ПАМЯТКА «О МЕРАХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ»

Соблюдение рекомендаций, содержащихся в Памятке, позволит обеспечить максимальную сохранность банковской карты, ее реквизитов, ПИН-кода 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. Банковская карта является Вашим средством доступа к денежным средствам, находящимся на Вашем банковском счете, поэтому отношение к ее использованию и хранению должно быть аналогично отношению к наличным денежным средствам!

Конфиденциальной информацией являются : полный номер карты, срок ее действия, ПИН-код, CVV2/CVC2-код. **ПИН-код** – 4 цифры, содержащиеся в отдельно выданном Вам ПИН-конверте – используется в банкоматах и терминалах. **CVV2/CVC2-код** – 3 цифры, отпечатанные на оборотной стороне карты – используется при покупках через сеть Интернет.

Общие рекомендации

1. Никогда не сообщайте ПИН-код или CVV2/CVC2-код третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим Вам в использовании банковской карты.
2. ПИН-код необходимо запомнить или, в случае если это является затруднительным, хранить его отдельно от банковской карты в неявном виде и в 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. Картой имеет право пользоваться только то лицо, на чьё имя выпущена карта (за исключением подарочных карт).
4. 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.
5. При получении банковской карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты. Это снизит риск использования банковской карты без Вашего согласия в случае ее утраты.
6. Телефон круглосуточной службы поддержки Банка для держателей банковских карт указан на оборотной стороне банковской карты. Необходимо всегда иметь при себе этот контактный телефон в записной книжке, мобильном телефоне и/или других носителях информации.
7. При получении посторонней просьбы (в том числе даже от лиц, представляющихся сотрудниками Банка) сообщить под любым предлогом (проверка, блокирование операции, подтверждение оплаты и т.п.) персональные данные или информацию о банковской карте (ее номер, срок действия, ПИН-код и/или CVV2/CVC2-код), не сообщайте их. Перезвоните в Банк по номеру, указанному на оборотной стороне карты, и сообщите о данном факте.
8. 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 Банке.
9. Дополнительная защита от мошенничества при совершении операций в сети Интернет обеспечивается подключением банковской карты к бесплатному сервису «Безопасные платежи в Интернете» (технология "3D Secure"/«MirAccept»). Подключение к сервису обеспечивается автоматически при предоставлении Основного номера мобильного телефона. При совершении Интернет-операций на Ваш Основной номер мобильного телефона с помощью SMS будет высылаться уникальный одноразовый пароль, известный только Вам. Никогда не сообщайте посторонним лицам (даже выдающим себя за работников Банка), SMS-пароли для подтверждения покупки.
10. Не реже раза в месяц получайте выписку по Вашим карточным счетам в отделении Банка или оформите заявление о ежемесячном предоставлении ее Вам по электронной почте. Эта информация позволит Вам своевременно заявить в Банк о несогласии с операцией (например, в случае повторного списания средств по ранее уже оплаченной Вами операции).

11. Не отключайте без необходимости телефон, на который должны приходить сообщения об операциях и/или одноразовые коды "3D Secure""/«MirAccept». При смене номера мобильного телефона не забудьте незамедлительно уведомить об этом Банк! Замена номера мобильного телефона для целей уведомления клиента об операциях по банковской карте производится при личном обращении клиента (с паспортом) в любое отделение Банка.
12. Не рекомендуется отвечать на электронные письма, в которых от имени Банка предлагается предоставить персональные данные. Не следуйте по "ссылкам", указанным в письмах, т.к. они могут вести на сайты-двойники.
13. Не переводите деньги сомнительным личностям и организациям за заведомо несуществующий товар или услугу (не реагируйте на сообщения о сомнительных выигрышах в лотереях, получения бонусов).

Операции в банкомате / информационном киоске

1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.). Не используйте устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат.
2. Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его привычному виду, конструкции и расположенных в месте набора ПИН-кода и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры). Воздержитесь от использования такого банкомата.
3. Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.
4. В случае если поблизости от банкомата находятся подозрительные посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом. Всегда набирайте ПИН-код таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН-кода прикрывайте клавиатуру рукой.
5. 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.
6. При запросе наличных денежных средств в банкомате после завершения операции извлеките банковскую карту, извлеките и пересчитайте банкноты полистно, дождитесь выдачи квитанции (при ее запросе), затем положите денежные средства и карту в сумку (кошелек, карман) и только после этого отходите от банкомата.
7. Сохраняйте распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.
8. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.
9. 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 Банк, и далее следовать инструкциям сотрудника кредитной организации.

Безналичная оплата 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. Не разрешайте уносить Вашу карту из поля Вашего зрения.
3. 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 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.

