I. Меры безопасного использования платежных карт

Соблюдение рекомендаций, в Памятке, позволит обеспечить максимальную сохранность платежной карты, ее реквизитов, ПИН и других данных, а также снизит возможные риски при совершении операций с использованием платежной карты в банкомате, при безналичной оплате товаров и услуг, в том числе через сеть Интернет.

Общие рекомендации

1. Подключите услугу SMS-информирования и контролируйте проведение операций по вашим счетам и картам.
2. Не забывайте актуализировать номер телефона и другие данные. Если у сотрудников банка будут устаревшие данные, они не смогут оперативно связаться с вами для уточнения информации в случае проведения подозрительных операций или при возникновении спорных ситуаций.
3. Регулярно проверяйте выписку по своим счетам.
4. Ваша карта — это доступ к вашим деньгам, поэтому обращайтесь с ней так, как вы бы поступили с наличными. Храните карту в недоступном для других месте и не оставляйте ее там, где посторонние могут скопировать номер карты
5. Никогда не сообщайте ПИН-код третьим лицам, в том числе родственникам, знакомым, сотрудникам банка, кассирам и лицам, помогающим вам в использовании платежной карты. Ответственность за все совершенные по счету операции несете вы как владелец карты.
6. ПИН-код необходимо запомнить, а в случае если это является затруднительным, хранить его отдельно от платежной карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте.
7. Никогда ни при каких обстоятельствах не передавайте платежную карту для использования третьим лицам, в том числе родственникам. Если на платежной карте нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать платежную карту.
8. Будьте внимательны к условиям хранения и использования платежной карты. Не подвергайте платежную карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Платежную карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.
9. Телефон круглосуточной службы поддержки (Контакт-центра) указан на оборотной стороне платежной карты. Также необходимо всегда иметь при себе телефоны круглосуточной службы поддержки, Банка, и номер платежной карты на других носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации, но не рядом с записью о ПИН-коде. При этом рекомендуется номер платежной карты хранить (указывать) таким образом, чтобы при его обнаружении третьими лицами невозможно было сделать предположение о том, что это номер платежной карты.
10. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета целесообразно установить суточный лимит на сумму операций по платежной карте и одновременно подключить услугу SMS-информирования.
11. При получении просьбы, в том числе со стороны сотрудника АО Банк «Развитие-Столица», сообщить персональные данные или информацию о платежной карте (в том числе ПИН-код) не сообщайте их. Перезвоните в АО Банк «Развитие-Столица» или по телефону, указанному на оборотной стороне платежной карты, и сообщите о данном факте.
12. Не рекомендуется отвечать на электронные письма, в которых от имени Банка предлагается предоставить персональные данные. Не следуйте по «ссылкам», указанным в письмах (включая ссылки на сайт кредитной организации), т.к. они могут вести на сайты-двойники.
13. В целях информационного взаимодействия с Банком рекомендуется использовать только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных web-сайтов/порталов, обычной и электронной почты и пр.), которые указаны в документах,

полученных непосредственно в офисах АО Банк «Развитие-Столица».

14. Помните, что в случае раскрытия ПИН-кода, номера платежной карты, персональных данных, утраты платежной карты существует риск совершения неправомерных действий с денежными средствами на вашем банковском счете со стороны третьих лиц.

В случае если имеются предположения о раскрытии ПИН-кода, номера платежной карты, персональных данных, позволяющих совершить неправомерные действия с вашим банковским счетом, а также, если платежная карта была утрачена, необходимо немедленно обратиться в банк или Контакт-центр, заблокировать карту и следовать указаниям сотрудника. До момента обращения в банк вы несете риск, связанный с несанкционированным списанием денежных средств с вашего банковского счета. Согласно условиям «Правил выпуска и обслуживания платежных карт «МИР» АО Банк «Развитие-Столица» для физических лиц» денежные средства, списанные с вашего банковского счета в результате несанкционированного использования вашей платежной карты до момента уведомления об этом банка, не возмещаются.

15. Сохраняйте чеки в течение 60 календарных дней для самостоятельного контроля расходов: при получении выписки вы сможете сверить списанные суммы с вашими реальными покупками. Также Вы обязаны их предоставить в течение 3 дней по требованию Банка в целях урегулирования спорных вопросов.

