляется, воздержитесь от использования такого устройство, которое возможно неисправно или подверглось мошенническим действиям.

В случае если устройство самообслуживания работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается и пр.), отказаться от использования такого устройства, отменить текущую операцию, нажав на клавиатуре кнопку «Отмена», и дождаться возврата банковской карты.

После получения наличных денежных средств, забрать банковскую карту, пересчитать банкноты полистно, дождаться выдачи квитанции, затем положить их в сумку (кошелек, карман) и только после этого отойти от устройства.

Если устройство самообслуживания не возвращает банковскую карту, позвонить по телефону, указанному на нем, и объяснить обстоятельства произошедшего, а также обратиться в Банк для блокировки карты.

При приеме и возврате карты устройством самообслуживания не толкать и не выдергивать карту до окончания ее прерывистого движения в картоприемнике. Неравномерное движение карты не является сбоем, а необходимо для защиты от мошеннических действий.

Рекомендуется:

Осуществлять операции с использованием устройств самообслуживания, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).

Сохранять распечатанные квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.

Не прислушиваться к советам третьих лиц, а также не принимать их помощь при проведении операций с банковской картой, тем более не давайте им в руки свою банковскую карту.

4.2. При безналичной оплате банковской картой товаров и услуг

Необходимо:

Не использовать банковские карты в организациях торговли и услуг, не вызывающих доверия.

Требовать проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных и платежных данных указанных на карте.

При проведении операции с вашей банковской картой не упускайте ее из виду. Не допускайте ситуаций, когда банковская карта находится вне Вашего поля зрения (например, загораживается монитором кассы).

При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт, подписать чек или ввести ПИН-код. Перед набором ПИН-кода необходимо убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем как подписать чек или набрать ПИН-код, в обязательном порядке проверьте сумму операции.

Не подписывать чек, выданный кассиром по завершении операции, в котором не проставлены (не соответствуют действительности) сумма, валюта, дата операции, тип операции, название торгово-сервисной точки.

В случае если при попытке оплаты банковской картой имела место «неуспешная» операция, необходимо потребовать у кассира и сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

В случае Вашего отказа от покупки сразу же после завершения операции, требовать отмены операции и убедиться в том, что ранее оформленный чек уничтожен.

Не выбрасывать (уничтожать) чеки, на которых указан полный номер карты.

Рекомендуется:

Сохранять все чеки (слипы) в течение длительного времени.

Защищать от подсматривания данные банковской карты, находящиеся на ее обратной стороне (код CVV2/CVC2/ППК2).

4.3. При совершении операций с банковской картой через сеть Интернет

Необходимо:

Не использовать ПИН-код при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.

Не сообщать персональные данные или информацию о банковской карте или банковском счете через сеть Интернет, например, ПИН-код, срок действия банковской карты, кредитные лимиты, историю операций и пр.

Помнить о том, что сотрудники Банка не запрашивают у клиентов информацию о логинах и паролях, не просят выполнять денежные переводы.

Обязательно убедиться в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т. к. похожие адреса могут использоваться для мошеннических действий. Имейте в виду, что буква «о» и цифра «0», буква «l» и цифра «1» могут выглядеть одинаково. Ссылки из писем открывайте, копируя текст через буфер обмена в адресную строку браузера, не кликая на них мышкой, поскольку ссылка пользователю может показываться одна, а открываться другая, ведущая на мошеннический сайт.

Убедиться, что интернет-сайт содержит справочную информацию об интернет-магазине, которая включает в себя: наименование юридического лица или индивидуального предпринимателя, юридический и фактический адреса, контактный номер телефона и адрес электронной почты для обращения покупателей.

Установить на свой компьютер антивирусное программное обеспечение и регулярно производить его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ).

Рекомендуется:

С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета для оплаты покупок в сети Интернет использовать отдельную банковскую карту с минимальной суммой денежных средств, предназначенную только для указанной цели.

