Банк России

БАНКОВСКИЕ ПЛАТЕЖНЫЕ КАРТЫ И ПРАВИЛА ИХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ

2021 г.

Банковская карта – КЛЮЧ К СЧЕТУ

Денежные средства находятся в банке

Почему банковская карта лучше наличных

✓ Контроль расходов,
возможность экономить и получать доход

✓ Эпидемиологически более безопасна

✓ Позволяет быстро решать временные финансовые проблемы

✓ Удобнее наличных денег

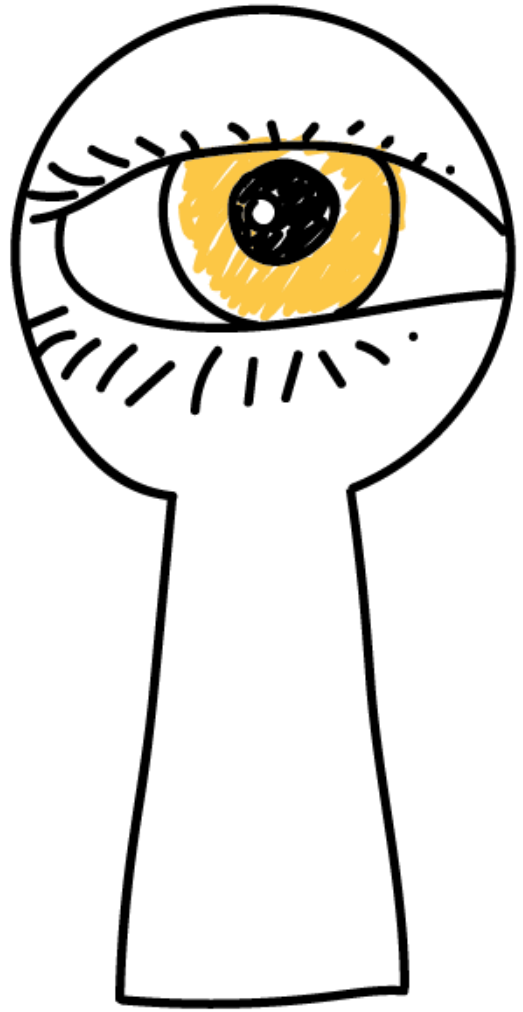
✓ Безопаснее наличных денег

✓ Позволяет пользоваться дистанционными банковским сервисами для получения финансовых услуг

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Мошенникам нужны:

КАК И ГДЕ МОГУТ УКРАСТЬ ВАШИ ДАННЫЕ?



В банкомате — на нем мошенники могут установить скиммер и видеокамеру

КАК НЕ ПОПАСТЬСЯ

- Используйте банкоматы, которые расположены во внушающих доверие местах
- Отказывайтесь от помощи «доброжелателей»
- Сохраняйте квитанции о совершенной операции