16. Некоторые торгово-сервисные точки (например, гостиницы, пункты проката автомобилей) в качестве гарантии платежеспособности клиента до фактического оказания услуг блокируют необходимую сумму на счете карты, как при проведении оплаты. Окончательно сумма списывается со счета только после оказания услуг. Если услуга не была оказана - сумма будет автоматически разблокирована.

Рекомендации при совершении операций с платежной картой в банкомате

1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).
2. Не используйте устройства, которые требуют ввода ПИН для доступа в помещение, где расположен банкомат.
3. В случае если поблизости от банкомата находятся посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом.
4. Перед использованием банкомата осмотрите его на наличие дополнительных устройств, несоответствующих его конструкции и расположенных в месте набора ПИН и в месте (прорезь), Приложение 4 предназначенном для приема карт (например, наличие неровно установленная клавиатура набора ПИН). В указанном случае воздержитесь от использования такого банкомата.
5. В случае если клавиатура или место для приема карт банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержитесь от использования платежной карты в данном банкомате и сообщите о своих подозрениях сотрудникам банка по телефону, указанному на банкомате.
6. Не применяйте физическую силу, чтобы вставить платежную карту в банкомат. Если платежная карта не вставляется, воздержитесь от использования такого банкомата.
7. Набирайте ПИН-код таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН-кода прикрывайте клавиатуру рукой.
8. В случае если банкомат работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого банкомата, отменить текущую операцию, нажав на клавиатуре кнопку «Отмена», и дождаться возврата платежной карты.
9. После получения наличных денежных средств в банкомате следует пересчитать банкноты полистно, убедиться в том, что платежная карта была возвращена банкоматом, дождаться выдачи квитанции при ее запросе, затем положить их в сумку (кошелек, карман) и только после этого отходить от банкомата.

10. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.
11. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с платежной картой в банкоматах.
12. Если при проведении операций с платежной картой в банкомате банкомат не возвращает платежную карту, следует, не отходя от банкомата, связаться по телефону со службой клиентской поддержки (Контакт-Центр) Банка, описать сложившуюся ситуацию и осуществить блокирование платежной карты, а если операция проводилась в банкомате иной кредитной организации, то необходимо также позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего.
13. Внимательно читайте сообщения на экране банкомата - сторонние банки могут взимать дополнительные комиссии.

Рекомендации при использовании платежной карты для безналичной оплаты товаров и услуг

1. Не используйте платежные карты в организациях торговли и услуг, не вызывающих доверия.
2. Требуйте проведения операции с использованием карты в вашем присутствии. Старайтесь не допускать исчезновения карты из поля зрения даже на незначительное время. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на платежной карте.
3. При использовании платежной карты для оплаты товаров и услуг кассир может потребовать от владельца платежной карты предоставить паспорт, подписать чек или ввести ПИН. Перед набором ПИН следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке.
4. В случае если при попытке оплаты платежной картой имела место "неуспешная" операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.
5. Не забудьте забрать карту после проведения операции. Убедитесь в том, что это именно ваша карта.
6. Если вы решили отказаться от покупки - верните покупку в магазин, предъявите документ, удостоверяющий личность, чек и карту, с помощью которой была совершена покупка. Кассир выполнит операцию возврата, и деньги будут возвращены на счет карты. Сумма покупки наличными не возвращается.

Меры безопасности при совершении операций через сеть Интернет

1. Не совершайте покупки в интернет-магазинах, используя перевод средств с карты на карту.
2. Не используйте ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.
3. Не сообщайте персональные данные или информацию о банковской(ом) карте (счете) через сеть Интернет, например, ПИН, пароли доступа к ресурсам банка, срок действия платежной карты, установленные лимиты, историю операций, персональные данные.
4. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в сети Интернет использовать отдельную платежную карту, пополняя ее непосредственно перед оплатой.
5. Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.
6. Пользуйтесь услугами только проверенных интернет-магазинов, которые поддерживают технологии 3D Secure (при проведении операций запрашиваются коды подтверждения из SMS).
7. Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.

8. Рекомендуется совершать покупки только со своего компьютера (или иного устройства) в целях сохранения конфиденциальности персональных данных и информации о банковской(ом) карте (банковском счете).
9. Установите на свой компьютер лицензионное антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых вами программных продуктов (операционной системы и прикладных программ), это может вам защититься от проникновения вредоносного программного обеспечения.