Пользоваться интернет-сайтами только известных и проверенных организаций, поддерживающих технологию 3DSecure (см. ниже).

Совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и информации о банковской карте и банковском счете. В случае, если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что указанная информация не сохранились (вновь загрузив в браузере интернет-страницу продавца, на которой совершались покупки).

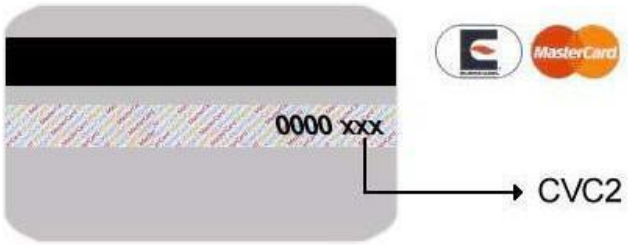
Не открывать письма электронной почты или сообщения интернет-мессенджеров (ICQ, Viber, WhatsUp, Facebook и проч.) от неизвестных отправителей, сразу удалять их, не открывать вложенные файлы, не переходить по содержащимся в таких письмах ссылках.

4.3.1. 3DSecure

3DSecure – это защищенный протокол авторизации пользователей. Технология разработана платежными системами для безопасной оплаты товаров и услуг по картам Мир, VISA и MasterCard в Интернете.

Как это работает?

На первом шаге запрашиваются данные: номер карты, срок ее действия, имя держателя карты и код проверки ее подлинности (цифровой код на обратной стороне карты CVV2/ CVC2/ППК2).



На втором шаге используется протокол 3DSecure. Сайт магазина делает переадресацию на страницу Банка, где предлагается ввести одноразовый код подтверждения. Одноразовый код подтверждения можно получить из SMS-сообщения на своем мобильном телефоне, который был указан в заявлении на выпуск карты.

Как узнать, что интернет-магазин поддерживает технологию 3DSecure?

Онлайн магазины, которые принимают платежи строго с использованием 3DSecure, можно узнать по размещенным на сайте логотипам:

Как подключить банковскую карту к технологии 3DSecure?

В АО Банк «Национальный стандарт» технология 3DSecure доступна на всех картах Мир, VISA и MasterCard, эмитируемых Банком.

Как оплачивать товары и услуги в Интернете картой, подключенной к 3DSecure?

Убедитесь, что интернет-магазин или онлайн-сервис поддерживает технологию 3DSecure. Помните, что если указанная технология на сайте не поддерживается, то риск компрометации данных Вашей карты значительно выше.

Заказывая товар или услугу в Интернете, выберите способ оплаты банковской картой.

Укажите на сайте данные, которые запрашиваются:

- номер карты (16 цифр на лицевой стороне карты);
- CVV2/CVC2/ППК2 (три цифры на оборотной стороне карты, на полосе для подписи);
- фамилию и имя (латинскими буквами, указаны на лицевой стороне карты);
- срок действия карты (месяц и год, будьте внимательны – не перепутайте местами эти два поля);
- другие сведения, которые запрашивает интернет-магазин (например, название банка, БИН – первые четыре или первые шесть цифр из номера карты и т.п.). Указывать ПИН-код запрещено.

После этого Вы будете переадресованы на страницу ввода одноразового кода подтверждения, который вы получите посредством SMS.

После ввода одноразового кода и успешной проверки данных Банком, покупка совершается.

Затем Вы вновь вернетесь на сайт интернет-магазина.

4.4. Особенности совершения с использованием банковских карт операций оплаты сделок (услуг) в торгово-сервисных предприятиях (далее - ТСП), находящихся за пределами Российской Федерации, и операций перевода денежных средств в адрес иностранных организаций, которые предоставляют возможность участия в инвестиционной деятельности:

- При совершении операции оплаты в иностранном ТСП Вы заключаете договор с ТСП на поставку товара, оказание услуг или совершение инвестиционных операций. При этом следует иметь в виду, что заключение договора может осуществляться посредством совершения действий по выполнению условий, указанных в оферте (например, уплата соответствующей суммы). Совершение данных действий будет считаться принятием предложения заключить договор на условиях оферты.
- Вам необходимо внимательно ознакомиться с условиями договора с ТСП до момента оплаты товаров (услуг), заранее оценив риски утраты денежных средств. Защита гражданами Российской Федерации своих прав в случае недобросовестности иностранных ТСП может быть затруднительной вследствие необходимости применения норм иностранного законодательства.

