«Нажить много денег — храбрость, сохранить их — мудрость, а умело расходовать — искусство»

Сэмюэл Батлер.

Банк России рекомендует всем держателям платежных карт соблюдать основные меры по обеспечению безопасности при получении платежной карты в банке, при ее хранении, использовании в банкомате, предприятиях торговли и услуг, в том числе для оплаты товаров и услуг в сети Интернет.

1. Получение карты в банке и ее хранение:

- при получении платежной карты и конверта с ПИН-кодом проверьте отсутствие следов вскрытия конверта, сохраните его в недоступном для посторонних лиц месте.
- не записывайте ПИН-код на платежной карте, его рекомендуется запомнить либо хранить отдельно от карты в недоступном для посторонних лиц месте.
- следует игнорировать электронные письма, в которых от имени кредитной организации поступают просьбы сообщить любые данные о карте.
- существует риск потерять все денежные средства с банковского счета в случае потери платежной карты, либо если карта была украдена, а также в случае кражи ПИН-кода и Ваших персональных данных.

2. Использование карты в банкомате:

- выбирайте банкоматы, установленные в безопасных местах, а также в местах, в которых банкоматы находятся под видеонаблюдением.
- не используйте устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат.
- убедитесь в наличии на банкомате эмблемы платежной системы, соответствующей карте, а также информации о банке, обслуживающем банкомат.
- осмотрите банкомат, если обнаружены «посторонние» устройства, не соответствующие его конструкции, или дополнительные устройства на картоприемнике или клавиатуре для набора ПИН- кода, необходимо использовать другой банкомат.
- при вводе ПИН-кода прикрывайте клавиатуру рукой.
- если банкомат «зависает» либо самовольно перезагружается, следует забрать карту и воспользоваться другим банкоматом.
- получив денежные средства, не забудьте забрать карту.
- не доверяйте советам третьих лиц при совершении операций в банкомате, за исключением работников кредитной организации.
- если банкомат не вернул карту, позвоните в банк, чтобы сообщить о случившемся и следовать указаниям работника кредитной организации.
- если деньги не были выданы банкоматом, но были списаны с банковского счета, следует обратиться в кредитную организацию и написать заявление о несогласии с операцией.

3. Использование карт в магазинах:

- не следует использовать платежную карту в предприятиях торговли и услуг, не вызывающих доверия.
- требуйте проведения операций с платежной картой только в Вашем присутствии, это снизит риск неправомерного получения персональных данных, указанных на платежной карте.
- перед тем, как ввести ПИН-код убедитесь в том, что находящиеся в непосредственной близости люди, не смогут его увидеть, либо прикрывайте ввод ПИН-кода рукой.
- если оплата по карте не прошла, сохраните чек, выданный терминалом, чтобы в дальнейшем проверить отсутствие этой операции в выписке по счету.

4. Использование карты в Интернете:

- заказывая товары и услуги по телефону или при работе в сети Интернет, не следует сообщать и вводить ПИН-код.
- установите суточный лимит на сумму операций по карте.
- используйте отдельную карту, предназначенную для оплаты товаров и услуг через сеть Интернет.
- рекомендуется делать покупки со своего компьютера, если покупки осуществлялись на чужом компьютере, не сохраняйте на нем персональные данные.
- установите на компьютер антивирусное программное обеспечение, регулярно его обновляйте.

5. Перевод денежных средств:

При осуществлении переводов денежных средств с использованием Мобильного банка, злоумышленники зачастую действуют в целях хищения логинов и паролей, иной информации, позволяющей получить доступ в Мобильный банк.

6. Платежи через мобильный банк с помощью компьютера:

- **о**граничьте доступ посторонних лиц к компьютеру (ноутбуку, планшету), используемому для работы в Мобильном банке, например, установив пароль.
- если есть подозрения, что логин или пароль для входа в Мобильный банк узнали посторонние лица, а также при осуществлении попытки несанкционированного доступа к системе Мобильный банк под Вашей учетной записью, обязательно сообщите в банк.
- не храните пароль на вход в Мобильный банк на компьютере или около него.
- внедрение на компьютер вредоносного кода позволяет злоумышленнику собирать информацию о действиях в системе Мобильный банк и управлять удаленно компьютером. Необходимо устанавливать на компьютер антивирус.
- не рекомендуется использовать открытые сети для доступа к системе Мобильный банк, например точки доступа wi-fi.
- необходимо исключить посещение сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения.

7. Платежи через мобильный банк при помощи телефона:

- устанавливайте только официальные мобильные приложения.
- используйте специализированное приложение кредитной организации.
- вовремя обновляйте операционную систему и мобильные приложения на телефоне.
- используйте антивирусное приложение, вовремя обновляйте его.
- не переходите по ссылкам и не устанавливайте приложения и обновления программ, направленные по смс или электронной почте, в том числе от имени кредитной организации.
- не храните в телефоне пароли и иную информацию, необходимую для доступа к мобильному банку.
- установите пароль на телефон.
- не передавайте мобильный телефон и SIM-карту третьим лицам.
- если сменили номер или потеряли телефон, в обязательном порядке обратитесь в банк для отключения услуги мобильный банк.

Важная информация!

Безопасность платежных услуг требует комплексного подхода, сочетающего технические методы защиты с бдительностью пользователей.

Основной вывод: защита средств — это ответственность, как банков, так и клиентов, где ключевым является соблюдение правил цифровой гигиены, распознавание фишинга и использование официальных приложений.

Наш адрес:

662501, Красноярский край
г. Сосновоборск,
ул. Весенняя, 9,

тел. 8 (39131) 3-30-06

Наш сайт:
http://kcson-16.ru

График работы:

Понедельник – пятница

с **09:00 до 18:00**
Обеденный перерыв с **13:00 до 14:00**
Выходные дни: суббота, воскресение

Министерство социальной политики Красноярского края

краевое государственное бюджетное учреждение социального обслуживания «Комплексный центр социального обслуживания населения «Сосновоборский»

Безопасность платежных услуг

г. Сосновоборск, 2026