Общие рекомендации по мерам безопасности

Банковские карты Газпромбанка являются средством доступа к денежным средствам, находящимся на Вашем банковском счете, поэтому отношение к их использованию и хранению должно быть аналогично отношению к наличным денежным средствам. Чтобы использование банковских карт было удобным и приятным, а Ваши денежные средства оставались в сохранности, просим Вас обратить внимание на следующие простые правила и рекомендации.

1. Храните карту вне доступа третьих лиц, не передавайте карту и/или не сообщайте ее реквизиты (номер, срок действия, код безопасности на полосе для подписи) третьим лицам, кроме случаев, когда это требуется в процессе оплаты товаров/услуг.
2. Проявляйте аккуратность при хранении и вводе ПИНа (не храните записанным вместе с банковской картой). Помните о том, что ответственность за операции, совершенные с использованием ПИНа, возлагается на клиента.
3. Будьте бдительны при получении электронных писем или sms-сообщений якобы от имени Газпромбанка (например, о блокировке карты или каких-либо платежах), особенно если они содержат ссылки или номера телефонов для связи, отличные от телефонов на оборотной стороне Вашей карты. Ссылки в электронных письмах могут вести на мошеннический сайт. Не сообщайте никакой информации о себе и Ваших картах позвонившим лицам. При возникновении подозрений звоните в Газпромбанк по телефонам «горячей линии». Помните о том, что информация о коде безопасности карты (CVV2), ПИНе, а также о паролях/кодах на проведение/отмену операций никогда не запрашивается сотрудниками Газпромбанка!
4. Используйте услугу «Система Телекард» или ее бесплатный аналог с базовым функционалом - сервис «SMS-информирование» для контроля операций по своим банковским картам и управления суточным лимитом операций. Оперативное получение sms-уведомлений по операциям с Вашей банковской картой и возможность моментальной самостоятельной блокировки банковской карты без телефонного звонка в Газпромбанк позволит Вам своевременно отреагировать на несанкционированный доступ к карточному счету.
5. При совершении операций с использованием банковских карт в торгово-сервисных предприятиях или банкоматах таких стран, как Украина, Таиланд, США, Бразилия, Турция существует высокая вероятность того, что данные карты и ПИН станут доступны мошенникам без ведома держателя карты. Поэтому после посещения этих стран рекомендуется по возможности установить необходимый Вам суточный лимит расходования по карте и географические ограничения. Использование возможностей системы «Телекард» или сервиса «SMS-информирование» позволят Вам оперативно и просто управлять установленными Вами ограничениями со своего мобильного устройства. В целях повышения уровня безопасности использования карт рекомендуется применять систему ограничений ко всем Вашим картам, в том числе при использовании их на территории Российской Федерации.
6. Защиту карты от подделки обеспечивает наличие на карте встроенного чипа. В тех регионах мира, где платежными системами предусмотрено требование обслуживать чиповую Карту в электронных терминалах и банкоматах только по чипу и не допускается обслуживание чиповой карты по магнитной полосе, риск мошенничества по поддельным Картам минимален. Список таких регионов положен в основу формирования стандартной схемы предустановленных географических ограничений по картам Газпромбанка.
7. Банк предоставляет Вам возможность самостоятельного выбора регионов обслуживания и видов операций, разрешенных для Вашей банковской карты. Рекомендуется выпускать банковскую карту для использования только в регионе пребывания, и менять настройки в соответствии с планируемыми поездками. Подробнее о геоограничениях и возможностях управления ими здесь.
8. Защита от мошенничества по реквизитам банковской карты (в сети Интернет) обеспечивается подключением банковской карты к бесплатному сервису «Безопасные платежи в Интернете», за счет проведения дополнительной аутентификации платежей по технологии 3D Secure при операциях на сайтах с логотипами Verified By Visa/MasterCard SecureCode (защищенные сайты). Платежи на таких сайтах заведомо не предусматривают возможности опротестования в случае неподтверждения операции держателем карты, для их проведения предусмотрено введение одноразового пароля, направляемого в момент операции на номер

мобильного телефона. Поскольку кража реквизитов банковской карты возможна не только через интернет, данный сервис служит Вам независимо от того, используете ли Вы свою карту в интернете.

9. Не реже раза в месяц получайте выписку по Вашим карточным счетам в отделении Газпромбанка или оформите заявление о ежемесячном предоставлении ее Вам по электронной почте. Из-за специфики проведения расчетов через платежные системы, только из выписки можно почерпнуть полную информацию о движениях по счету. Эта информация позволит Вам своевременно заявить в Газпромбанк о несогласии с операцией (например, в случае повторного списания средств по ранее уже оплаченной Вами операции). Воспринимайте sms-уведомления об операциях и выписку из банкомата только как дополнительные источники информации.
10. Для звонков в Газпромбанк используйте только телефоны «горячей линии» Банка, указанные на оборотной стороне карты и на официальном сайте Банка.
11. Не отключайте без необходимости телефон, на который должны приходить сообщения об операциях! При смене номера мобильного телефона не забудьте незамедлительно уведомить об этом Газпромбанк. Замена номера мобильного телефона для целей уведомления клиента об операциях по банковской карте производится при личном обращении клиента (с паспортом) в любое отделение Газпромбанка, либо через банкоматы Газпромбанка.