- Вам следует осуществлять взаимодействие с ТСП в соответствии с договором, в том числе в случаях, когда ТСП не была оказана либо некачественно оказана оплаченная с использованием банковской карты услуга, не была осуществлена поставка оплаченного товара.
- Отношения между Вами и иностранными ТСП носят гражданско-правовой характер. Защиту нарушенных или оспоренных гражданских прав целесообразно осуществлять в судебном порядке.
- При наличии у Вас оснований полагать, что в отношении Вас со стороны третьих лиц под видом иностранного ТСП были осуществлены противоправные действия, Вам необходимо обратиться с соответствующим заявлением в правоохранительные органы.

5. При использовании систем «Банк-Клиент», «Банк-Клиент через Internet» (для юридических лиц) и «Интернет-Банк» (для физических лиц)

Необходимо:

В случае компрометации или подозрения на компрометацию незамедлительно обратиться в Банк для блокирования доступа в систему.

Перед осуществлением входа в систему убедиться, что Вы находитесь на подлинном сайте. Не входите в систему по ссылкам с других сайтов или сообщений электронной почты, т.к. злоумышленники часто используют фишинговые сайты (сайты-двойники) для хищения Вашей аутентификационной информации (логин, пароль).

При обнаружении сайта-двойника немедленно сообщить об этом в службу технической поддержки Банка, для проведения расследования.

Убедиться, что при входе в систему установлено защищенное соединение («https» в начале адресной строке).

Никому и никогда не сообщать свой пароль к системе.

Не использовать предлагаемую браузером функцию сохранения паролей к сайтам.

Не запускать неизвестные программы, не открывать почтовые вложения от неизвестных отправителей.

Включить и настроить межсетевой экран (брандмауэр).

Установить на свой компьютер антивирусное программное обеспечение и регулярно производить его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ).

Не использовать операционную систему, антивирусное и иное программное обеспечение, для которых прекращен предусмотренный разработчиком выпуск обновлений безопасности, антивирусных баз (Windows XP, Windows Server 2003 и пр.).

Использовать программное обеспечение (операционные системы, приложения) только из проверенных и надёжных источников.

Не оставлять без контроля компьютер при активной сессии работы в системе. При оставлении компьютера необходимо осуществлять выход из системы, используя соответствующие кнопки системы «Выйти» или «Завершить», после чего закрыть окно Интернет-браузера, извлечь ключевой носитель (если имеется) и произвести блокировку компьютера одновременным нажатием на клавиатуре ⊞ и L. Возобновление работы на компьютере производить с использованием пароля доступа. По окончании рабочего дня производить выключение компьютера.

Отключать режим автозапуска на сменных носителях (CD, флешки и т.п.). Всегда проверять все, подключаемые к компьютеру, сменные носители на отсутствие вирусов и иных вредоносных программ.

Исключить удаленное управление компьютером, с которого осуществляется доступ в систему, без явного подтверждения каждого подключения уполномоченным на доступ в систему лицом.

Не устанавливать надстройки и плагины (например, от поисковых служб Яndex, Google и т.п., дополнительные панели, различные «ускорители интернет» и т.п.) в интернет-браузер, который используется для доступа к системе.

Установить для повседневной работы ограниченные права доступа к компьютеру. Не работать с правами Администратора. Административные полномочия в операционной системе следует использовать только для установки и настройки операционной системы и программного обеспечения.

В случае если возникает подозрение на заражение компьютера вирусом, немедленно прекратить работу в системе и провести полную проверку компьютера на наличие вредоносного программного обеспечения.