Меры безопасности за пределами Российской Федерации

1. При использовании карты за границей будьте особенно внимательны - пользуйтесь банкоматами в отделениях банков или гостиницах, а покупки совершайте в крупных или престижных магазинах.
2. Не забывайте, что риск существует в любой стране, поэтому, прежде всего, будьте внимательны при использовании карты.

II. Меры безопасности при работе в Интернет-банк для физических лиц

1. Для входа в Интернет-банк необходимо ввести только логин и пароль. Не сообщайте никому свой логин и пароль доступа к Интернет-банку.
2. Используйте только доверенные компьютеры с лицензионным программным обеспечением. Проверяйте свои устройства на вирусы. Регулярно обновляйте программное обеспечение.
3. Проверьте, что веб-адрес в адресной строке начинается с «https». Иначе не входите в Интернет-банк!
4. Не сообщайте никому свои персональные данные, так же Логин и Пароль доступа в Интернет-банк, Одноразовые пароли подтверждения операции и реквизиты банковской карты. Банк не запрашивает у своих клиентов указанную информацию. Будьте бдительны: не отвечайте на подобные запросы, злоумышленники могут представиться кем угодно!
5. При проведении операций в Интернет-банке на Ваш мобильный телефон приходят сообщения с Одноразовыми секретными паролями для подтверждения операций в SMS и push сообщениях, убедитесь в том, что у посторонних нет доступа к указанным сообщениям. Установите ограничение доступа на телефон используя ПИН-код, графический ключ, пароль или воспользуйтесь другой технологией ограничения доступа к устройству.
6. Если вам пришло SMS с одноразовым паролем подтверждения для платежа, который вы не совершали, известите банк! Ни в коем случае не вводите и никому не сообщайте пришедший пароль!
7. Не указывайте номер мобильного телефона, на который приходят SMS с разовым паролем, в социальных сетях и других открытых источниках.
8. В случае утери мобильного телефона, на который приходят SMS с разовым паролем, немедленно заблокируйте SIM-карту! Если вы сменили номер мобильного телефона – обязательно сообщите в банк.
9. Если вам пришло уведомление о блокировке SIM-карты - немедленно сообщите в банк для блокировки доступа в Интернет-банк!
10. Запишите контактный телефон банка. Если вас просят связаться с банком по другому номеру, это может означать попытку мошенничества.
11. Устанавливайте мобильные приложения только из App Store и Google Play (разработчик - Center of Financial Technologies).

III. Меры безопасности при работе в Интернет-банк для юридических лиц

1. Храните носители ключей (смарт-ключи, USB-флеш, CD) в месте, недоступном посторонним лицам. Исключите хранение ключей на жёстком диске, в сетевых каталогах и прочих общедоступных ресурсах, либо используйте крипто-контейнеры.
2. Храните в тайне пароль доступа к ключу, исключите запись пароля на стикерах, носителях ключей и т.п., никому не сообщайте пароль по телефону, даже сотрудникам банка.

3. Подключите email или SMS/PUSH-уведомления об отправке платежей и при обнаружении подозрительных операций незамедлительно обращайтесь в банк!
4. Используйте встроенные средства блокировки и разблокировки мобильного телефона (логин/пароль для входа в ОС, логин/PIN-код/отпечаток пальца).
5. Используйте только доверенные компьютеры с лицензионными программами, установленным антивирусом. Регулярно проверяйте компьютер на вирусы, обновляйте операционную систему, браузеры и антивирусные базы.
6. Проверьте, что веб-адрес в адресной строке начинается с «https». Иначе не входите в Интернет-банк!
7. При работе с электронной почтой не открывайте письма, полученные от неизвестных отправителей, и вложения к ним, не переходите по ссылкам из таких писем.
8. Не используйте права администратора без крайней необходимости. В повседневной практике входите в систему, как пользователь без прав администратора.
9. При работе в Интернет не соглашайтесь на установку дополнительных программ.
10. По возможности используйте выделенный компьютер только для работы с Интернет-банком.
11. Не сохраняйте логин и пароль на общедоступных компьютерах/терминалах.
12. Храните в тайне номер банковской карты, срок ее действия, CVV/CVC/batch коды.
13. Запишите контактный телефон банка. Если вас просят связаться с банком по другому номеру, это может означать попытку мошенничества.
14. Если вам пришло SMS с одноразовым паролем подтверждения для платежа, который вы не совершали, известите банк! Ни в коем случае не вводите и никому не сообщайте пришедший пароль!
15. Устанавливайте мобильные приложения только из App Store и Google Play (разработчик - Center of Financial Technologies).