

Рекомендации по безопасному осуществлению операций с платежными карточками

Операции с использованием банкомата:

- Не менее одного раза в месяц получайте в Банке контрольную выписку по карточному счету.
- Подключитесь к услуге GSM-banking*.
- Не используйте устройства, которые нуждаются в введении пин-кода для доступа в помещение, где расположен банкомат.
- Никому не сообщайте пин-код платежной карточки (далее - карточка), даже сотрудникам Банка.
- Набирайте пин-код на клавиатуре банкомата таким образом, чтобы третьи лица не смогли его увидеть.
- Отказывайтесь от помощи и не следуйте подсказкам третьих лиц во время осуществления операций через банкомат с использованием карточки.
- Прежде чем начать осуществление операции в банкомате:
 - обязательно осмотрите его на предмет наличия лишних дополнительных устройств/ приборов на клавиатуре и на устройстве, предназначенном для принятия карточек;
 - сравните внешний вид устройств банкомата с образцом на заставке банкомата.

**GSM-banking – это услуга Банка, которая предоставляет Вам возможность контролировать движение денег по карточному счету. При проведении каких-либо операций по Вашему карточному счету на Ваш мобильный телефон незамедлительно поступит sms-сообщение о сумме, времени и месте совершения операции.*

В случае выявления посторонних устройств, которые не отвечают конструкции данного терминального оборудования, откажитесь от выполнения операций и обязательно сообщите об этом факте в Информационно-справочный центр Банка по номеру телефона 0 800 50-77-60.

Внимание! На банкоматы установлены антискимминговые устройства. Банкомат должен выглядеть так:



Другие операции:

1. Не используйте карточку в торговой сети (в ресторане, магазине, на АЗС и тому подобное) для оплаты товаров или услуг, если продавец/кассир вызывал у вас недоверие.
2. Во время использования карточки для оплаты товаров или услуг продавец/кассир может требовать от держателя карточки предоставить паспорт, подписать квитанцию или ввести пин-код. Обращаем Ваше внимание, что требование относительно ведения пин-кода является обязательным только для карточек Maestro или Mastercard Unembossed.
3. Перед набором пин-кода убедитесь, что третьи лица, которые находятся в непосредственной близости от Вас, не имеют возможности его увидеть. Перед тем, как подписать квитанцию, в обязательном порядке проверьте сумму, которая отмечена на ней.
4. Не сообщайте информацию о карточке или карточном счете при расчетах в сети Интернет, например, данные о пин-коде, пароли доступа к счетам, кредитные лимиты, персональные данные и тому подобное.
5. При осуществлении расчетов за товары (услуги) в сети Интернет обязательно убедитесь в правильности указания url-адреса сайта/портала, к которому осуществляется подключение и через который осуществляется оплата товаров (услуг), поскольку похожие url-адреса могут использоваться для осуществления операций с использованием персональных данных карточки, несанкционированных держателями.

От простых правил к уверенным действиям!