

Рекомендации по безопасной работе с пластиковыми картами

Банк рекомендует всем владельцам пластиковых карт следовать правилам безопасности:

Пин-код - ключ к вашим деньгам:

Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить. Относитесь к ПИН-коду как к ключу от сейфа с вашими средствами. Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё - в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.

Ваша карта - только ваша:

Не позволяйте никому использовать Вашу пластиковую карту - это всё равно что отдать свой кошелек, не пересчитывая сумму в нём.

Ни у кого нет права требовать ваш пин-код:

Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предложениями, не спешите её выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники. Помните: хранение реквизитов и ПИН-кода в тайне - это Ваша ответственность и обязанность.

Немедленно блокируйте карту при ее утере:

Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

Пользуйтесь защищёнными банкоматами:

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д. Граждане, пользующиеся банкоматами без видеонаблюдения, могут подвергнуться нападениям злоумышленников.

Опасайтесь посторонних:

Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом. Набирая ПИН-код, прикрывайте клавиатуру рукой. Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.

Банкомат должен быть «чистым»:

Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нём телефону.

Банкомат должен быть полностью исправным:

В случае некорректной работы банкомата - если он долгое время находится в режиме ожидания или самопроизвольно перезагружается - откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

Советуйтесь только с банком:

Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах. Свяжитесь с Вашим банком - он обязан предоставить консультационные услуги по работе с картой.

Не доверяйте карту официантам и продавцам:

В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

- Не используйте устройства, которые требуют ввода ПИН для доступа в помещение, где расположен банкомат.
- Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.
- При выдаче карты в банке, держатель расписывается на её обороте, на специально предназначенной полосе для подписи. Таким образом, он «заверяет» пластиковую карту своей подписью. Хотя это скорее формальность, чем реальная защита от мошенничества, но иногда в магазине карту без подписи просто не примут к оплате
- Храните телефонные номера службы поддержки клиентов банка и кодовое слово, зафиксированное в договоре в надежном, и что важно – в быстродоступном месте. Контакты банка присутствуют, как правило, на самой карте, но если вы её потеряете (её украдут или «съест» банкомат), то важно своевременно позвонить в банк и заблокировать карту. Поэтому занесите контакты себе в сотовый вместе с кодовым словом – оно может потребоваться для вашей идентификации при разговоре с сотрудником контактного центра. Пользуйтесь контактными данными, указанными в официальных (!) документах, выданных самим банком, чтобы не попасть на мошенников.
- Храните втайне сведения о карте (номер, окончание срока действия, секретный код SVC2/CVV2, пин-код др.). При звонке в банк у вас спросят ваше ФИО, паспортные данные и контрольную информацию. Если вдруг у вас спрашивают пин-код, или код SVC2/CVV2 (последние три цифры с обратной стороны карты) – это мошенники! Убедитесь, что номер, по которому вы звоните, действительно принадлежит банку.
- Никогда никуда ничего не отправляйте! Банки не присылают электронные письма и смс-сообщения с запросами указать конфиденциальные сведения или перейти на адрес сайта.

Не открывайте такие письма, это мошенничество. При приеме подозрительных звонков или смс, связанных с платежной картой, свяжитесь со службой поддержки банка.

- Своевременно перевыпускайте карточку. До истечения срока действия карты требуется подать в банк заявление о её перевыпуске. В некоторых случаях банк перевыпускает карточку автоматически. В любом случае, если вдруг с картой что-то не так – посмотрите, не закончился ли срок действия карты!
- Закрывайте неиспользуемые кредитные карты или дебетовые карты с овердрафтом.
- Не подвергайте карту воздействиям агрессивных сред и держите их подальше от магнитов. В современной карточке есть электронный чип и магнитная полоса – не допускайте попадания на неё жидкости, не оставляйте рядом с источниками тепла и магнитных волн (обогреватель, мобильный телефон, бытовая или офисная техника). Не носите в сумке с магнитной застёжкой и не кладите на металлические поверхности. Пластик не имеет антивандальной защиты – старайтесь его не царапать и использовать по назначению.
- 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.
- В случае если при попытке оплаты банковской картой имела место «неуспешная» операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.