

Общие меры безопасности при совершении операций по банковской карте

1. Ваш ПИН-код является аналогом собственноручной подписи и используется для доступа к денежным средствам на Вашем счете. Никому не сообщайте ПИН-код, в том числе родственникам, знакомым, кассирам и людям, помогающим Вам в использовании карты. Кроме Вас никто не знает ПИН-код (даже сотрудники банка). При получении через электронную почту писем от Банка с просьбой подтвердить данные своей карты и сообщить свой ПИН, сообщите об этом в Банк и ни в коем случае не следуйте указанным в письме инструкциям. Имитирование запросов от банков с просьбой подтверждения данных держателей карт (владельцев счета) является одним из видов мошенничества, позволяющим получить конфиденциальные данные о карте для последующего их использования в мошеннических целях.

2. Запомните ПИН-код или, если не можете этого сделать, храните его отдельно от карты в неявном виде и недоступном для посторонних месте. Помните, ответственность за все операции с использованием ПИН-кода всегда возлагается на клиента.

3. Не передавайте карту другим лицам, только держатель банковской карты, чье имя на ней написано, имеет право её использовать.

4. При получении карты распишитесь шариковой ручкой на обратной её стороне в месте, предназначенном для подписи держателя банковской карты (если данное поле предусмотрено действующими правилами платежной системы). Подпись на карте является образцом для сверки при оформлении операций с использованием карты в присутствии кассира и служит для предотвращения несанкционированного использования карты.

5. Предохраняйте карту от сильных механических, температурных и электромагнитных воздействий.

6. Регулярно получайте выписки по Вашему счету в Банке или дополнительных офисах Банка в мобильном приложении Интернет-Банка и контролируйте все операции. Иногда возможность опротестовать операцию зависит от того, как быстро Вы заявили об этом в Банк.

7. Сохраняйте все документы по операциям с использованием карты, в том числе и по неуспешным операциям (попыткам).

8. Не сообщайте реквизиты своей карты (номер банковской карты, ее срок действия, три последние цифры на полосе для подписи) по открытым каналам связи, особенно в письмах электронной почты, где они могут стать добычей мошенников. В случае, если предоставление данных необходимо для проведения операции оплаты (операции по телефону, через интернет, факс для бронирования отеля, тура), старайтесь пользоваться услугами компаний с безупречной репутацией и использовать максимально безопасный способ предоставления данных (например, Интернет сайты с использованием современных технологий защиты данных). Помните о том, что ПИН-код не входит в число реквизитов карты для удаленного проведения операций, соответственно, предоставление Вами кому-либо информации о ПИН-коде (под каким бы предлогом она ни требовалась) должно быть исключено.

9. При звонке по телефону от имени сотрудника Банка с просьбой сообщить конфиденциальные данные запишите Ф.И.О., должность и номер телефона звонившего; ничего не сообщайте ему, после этого перезвоните в Банк по имеющимся у вас телефонам (например, по указанному на оборотной стороне карты) и сообщите о случившемся.

10. Сотрудники Банка никогда и ни при каких условиях не должны спрашивать у вас реквизиты карты.

11. Если вы считаете, что какая-либо персональная информация была раскрыта, то немедленно свяжитесь с Банком.

12. Застраховать себя от больших потерь Вы можете, установив суточный лимит на сумму операций по своей карте. Если Вам понадобится снять сумму, превышающую сумму лимита, всегда можно обратиться в Банк и на время повысить лимит.

13. Используйте систему информирования об операциях по карточке по мобильному телефону при помощи SMS-сообщений. Это позволит не только сразу же узнать о несанкционированной Вами операции по карте, но и принять решение об экстренной блокировке карты.

14. Относитесь к хранению карточки также как Вы относитесь к наличным денежным средствам.

15. Запишите и всегда храните с собой, но отдельно от карточки, номер Вашей карты, номер телефона Банка, кодовое слово, по которому Банк аутентифицирует Вас как законного держателя. Эта информация будет необходима Вам в случае возникновения каких-либо проблем с карточкой (например, в случае ее утраты).

16. Если Вы утратили карту или в результате какой-либо подозрительной ситуации Вам показалось, что Ваш ПИН-код стал известен посторонним людям, немедленно сообщайте об этом по телефону круглосуточной Службы поддержки держателей банковских карт: +7 (495) 785-15-15. После блокировки карты обязательно направьте в Банк письменное заявление о ее утрате, так как согласно Условий использования карт Вы несете ответственность за все операции с картой до даты направления в Банк письменного заявления о ее утрате включительно. Своевременная блокировка карты позволит снизить риск ее несанкционированного использования

Меры безопасности при использовании банковской карты в сети Интернет

1. Не отвечайте на электронные письма, в которых якобы от имени Банка Вас просят предоставить персональную информацию. Свяжитесь с Банком по номеру телефона, который известен Вам как истинный, чтобы выяснить подлинность письма.

2. Никогда не следуйте по ссылкам в таких письмах (даже на сайт банка), т.к. они могут вести на мошеннические сайты.

3. Никогда не раскрывайте через Интернет-ресурсы такую информацию как ПИН-код и пароли доступа к ресурсам Банка.

4. Для оплаты покупок через сайты в сети Интернет лучше использовать отдельную карту (с отдельным счетом или ограниченным лимитом), предназначенную только для данной цели. Денежные средства на нее рекомендуется переводить непосредственно перед намерением совершить покупку в объеме немногим больше планируемых расходов.