Использовать надежные пароли для доступа в систему дистанционного банковского обслуживания и пароли для входа в операционную систему компьютера, имеющие длину не менее 10 символов и содержащих буквы из различных регистров (заглавные и строчные) и цифры. Производить регулярную смену паролей не реже одного раза в месяц и немедленно после любого подозрения на компрометацию. Использовать пароли только соответствующему уполномоченному для работы в системе лицу. Пароли запрещено произносить вслух, выводить на экран, кому-либо передавать.

Помнить о том, что сотрудники Банка не запрашивают у клиентов информацию о логинах и паролях, не просят выполнять денежные переводы.

Рекомендуется:

Избегать входа в систему в местах, где услуги Интернета являются общедоступными, например: Интернет-кафе, а также с неизвестных Вам компьютеров.

Не хранить на серверах электронной почты (в особенности, бесплатных ресурсов веб-почты) письма, содержащие конфиденциальную информацию.

Не устанавливать на компьютере, используемом для доступа в систему, программное обеспечение без особой необходимости.

Установить пароль на вход в BIOS Setup компьютера. Настроить в BIOS Setup возможность загрузки операционной системы только с основного жесткого диска и пароль на загрузку компьютера.

Не открывать письма электронной почты или сообщения интернет-мессенджеров (ICQ, Viber, WhatsUp, Facebook messenger и проч.) от неизвестных отправителей, сразу удалять их, не открывать вложенные файлы, не переходить по содержащимся в таких письмах ссылках.

5.1. При использовании систем «Банк-Клиент» и «Банк-Клиент через Internet» (для юридических лиц)

Необходимо:

Осуществлять вход в систему Банк-Клиент только по официально предоставленным ссылкам **https://enter1.ns-bank.ru, https://enter2.ns-bank.ru и https://business.faktura.ru/f2b/.** Банк никогда не помещает ссылки на страницу входа в систему в исходящей корреспонденции клиентам. Имейте в виду, что буква «l» и цифра «1» в некоторых шрифтах выглядят одинаково.

Настроить сетевые устройства таким образом, чтобы ограничить доступ как к сети Интернет, так и из неё к внутренним информационным ресурсам.

При увольнении ответственного работника, имевшего доступ к ключам ЭП, выполнить замену ключей.

При увольнении специалиста, обслуживавшего компьютеры с установленной системой, проверить компьютеры на отсутствие вредоносных программ и сменить все электронные ключи, расположенные на незащищенных носителях (любые, кроме Рутокен).

Использовать ключевой носитель (Рутокен, флеш-накопитель, дискета), подключаемый к компьютеру только на время использования (вход в систему и непосредственно подпись документа).

При использовании незащищенных ключевых носителей (все, кроме Рутокен), создавать резервные копии на дополнительном носителе и хранить его в защищенном месте (сейфе). Не хранить на ключевом носителе посторонние файлы. Не объединяйте на одном носителе ключи разных банков.

Не оставлять ключевой носитель без присмотра, не передавать его другим лицам, включая других уполномоченных для работы в системе лиц. Хранить ключевые носители разных уполномоченных лиц раздельно, в защищенном месте.

Не посещать с компьютера, используемого для работы с системой, сайты социальных сетей, развлекательные и игровые сайты, сайты знакомств, сайты, распространяющие программное обеспечение, музыку, фильмы и т.п. в целях предотвращения заражения компьютера. Помните, что новые модификации вирусов, описания которых еще не включены в антивирусные базы, успешно преодолевают антивирусное программное обеспечение и могут быть использованы злоумышленниками для хищения денежных средств.

Все работы, связанные с поддержкой и обслуживанием компьютера, осуществлять под контролем лица, уполномоченного для работы в системе.

Рекомендуется:

Использовать защищенный ключевой носитель Рутокен для хранения ключей.

Использовать компьютер, на котором установлена система только для работы с банком и бухгалтерского учета.

