Приложение №3
к Условиям комплексного банковского обслуживания
физических лиц в ООО Банк «Саратов»

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 снизить 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 НИКОМУ (в том числе родственникам, знакомым, сотрудникам кредитной организации,) НЕ СООБЩАЙТЕ:
   - ДАННЫЕ КАРТЫ (полный номер банковской карты, трехзначный код с оборотной стороны карты);
   - ПИН-КОД;
   - ЛОГИН И ПАРОЛЬ ИНТЕРНЕТ – БАНКА И МОБИЛЬНОГО ПРИЛОЖЕНИЯ;
   - КОДЫ ИЗ SMS – СООБЩЕНИЙ и PUSH - СООБЩЕНИЙ;
   - ПЕРСОНАЛЬНЫЕ ДАННЫЕ.
2. Для минимизации риска телефонного мошенничества обращаем Ваше внимание, что сотрудники банка никогда:
   - не осуществляют звонки с просьбой предоставления персональных данных, номеров карт, одноразовых паролей из СМС для подтверждения финансовых операций;
   - не просят коды из СМС для отмены совершенных «мошеннических «операций»;
   - не предлагают для сохранности перевести деньги на специальные или «безопасные» счета, установить специальные программы для обеспечения удаленного доступа и управления компьютерами (TeamViewer, RDP, Radmin и пр.).
3. ПИН-код 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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 или push-уведомлений о проведенных операциях.
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 по телефону Центра обслуживания Держателей карт ООО Банк «Саратов», размещенному на web-сайте Банка в сети Интернет по адресу: www.banksaratov.ru и в Мобильном приложении «Банк Саратов»;

- для блокировки карты: по телефонам круглосуточного Центра обслуживания Держателей карт (ЗАО Процессинговый Центр «КартСтандарт») размещенным на web-сайте Банка в сети Интернет по адресу: www.banksaratov.ru и в Мобильном приложении «Банк Саратов»;
- для блокировки Интернет-банка и мобильного приложения: по телефону Центра обслуживания Держателей карт ООО Банк «Саратов», размещенному на web-сайте Банка в сети Интернет по адресу: www.banksaratov.ru и в Мобильном приложении «Банк Саратов».

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, чтобы 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. При оплате в интернет-магазине убедитесь, что сайт работает через защищенное соединение – адрес сайта должен начинаться с https://.
6. 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.
7. 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).
8. 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 ИНТЕРНЕТ-БАНКА И МОБИЛЬНОГО ПРИЛОЖЕНИЯ Банк «Саратов»

1. Создайте сложный пароль из букв и цифр для входа в интернет-банк и мобильные приложения и храните его в секрете.
2. Используйте только официальное мобильное приложение установленное из официальных магазинов App Store и Google Play. Разработчик мобильного приложения JSC Center of Financial Technologies.
3. Для входа в интернет-банк используйте только официальный сайт банка.
4. Используйте лицензионную операционную систему на Вашем компьютере.
5. Используйте антивирусное программное обеспечение для компьютера и мобильных устройств, своевременно обновляйте его.
6. Своевременно обновляйте операционную систему своего компьютера и мобильного устройства.
7. 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 отказаться от его установки.
8. Не вносите несанкционированные изменения в операционную систему своего мобильного устройства (перепрошивка, установка ROOT прав), это может существенно увеличить уязвимость устройства к заражению вирусами.
9. Установите парольную защиту на мобильное устройство.
10. Никому не сообщайте пароль и одноразовые коды из sms-сообщениq или push-уведомлениq, даже родственникам, друзьям и сотрудникам банка. Пароли и коды запрашивают только мошенники.
11. Не открывайте подозрительные ссылки от неизвестных отправителей.
12. Завершайте работу в мобильном приложении штатными средствами ПО (через кнопку «Выход»).
13. При утере телефона/SIM карты необходимо незамедлительно сообщить об этом в Банк, также оперативно обратиться к Вашему оператору сотовой связи и заблокировать SIM-карту. При смене номера телефона необходимо сообщить об этом в Банк, для внесения соответствующих изменений.