5. Пользуйтесь услугами только известных и проверенных торговых предприятий. Предпочтение необходимо отдавать предприятиям, подключенным к программам Verified by Visa (Проверено Визой) и SecureCode (Безопасный Код), MirAccert

6. Убедитесь, что у вас есть возможность связаться с торговцем в случае спорной ситуации или вопроса. Убедитесь в правильности адресов (телефонов), данных на странице.

7. Проверяйте адреса Интернет-сайтов, к которым Вы подключаетесь, т.к. злоумышленники могут использовать похожие названия для создания мошеннических ресурсов.

8. Избегайте пользоваться услугами Интернет-ресурсов сомнительного содержания; зачастую они создаются специально для получения информации о банковских картах и последующего ее неправомерного использования.

9. Если есть какие-либо подозрения по странице, или вы не хотите предоставлять детали по карте или персональные сведения, то покиньте страницу, сообщите о подозрениях в банк, произведите покупку в другом месте.

10. Контролируйте свою электронную почту, не открывайте сообщения от неизвестных адресатов, не передавайте свои личные данные. В случае необходимости передать свою персональную информацию доверенному получателю используйте средства криптографической защиты, т.к. обычные почтовые послания могут быть перехвачены и использованы для нанесения вам вреда.

11. 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 защитит Вас от вирусов и других деструктивных программ.

12. Установите на компьютер межсетевой экран (firewall), который поможет предотвратить неавторизованный доступ к вашему компьютеру.

13. Совершайте покупки только со своего компьютера, не пользуйтесь Интернет-кафе и другими доступными средствами, где могут быть установлены программы-шпионы, запоминающие вводимые вами конфиденциальные данные.

14. Выбирайте нетривиальные пароли, которые не связаны с вашим днем рождения или другими персональными данными. Если возможно, выбирайте символно-цифровые пароли. Не записывайте пароли и никому не сообщайте их. Если Вы боитесь забыть свой пароль, придумайте понятную только Вам систему его записи (например, в виде номера телефона или адреса в телефонной книжке).

15. Соблюдайте осторожность при совершении оплаты с помощью карты на интернет-сайтах операторов мобильной связи, Интернет-провайдеров, игровых сайтах, социальных сетях и сайтах лотерей. Просьба производить данную оплату через терминалы, банкоматы, а также с помощью электронных кошельков.

Меры безопасности при использовании банковских карт в банкоматах и торгово-сервисных предприятиях:

1. Старайтесь пользоваться одними и теми же банкоматами, которые Вам хорошо известны.
2. В случае необходимости использовать новый банкомат, выбирайте хорошо освещенный и установленный в удобном месте.

3. Прежде чем подойти к банкомату, осмотрите окружающее пространство. В случае нахождения поблизости подозрительных людей, воспользуйтесь другим банкоматом.

4. Перед тем как подойти к банкомату, достаньте свою карточку и держите ее в руках. Не открывайте бумажник, кошелек, сумку, барсетку непосредственно около банкомата или в очереди к нему.

5. Перед использованием банкомата осмотрите его внешний вид. Если Вы обнаружите наличие каких-либо посторонних изделий, предметов, проводов, следов конструктивных изменений, воздержитесь от использования карты в таком банкомате.

6. Будьте особенно осторожны, если кто-то посторонний предлагает Вам около банкомата помощь, даже если у Вас застряла карточка или возникли проблемы с проведением операции. Не набирайте ПИН-код на виду у третьих лиц (включая друзей и родственников), не позволяйте себя отвлечь, т.к. в этот момент мошенники могут забрать из банкомата Вашу карточку или выданные денежные средства.

7. Если у банкомата за Вами находится очередь, убедитесь, что никто не может увидеть Ваш ПИН-код.

8. При вводе ПИН-кода находитесь как можно ближе к банкомату, вводите ПИН-код средним пальцем руки (при этом, ладонь руки оказывается раскрытой и злоумышленнику гораздо сложнее увидеть, какие кнопки Вы нажимаете), по возможности, второй рукой закрывайте клавиатуру от постороннего обзора.

9. Вводите ПИН-код только после того как банкомат попросит Вас об этом.

10. Не применяйте физическую силу, чтобы вставить карточку в банкомат.

11. Если Вам кажется, что банкомат работает неправильно, нажмите кнопку "отмена", заберите свою карточку и воспользуйтесь другим банкоматом. Если проблемы возникли после момента ввода запрошенной суммы, или банкомат захватил Вашу карту, не отходите от банкомата до тех пор, пока не убедитесь в завершении операции, отказе в выдаче или в появлении на экране приглашения провести новую операцию. В противном случае, после того как Вы отойдете от банкомата, он может вернуть карту или выдать запрошенные Вами денежные средства.

12. При невыдаче денежных средств обязательно дождитесь окончания операции, лучше при этом для уверенности провести запрос остатка.

13. После получения денежных средств положите наличность и карточку в бумажник, кошелек, сумку и т.п. и только после этого отходите от банкомата.

14. При пользовании карточкой в торговых предприятиях следите, чтобы карточка не исчезала из Вашего поля зрения. При необходимости ввести ПИН-код закройте клавиатуру рукой так, чтобы ни продавец, ни находящиеся рядом с Вами клиенты не видели введенных цифр. Если кто-то увидит Ваш ПИН-код, после этого карточку могут украсть и быстро снять все денежные средства в банкомате.

15. Перед тем, как ставить подпись на чеке или слипе, убедитесь в том, что указанная сумма совпадает с фактической. В случае, если в чеке не указана сумма или указанная сумма не совпадает с фактической, ни в коем случае не подписывайте чек.

16. В случае, если операция по карте приостановлена, необходимо убедиться в том, что Продавец отменил (отозвал) авторизацию производимой операции, в противном случае на счете карты на время будет заблокирована сумма неоконченной операции.