Операции через сеть Интернет

1. Не используйте ПИН-код при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.
2. Не пересылайте через сеть Интернет в незащищенном виде персональные данные или информацию о банковской карте (номер, ПИН-код, CVV2/CVC2-код, пароли доступа, срок действия карты, историю операций, другие 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, предназначенную только для указанной цели. Старайтесь поддерживать на этой карте минимальный остаток денежных средств.
4. Пользуйтесь 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 (особенно, если ссылка на сайт получена Вами по электронной почте), т.к. схожие (отличающиеся на 1-2 буквы) адреса могут использоваться злоумышленниками для кражи данных Вашей банковской карты. Все известные Интернет-сайты используют защищенное соединение для расчетов с использованием банковских карт (в браузере перед именем сайта отображается префикс https: а не http:, строка адреса или ее часть выделена зеленым фоном, текст на зеленом фоне совпадает с латинским наименованием компании). Если у Вас возникли подозрения при использовании Интернет-сайта (изменился его внешний вид, исчез зеленый фон в адресной строке браузера) – воздержитесь от ввода данных банковской карты.
6. По возможности осуществляйте Интернет-покупки только со своего компьютера с установленным антивирусным программным обеспечением 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. В случае если покупка совершается с использованием чужого компьютера, не сохраняйте на нем Ваши персональные данные и данные банковской карты. После завершения всех операций убедитесь, что введенная Вами информация не сохранилась (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).
7. Для обеспечения безопасных расчетов с использованием банковской карты в сети Интернет настоятельно рекомендуем Вам подключить сервис «SMS-информирование». Данный способ информирования Клиента является наиболее оперативным и позволяет Клиенту своевременно контролировать операции по Карте. Поскольку кража реквизитов банковской карты возможна не только через интернет, данный сервис предоставит Вам дополнительную защиту независимо от того, используете ли Вы свою карту в сети Интернет или нет.
8. По возможности не используйте один и тот же смартфон для совершения Интернет-покупок и получения уникальных SMS-паролей – в случае заражения его вирусом злоумышленники смогут преодолеть защиту "3D Secure""/«MirAccept».
9. Если Вы что- то покупаете или продаете через известные интернет-аукционы или торговые площадки (Авито, Юла, Джум.), то следует совершать все операции через стандартные механизмы сервисов. Не открывайте ссылки, которые Вам дает партнер по сделке. Их легко подделать, не доверяйте мошенникам;

Путешествия

1. Если вы отправляетесь в путешествие, подключитесь к услуге SMS-информирования. Это позволит Вам контролировать все операции, проводимые по Вашей карте, а также контролировать остаток денежных средств по счету, и в случае необходимости заблокировать карту во избежание финансовых потерь.
2. К странам с повышенным уровнем риска мошенничеств с банковскими картами относятся: Шри Ланка, Индия, Турция, Украина, Кипр, Болгария, Хорватия, Доминиканская Республика, Аргентина, Венесуэла, ОАЭ, Китай, Малайзия, Тайвань, Гонконг, Индонезия, Филиппины, Таиланд. В указанных государствах следует пользоваться пластиковой картой с особой осторожностью и как можно строже соблюдать все рекомендованные правила:
   - проводить осмотр банкомата перед совершением в нем операции;
   - обращать внимание на отсутствие дополнительно установленных элементов на устройстве (накладок), предназначенном для чтения карты, и на клавиатуре банкомата;
   - по возможности пользоваться банкоматами, расположенными на территории банков;
   - закрывать ПИН при вводе на банкомате от посторонних лиц;
   - не выпускать карту из вида, следить за действиями персонала при ее использовании.
3. Обращаем Ваше внимание на то, что звонки на номер круглосуточной Службы поддержки держателей банковских карт 8-800-100-55-22 являются бесплатными на территории Российской Федерации, однако, вне России данный номер не обслуживается. Для звонков из-за рубежа следует использовать телефон +7 (8202) 51-61-51 (указан вторым на оборотной стороне карты и на сайте Банка).
4. Рекомендуется брать с собой дополнительную карту, чтобы использовать ее при экстренной блокировке основной карты.

Экстренные случаи

Если Вы утратили карту или у Вас есть подозрения о том, что кому-либо стали известны данные Вашей карты или Ваши персональные данные, а так ПИН-код, CVV немедленно сообщайте о ситуации по телефону дежурной службы поддержки держателей банковских карт Банка 8-800-100-55-22 или 8-8202-51-61-51 для блокировки карты, или отправьте SMS-сообщение о блокировке Карты в рамках подключенного сервиса «SMS информирование» на номер +79210000830 с текстом BLOCK<пробел><шесть первых цифр номера карты>%<четыре последних цифры номера карты><пробел><Статус>, где статус равен 06-утеряна, 07-украдена.(Например: BLOCK 666666%4444 07) , а также возможно заблокировать карту через «СГБ-Онлайн/СГБ-Мобайл» и как можно скорее обращайтесь с письменным заявлением в Банк. Своевременная блокировка карты позволит снизить риск ее несанкционированного использования. До момента обращения в Банк/Контактный центр Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета.

Обращаем Ваше внимание, что Банк никогда:

1. не отправляет сообщения с просьбой подтвердить, обновить или предоставить персональные данные (ФИО, данные документа, удостоверяющего личность, номер мобильного телефона, информацию банковской карты, CVV, ПИН-код, контрольную информацию и пр.);
2. не отправляет сообщения с формой для ввода Ваших персональных данных;
3. не просит Вас зайти в личный кабинет системы «СГБ-Онлайн/СГБ-Мобайл» по ссылкам в письма.

Участились случаи, когда мошенники звонят клиентам Банка и сообщают о том, что карта заблокирована или другую недостоверную информацию, в результате чего, клиент банка перезванивает по указанному номеру. Злоумышленники представляются банковскими сотрудниками и предлагают выполнить определенные действия для разблокировки карточки. Чтобы этого избежать придерживайтесь простых правил безопасности описанных в данной памятке.