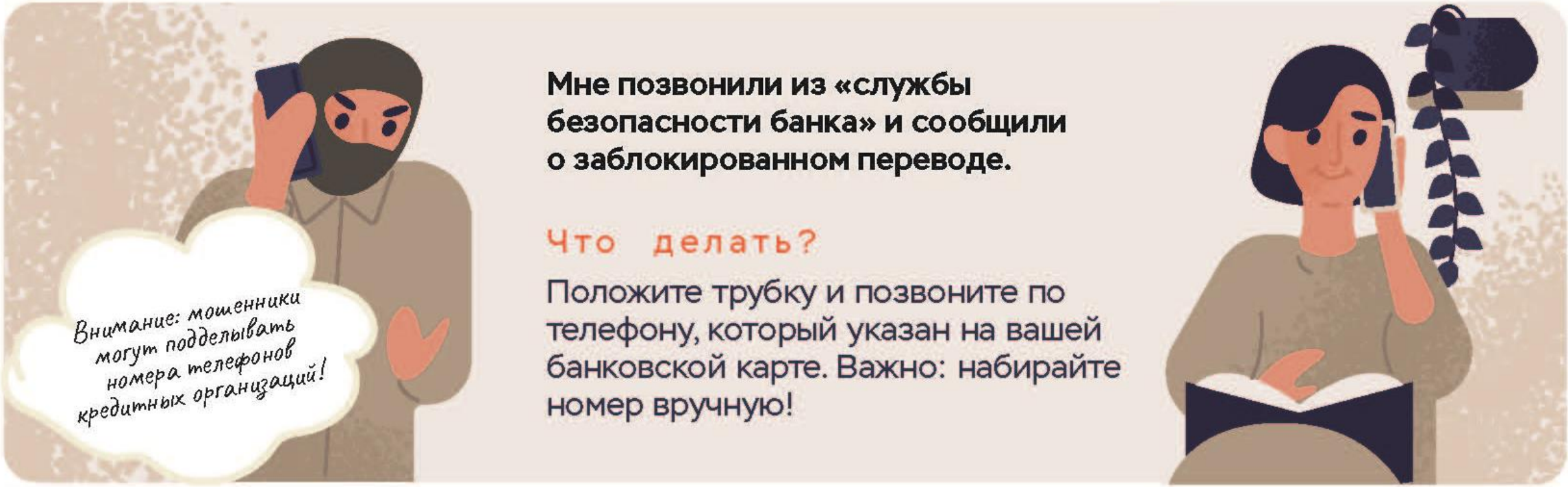
МЕСТО ДЕЙСТВИЯ: МАГАЗИН или КАФЕ

В кафе или магазине — сотрудник-злоумышленник может сфотографировать вашу карту

ОПЛАЧИВАЕМ ПОКУПКИ БЕЗ РИСКА – СОБЛЮДАЕМ ПРАВИЛА:

- НЕ упускать из виду карту
- Перед вводом ПИН-кода (оплатой бесконтактной картой) убедитесь в правильности набранной суммы
- Вводить ПИН-код так, чтобы он не был виден посторонним

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО:



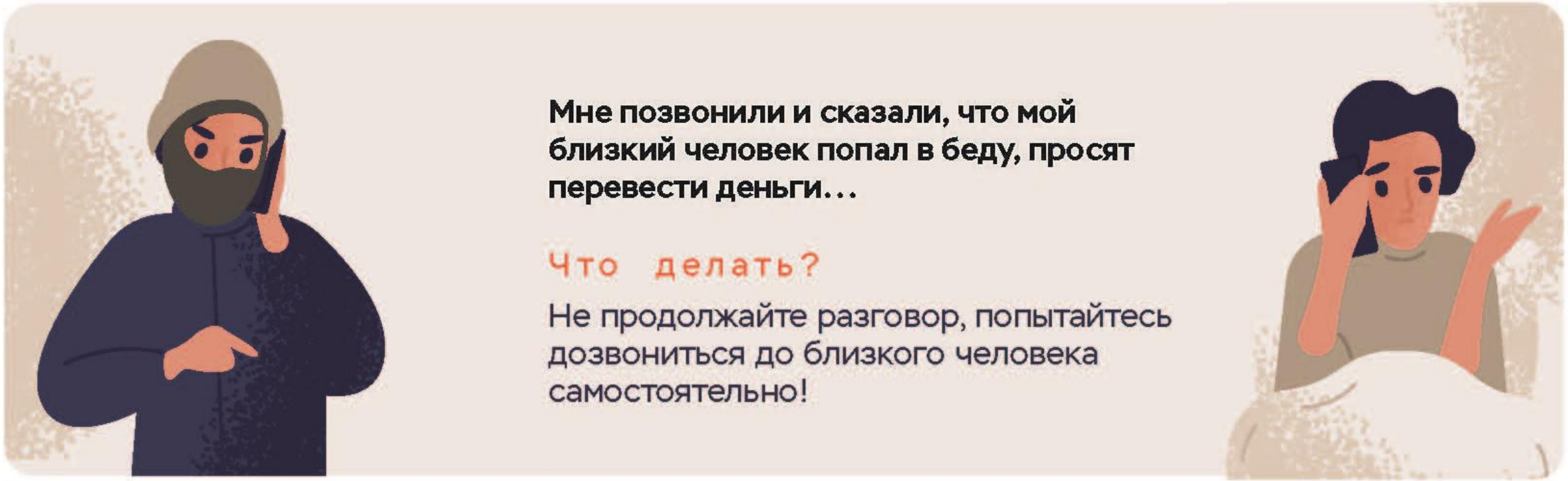
ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО:

Мне позвонили и сказали, что я выиграл (-а) в лотерею или розыгрыше призов / могу получить бесплатную путевку, льготы или выплаты...

Что делать?

Скорее всего, вы разговариваете с мошенниками! Возможно, вас попросят совершить платеж под каким-то предлогом, сообщить персональные данные или данные банковской карты. Не продолжайте разговор, не сообщайте преступникам личную информацию!

