Памятка
«О мерах безопасного использования банковских карт»

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

Общие рекомендации

1. Никогда не сообщайте ПИН третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим Вам в использовании банковской карты.
2. ПИН необходимо запомнить 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.
3. Никогда ни при каких обстоятельствах не передавайте банковскую карту для использования третьим лицам, в том числе родственникам. Если на банковской карте нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать банковскую карту.
4. При получении банковской карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования банковской карты без Вашего согласия в случае ее утраты.
5. Будьте внимательны к условиям хранения и использования банковской карты. Не подвергайте банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.
6. Телефон кредитной организации-эмитента банковской карты (кредитной организации, выдавшей банковскую карту), указан на оборотной стороне банковской карты. Также необходимо всегда иметь при себе контактные телефоны кредитной организации-эмитента банковской карты и номер банковской карты на других носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации, но не рядом с записью о ПИН.
7. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета, целесообразно установить суточный лимит на сумму операций по банковской карте и, одновременно, подключить услугу оповещения посредством SMS-сообщений о проведенных операциях.
8. При получении просьбы, в том числе со стороны сотрудника кредитной организации, сообщить персональные данные или информацию о банковской карте (в том числе ПИН), не сообщайте их. Перезвоните в кредитную организацию-эмитент банковской карты и сообщите о данном факте.
9. Не рекомендуется отвечать на электронные письма, в которых от имени кредитной организации (в том числе кредитной организации-эмитента банковской карты) 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.
10. В целях информационного взаимодействия с кредитной организацией-эмитентом банковской карты 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 кредитной организации-эмитенте банковской карты.
11. Помните, что в случае раскрытия ПИН, персональных данных, утраты банковской 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, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а также, если банковская карта была утрачена, необходимо немедленно обратиться в кредитную организацию-эмитент банковской карты и следовать указаниям сотрудника данной кредитной организации. До момента обращения в кредитную организацию-эмитент банковской карты Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета. Согласно условиям договора с кредитной организацией-эмитентом банковской карты, денежные средства, списанные с Вашего банковского счета в результате несанкционированного использования Вашей банковской карты до момента уведомления об этом кредитной организации-эмитента банковской карты, не возмещаются.

Рекомендации при совершении операций с банковской 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, не соответствующих его конструкции и расположенных в месте набора ПИН и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры 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 банковской карты в данном банкомате и сообщите о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.
6. Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.
7. Набирайте ПИН таким образом, что бы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН 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 банковской карты.
9. После получения наличных денежных средств в банкомате, следует пересчитать банкноты полистно, убедиться в том, что банковская 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 банковской картой в банкоматах.
12. Если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в кредитную организацию-эмитент банковской карты, которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника кредитной организации.

Рекомендации при использовании банковской карты для безналичной оплаты товаров и услуг
1. Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.
2. Требуйте проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте.
3. При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской 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 банковской картой имела место «не успешная» операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

Рекомендации при совершении операций с банковской картой через сеть Интернет
1. Не используйте ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.
2. Не сообщайте персональные данные или информацию о банковской (ом) карте (счете) через сеть Интернет, например, ПИН, пароли доступа к ресурсам банка, срок действия банковской карты, кредитные лимиты, историю операций, персональные данные.
3. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в сети Интернет использовать отдельную банковскую карту (так называемую виртуальную карту) с предельным лимитом, предназначенную только для указанной цели и не позволяющую проводить с ее использованием операции в организациях торговли и услуг.
4. Следует пользоваться Интернет-сайтами только известных и проверенных организаций торговли и услуг.
5. 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.
6. Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и (или) информации о банковской (ом) карте (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 персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).
7. Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ), это может защитить Вас от проникновения вредоносного программного обеспечения.

Рекомендации по безопасному использованию ДБО Системы «Интернет-Банк»
1. Установите, обновите и используйте антивирус на вашем компьютере. Вирусные программы могут запоминать и отсылать всю информацию злоумышленникам. Если у вас есть подозрение, что ваш пароль украден, как можно быстрее смените ваш пароль в ДБО Системе «Интернет-Банк». Используйте современное антивирусное программное обеспечение и следите за его регулярным обновлением. Регулярно выполняйте антивирусную проверку на своем компьютере для своевременного обнаружения вредоносных программ.
2. Проверяйте адрес ДБО Системы «Интернет-Банк», он должен быть https://banksaratov.handybank.ru. Вас могут пытаться обмануть, предлагая оставить ваши пароль и логин на поддельном сайте. Проверяйте, действительно ли соединение происходит в защищенном режиме SSL — в адресной строке вашего веб-браузера должен быть изображен значок закрытого замка (справа или слева, в зависимости от браузера).