Настроить аудит (протоколирование) событий в операционной системе и программах, установленных на компьютере, периодически просматривать журналы аудита, реагировать на ошибки и попытки несанкционированного доступа.

Регулярно выполнять резервное копирование операционной системы и данных.

5.2. При использовании системы Интернет-банк (для физических лиц)

Необходимо:

Убедиться в наличии символа замка в правом нижнем углу веб-страницы или справа/слева от адресной строки и зеленая картинка, например::  или 

. Их наличие означает, что соединение с Банком происходит по защищенному протоколу https.

Использовать виртуальную клавиатуру для ввода пароля.

В случае утери мобильного телефона, на который направлялись разовые пароли, или в случае обнаружения подозрительных действий, совершенных от вашего имени в системе, незамедлительно обратитесь в Банк для смены логина и пароля . Незамедлительно заблокировать SIM-карту, используемую для получения сообщений при работе с системой, включая SMS-сообщения с разовыми паролями.

Прежде, чем подтверждать платеж в Системе, внимательно проверить в полученном SMS-сообщении с разовым паролем информацию о сумме и получателе платежа.

В случае использования мобильного телефона с операционной системой Android для получения SMS-уведомлений системы или для работы с мобильным приложением установить лицензионное антивирусное программное обеспечение из официального источника (Google Play), не реже раза в сутки производить обновление антивирусных баз, не реже раза в неделю производить полное антивирусное сканирование мобильного телефона. Не устанавливать на телефон приложения, обладающие полномочиями работы с SMS-сообщениями.

6. Правила составления паролей

Правильно составленный пароль — одно из важнейших препятствий на пути злоумышленников. Составляйте пароль с учетом следующих требований:

длина пароля — не менее 10 символов;

пароль должен включать буквы верхнего и нижнего регистра, цифры и спецсимволы (@, #, $, %, <, ^, &, *)

Пароль не должен включать в себя повторяющиеся или легко вычисляемые сочетания символов (полные слова; полные слова в транслитерации; полные слова, набранные в другой, противоположной языковой раскладке или обратном порядке; символы, расположенные рядом на клавиатуре; имена; фамилии; памятные даты; адреса; номера телефонов и т.п.). Надежный пароль — это пароль не только легкий для запоминания, но и достаточно хорошо защищенный от угадывания или вычисления методом перебора по словарю/словарям.

Ниже приведены варианты генерации надежного пароля:

Придумайте в качестве пароля хорошо запоминающуюся осмысленную фразу, например: Santa Claus. Измените чередование строчных и прописных знаков, используйте вместо пробела знак подчеркивания: sANTA_cLAUS. Набирайте ваш пароль на клавиатуре со сдвигом на одну клавишу, например, вправо: dSMYS+l:SID.

Можно использовать в качестве пароля какую-нибудь стихотворную фразу (например, «Мне нравится, что вы больны не мной») и из каждого слова включить в пароль первые две буквы, при этом поставив английскую раскладку клавиатуры (например, в данном случае получится пароль Vyyhxnds,jytvy).

Взять какое-нибудь сложное, но известное вам профессиональное слово (например, цистрансизомерия) и вставить в его середину какой-нибудь цифровой код (например, год открытия изомерии Ю. Либихом – 1823), при этом установив английскую раскладку клавиатуры. Из этих данных получится хороший пароль - wbc18nhfyc23bpjvthbz.

Не используйте одинаковые пароли для разных применений.

В описанных случаях вам придется помнить лишь ключевую фразу и то, что с ней надо сделать. Это проще запоминания набора случайных символов, и в то же время данные преобразования дают достаточно надежный пароль.

7. Контактные данные службы поддержки

Круглосуточная служба поддержки держателей карт и пользователей системы «Интернет-банк» (для физических лиц):

Тел. 8-800-250-33-00

Служба поддержки пользователей систем дистанционного банковского обслуживания для физических и юридических лиц :

Тел. +7 (495) 725-59-53, +7 (495) 956-17-24

E-mail dbo@ns-bank.ru

Время работы: с 9:00 до 18:00