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО:



СМС, мессенджеры, соцсети

Мне пришла СМС от «банка» с информацией:

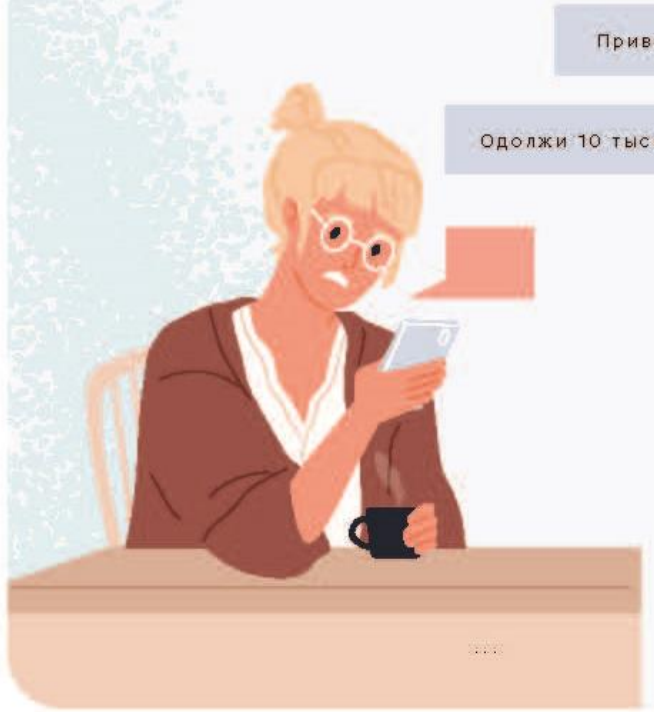
- **о заблокированном платеже;**
- **о выигрыше в лотерею;**
- **об ошибочном переводе на мой банковский счет**

или счет мобильного телефона с просьбой вернуть деньги.

Что делать?

- Не перезванивайте по номеру, указанному в сообщении. Обратитесь в ваш банк по номеру, который указан на оборотной стороне карты. Наберите его вручную!
- Не делайте того, о чем вас просят в сообщении.
- Не переходите по ссылке в сообщении.

СМС, мессенджеры, соцсети



Мой знакомый написал мне в соцсети: просит дать в долг или перевести средства на лечение

Аккаунт вашего знакомого могли взломать. Часто мошенники используют информацию о сборе средств, заменяя платежные реквизиты на свои.

Что делать?

Перезвоните этому человеку, чтобы выяснить ситуацию.

Тщательно проверяйте информацию, указанную в этой «просьбе о помощи», не совершайте импульсивных действий. Например, задайте вопрос, ответ на который не может знать мошенник.

Место действия: Интернет

Используйте только проверенные Интернет-ресурсы при оплате товаров и услуг

Защищенная страница - 

Не указывайте реквизиты Вашей карты на подозрительных сайтах и не сообщайте:

- номер карты
- имя держателя карты
- срок действия карты

Для подтверждения операции держателю карты приходит смс-сообщение с уникальным кодом, который нужно ввести на сайте для завершения покупки.

Этот код нельзя никому сообщать!

Социальная инженерия

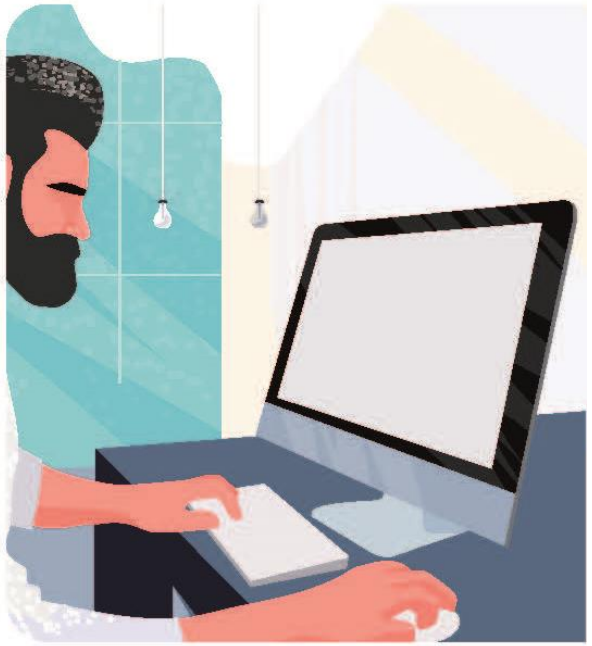
Цель – доступ к защищенной информации (пароли, данные о карте)

ФИШИНГ

Как распознать:

- Незнакомый отправитель, информация, не имеющая к вам отношения
- Файлы с расширениями .exe, .vbs, .rtf, .bat, .com, .msi, .reg, .scf, .lnk (возможна маскировка под безопасный формат)
- Психологические манипуляции – «срочность», «важность»

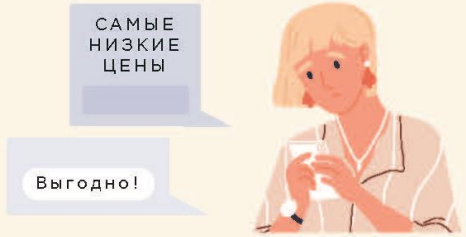
ИНТЕРНЕТ



На сайтах с объявлениями (Avito, Youla и т.п.) предлагают товары и услуги по заниженным ценам...