3. Для входа в ДБО Систему «Интернет-Банк» нужен только логин и пароль. Никому не говорите ваш пароль и одноразовый код. Сотрудники Банка или круглосуточной Службы поддержки ДБО Системы «Интернет-Банк» никогда не просят сообщить или ввести куда-либо конфиденциальную информацию (ваши персональные данные, номер карты, пароль или одноразовый код по SMS). Одноразовый код по SMS действует только для подтверждения платежа. Отменить операцию в ДБО Системе «Интернет-Банк» невозможно. Никто никогда не попросит у вас ввести одноразовый код для отмены операции.
4. Внимательно проверяйте параметры операции в SMS-сообщении, содержащем одноразовый код. Информация в нем должна совпадать с вашей операцией в ДБО Системе «Интернет-Банк», которую вы хотите подтвердить. Если эта информация не совпадает, не вводите одноразовый код и сообщите об этом в Банк или круглосуточную Службу поддержки ДБО Системы «Интернет-Банк».
5. Для звонков в Банк или круглосуточную Службу поддержки ДБО Системы «Интернет-Банк» используйте номера телефонов, указанных на вашей карте, на сайте Банка по адресу: www.banksaratov.ru, Условиях комплексного банковского обслуживания физических лиц в ООО Банк «Саратов». Часто мошенники на поддельных сайтах указывают неправильные номера, которые могут быть недоступны или по ним ответит оператор, который будет пытаться вас обмануть.
6. Не устанавливайте на компьютер приложения, полученные из неизвестных Вам источников. Помните, что Банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS/MMS/E-mail-сообщения.
7. Не используйте для доступа к «Интернет-банку» общедоступные сети Wi-Fi, а так же общедоступные компьютеры (интрнет-кафе, библиотеки и т.п.)
7. При утере/смене номера телефона незамедлительно сообщите об этом Банку. При утере также необходимо оперативно обратиться к Вашему оператору сотовой связи заблокировать SIM-карту.
8. Регулярно контролируйте состояние своих Карт и незамедлительно сообщайте сотрудникам Банка обо всех подозрительных или несанкционированных операциях.
9. В случае появления у Банка подозрения на проведение несанкционированной операции от Вашего имени Банк по собственной инициативе может временно заблокировать использование «Интернет-Банка». Для разблокировку Вам необходимо будет обратиться в Банк для подтверждения легитимности совершенных операций.
10. Обеспечивайте защиту от фишинга. В целях эффективного противодействия методам социальной инженерии рекомендуем Вам:

- не открывать присланные электронные письма от неизвестных Вам адресатов;
- не открывать ссылки на интернет-страницы, указанные в письмах неизвестных Вам адресатов;

не скачивать и не запускать подозрительные файлы или приложения из недоверенных источников сети Интернет или электронной почты.

Дополнительные рекомендации по безопасному использованию Мобильного приложения ДБО Системы «Интернет-Банк».

1. Используйте только официальное мобильное приложение установленное из официальных репозиториев производителей мобильных операционных систем.
2. Используйте антивирусное программное обеспечение для своих мобильных устройств и своевременно обновляйте его.
3. Своевременно обновляйте операционную систему своего мобильного устройства.
4. При установке нового ПО на мобильное устройство обратите внимание на разрешения, которое данное ПО запрашивает (особенно на доступ к SMS-сообщениям). Если новое ПО не вызывает Вашего доверия, лучше отказать от его установки.
5. Не вносите несанкционированные изменения в операционную систему своего мобильного устройства, это может существенно увеличить уязвимость устройства к заражению вирусами.
6. Установите парольную защиту на мобильное устройство.
7. Не используйте мобильное устройства для доступа к полнофункциональной версии «Интернет-банка». Используйте специализированное мобильное приложение.
8. Завершайте работу в мобильном приложении штатными средствами ПО (через кнопку «Выход»).