



ПОЛЕЗНЫЕ СОВЕТЫ

При использовании банковской карты

Не сообщайте ПИН-код другим лицам, в том числе родственникам, знакомым и сотрудникам банков.

Не записывайте ПИН-код на карте и не храните его рядом с картой (в сумке, кошельке, в сотовом телефоне).

Установите суточный лимит по карте во избежание несанкционированного снятия всей суммы денежных средств с банковского счета.

Подключите услугу SMS-уведомления к своему номеру мобильного телефона в целях получения SMS-сообщений об операциях по Вашей карте.

Отключите услугу «мобильный банк» в случае утери телефона или SIM-карты (ее замены). Помните, что услуга «мобильный банк», подключенная к номеру телефона, является доступом к Вашему банковскому счету с использованием этого номера телефона.

Взаимодействуйте с банком только с использованием контактов, получаемых непосредственно от банка или иных официальных его источников (офисы, сайт и т.д.).

Сообщите незамедлительно в банк о необходимости блокировки счета, если Ваша карта потеряна, скомпрометирована или с нее без Вашего согласия списаны денежные средства.

При использовании банкомата и терминала

Пользуйтесь банкоматами и терминалами, установленными в местах, вызывающих доверие (гос. учреждения, офисы банков, крупные торговые комплексы, гостиницы, аэропорт).

Не используйте банкомат, если рядом находятся посторонние лица с подозрительным поведением и не вступайте в контакт с незнакомыми людьми у банкомата.

Воздержитесь от использования банкомата, если клавиатура или приемник карт оборудованы подозрительными устройствами или накладками.

Звоните в банк по телефону, указанному на банкомате, если банкомат не возвратил карту, а также в банк, выдавший карту, и следуйте инструкциям сотрудника банка.

Не передавайте карту другим лицам для оплаты товаров и услуг. Проведение операций с использованием терминалов должно происходить только в Вашем присутствии.

Закрывайте клавиатуру от посторонних глаз при вводе ПИН-кода.

Проверяйте правильность суммы операции на чеке, сохраняйте выданные чеки, если оплата в банкомате или терминале была проведена некорректно.



При использовании сети Интернет, получении электронных или SMS уведомлений



Совершайте покупки в сети Интернет на проверенных сайтах и желательно с помощью отдельной карты.

Обращайте внимание на адрес сайта, с которого осуществляется оплата. Он должен начинаться с «https://». Сайты, начинающиеся с «http://» или других символов, являются слабо защищенными.

Не используйте ПИН-код при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.

Не отвечайте на электронные письма и телефонные звонки, в которых от имени банка предлагается предоставить персональные данные или реквизиты карт.

Не следуйте по «ссылкам», указанным в электронных письмах (включая ссылки на сайты банков), так как они могут вести на сайты – двойники.

Используйте тариф мобильного оператора без доступа к сети Интернет, это позволит снизить риски вирусного заражения телефона, на номер которого поступают SMS-сообщения об операциях по Вашей карте.

Установите на компьютер и мобильный телефон антивирусное программное обеспечение и регулярно обновляйте его.