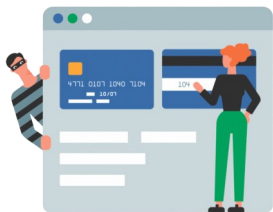


БАНКОВСКИЕ КАРТЫ: ПРАВИЛА БЕЗОПАСНОСТИ



ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОГО ОБРАЩЕНИЯ С БАНКОВСКИМИ КАРТАМИ

- 1 **Никогда и никому не сообщайте свой ПИН-код, CVC, срок действия или одноразовые СМС-коды — даже если звонит «сотрудник банка».**
- 2 **Не фотографируйте карту и не храните её данные в заметках телефона.**
- 3 **При вводе ПИН-кода в банкоматах и терминалах прикрывайте клавиатуру рукой.**
- 4 **Регулярно проверяйте выписки по карте и обращайте внимание на любые несанкционированные транзакции.**
- 5 **Установите доступный лимит списаний по карте в день .**
- 6 **Не переходите по ссылкам из подозрительных электронных писем или сообщений.**



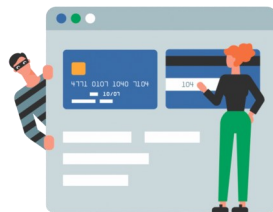
г. Нерюнгри 2026г .

БАНКОВСКИЕ КАРТЫ: ПРАВИЛА БЕЗОПАСНОСТИ



ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОГО ОБРАЩЕНИЯ С БАНКОВСКИМИ КАРТАМИ

- 1 **Никогда и никому не сообщайте свой ПИН-код, CVC, срок действия или одноразовые СМС-коды — даже если звонит «сотрудник банка».**
- 2 **Не фотографируйте карту и не храните её данные в заметках телефона.**
- 3 **При вводе ПИН-кода в банкоматах и терминалах прикрывайте клавиатуру рукой.**
- 4 **Регулярно проверяйте выписки по карте и обращайте внимание на любые несанкционированные транзакции.**
- 5 **Установите доступный лимит списаний по карте в день .**
- 6 **Не переходите по ссылкам из подозрительных электронных писем или сообщений.**



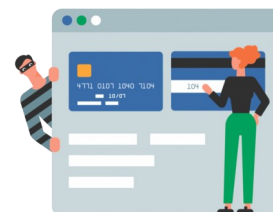
г. Нерюнгри 2026г .

БАНКОВСКИЕ КАРТЫ: ПРАВИЛА БЕЗОПАСНОСТИ



ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОГО ОБРАЩЕНИЯ С БАНКОВСКИМИ КАРТАМИ

- 1 **Никогда и никому не сообщайте свой ПИН-код, CVC, срок действия или одноразовые СМС-коды — даже если звонит «сотрудник банка».**
- 2 **Не фотографируйте карту и не храните её данные в заметках телефона.**
- 3 **При вводе ПИН-кода в банкоматах и терминалах прикрывайте клавиатуру рукой.**
- 4 **Регулярно проверяйте выписки по карте и обращайте внимание на любые несанкционированные транзакции.**
- 5 **Установите доступный лимит списаний по карте в день .**
- 6 **Не переходите по ссылкам из подозрительных электронных писем или сообщений.**



г. Нерюнгри 2026 г.

7 Платите только на защищённых сайтах — проверяйте, чтобы адрес начинался с <https://>, а рядом была иконка замка.

8 Оформите специальную карту для безопасных интернет-платежей — открыть виртуальную банковскую карту и электронный кошелёк и пополнять их перед покупкой.

9 Пользуйтесь сервисами безопасных платежей (Apple Pay, Google Pay, Samsung Pay) — они проводят оплату с помощью одноразового токена, поэтому реквизиты карты в интернет-магазин не попадают.

10 Сохраняйте чеки и переписку — чеки, электронные письма, скриншоты общения в мессенджере помогут банкам и правоохранительным органам разобраться в инциденте.

Что делать, если данные карты стали известны посторонним?

1 Заблокируйте карту через мобильное приложение, интернет-банк или по горячей линии.

2 Проверьте последние операции. При выявлении несанкционированных списаний — сразу сообщите в банк и подайте заявление.

3 Обратитесь в полицию. Особенно если сумма ущерба значительна.

4 Перевыпустите карту. Лучше оформить новую, чем рисковать повторным доступом.

5 Смените пароли в интернет-банке, платёжных сервисах, почте и соцсетях.



7 Платите только на защищённых сайтах — проверяйте, чтобы адрес начинался с <https://>, а рядом была иконка замка.

8 Оформите специальную карту для безопасных интернет-платежей — открыть виртуальную банковскую карту и электронный кошелёк и пополнять их перед покупкой.

9 Пользуйтесь сервисами безопасных платежей (Apple Pay, Google Pay, Samsung Pay) — они проводят оплату с помощью одноразового токена, поэтому реквизиты карты в интернет-магазин не попадают.

10 Сохраняйте чеки и переписку — чеки, электронные письма, скриншоты общения в мессенджере помогут банкам и правоохранительным органам разобраться в инциденте.

Что делать, если данные карты стали известны посторонним?

1 Заблокируйте карту через мобильное приложение, интернет-банк или по горячей линии.

2 Проверьте последние операции. При выявлении несанкционированных списаний — сразу сообщите в банк и подайте заявление.

3 Обратитесь в полицию. Особенно если сумма ущерба значительна.

4 Перевыпустите карту. Лучше оформить новую, чем рисковать повторным доступом.

5 Смените пароли в интернет-банке, платёжных сервисах, почте и соцсетях.



7 Платите только на защищённых сайтах — проверяйте, чтобы адрес начинался с <https://>, а рядом была иконка замка.

8 Оформите специальную карту для безопасных интернет-платежей — открыть виртуальную банковскую карту и электронный кошелёк и пополнять их перед покупкой.

9 Пользуйтесь сервисами безопасных платежей (Apple Pay, Google Pay, Samsung Pay) — они проводят оплату с помощью одноразового токена, поэтому реквизиты карты в интернет-магазин не попадают.

10 Сохраняйте чеки и переписку — чеки, электронные письма, скриншоты общения в мессенджере помогут банкам и правоохранительным органам разобраться в инциденте.

Что делать, если данные карты стали известны посторонним?

1 Заблокируйте карту через мобильное приложение, интернет-банк или по горячей линии.

2 Проверьте последние операции. При выявлении несанкционированных списаний — сразу сообщите в банк и подайте заявление.

3 Обратитесь в полицию. Особенно если сумма ущерба значительна.

4 Перевыпустите карту. Лучше оформить новую, чем рисковать повторным доступом.

5 Смените пароли в интернет-банке, платёжных сервисах, почте и соцсетях.