Что делать?

За привлекательными ценами часто прячутся мошенники. Не соглашайтесь на предоплату, пользуйтесь услугой «безопасная сделка», которая доступна на сайте с объявлениями. Не сообщайте секретные данные банковской карты. Не переходите по ссылкам под предлогом «ссылки для оплаты товара» или «ссылки на транспортную компанию».



Нужно перевести деньги или купить билеты. На одном из сайтов условия выгоднее, чем на знакомых ресурсах...

Что делать?

Пользуйтесь только проверенными ресурсами. Мошенники часто завлекают потенциальные жертвы отсутствием комиссий и привлекательными условиями.

ИНТЕРНЕТ

Предлагают поучаствовать в онлайн-опросе за деньги или какой-то товар...

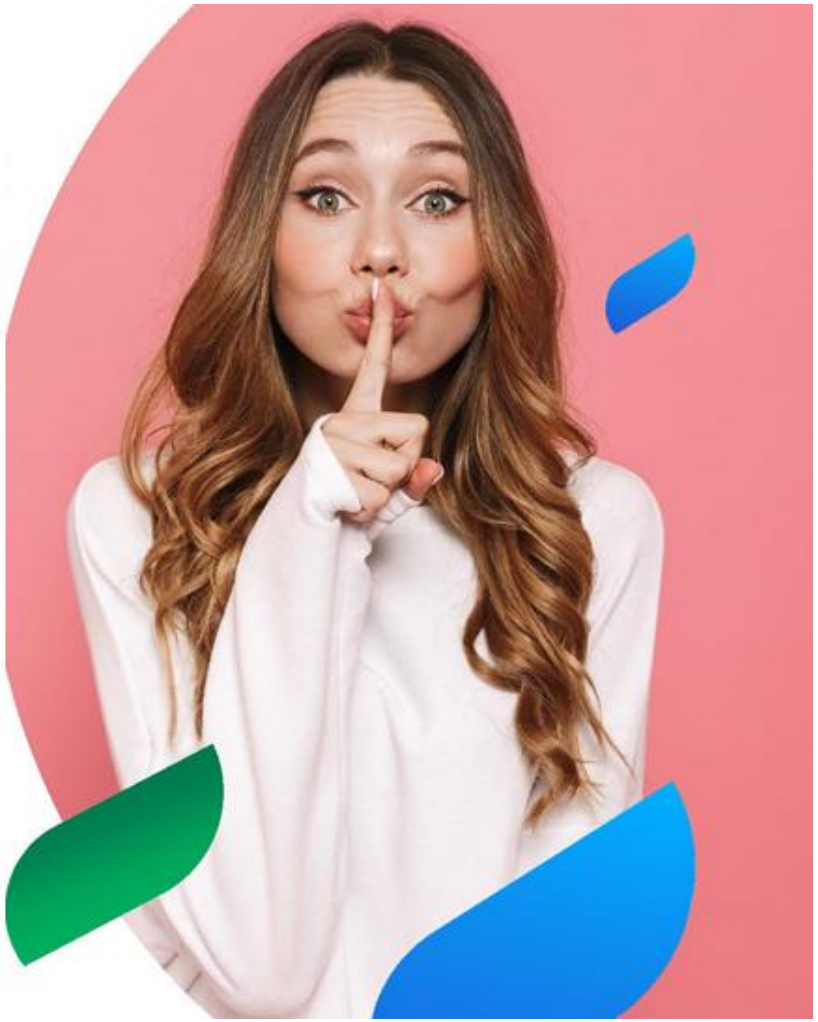
Что делать?

Цель таких предложений - данные вашей банковской карты и средства на ней. Злоумышленники просят оплатить комиссию за перевод суммы вознаграждения, например, «перевести 250 руб., чтобы получить 100 000 руб.». Это обман, будьте бдительны и не принимайте участие в подобных опросах!

Общие правила использования карт

Держите ПИН-код в тайне

Его не должен знать никто, кроме Вас, даже банковские сотрудники!



Что нельзя делать с ПИН-кодом:

- Записывать на карте
- Хранить в кошельке или сумке
- Хранить вместе с картой
- Сообщать третьим лицам
- Указывать в интернете

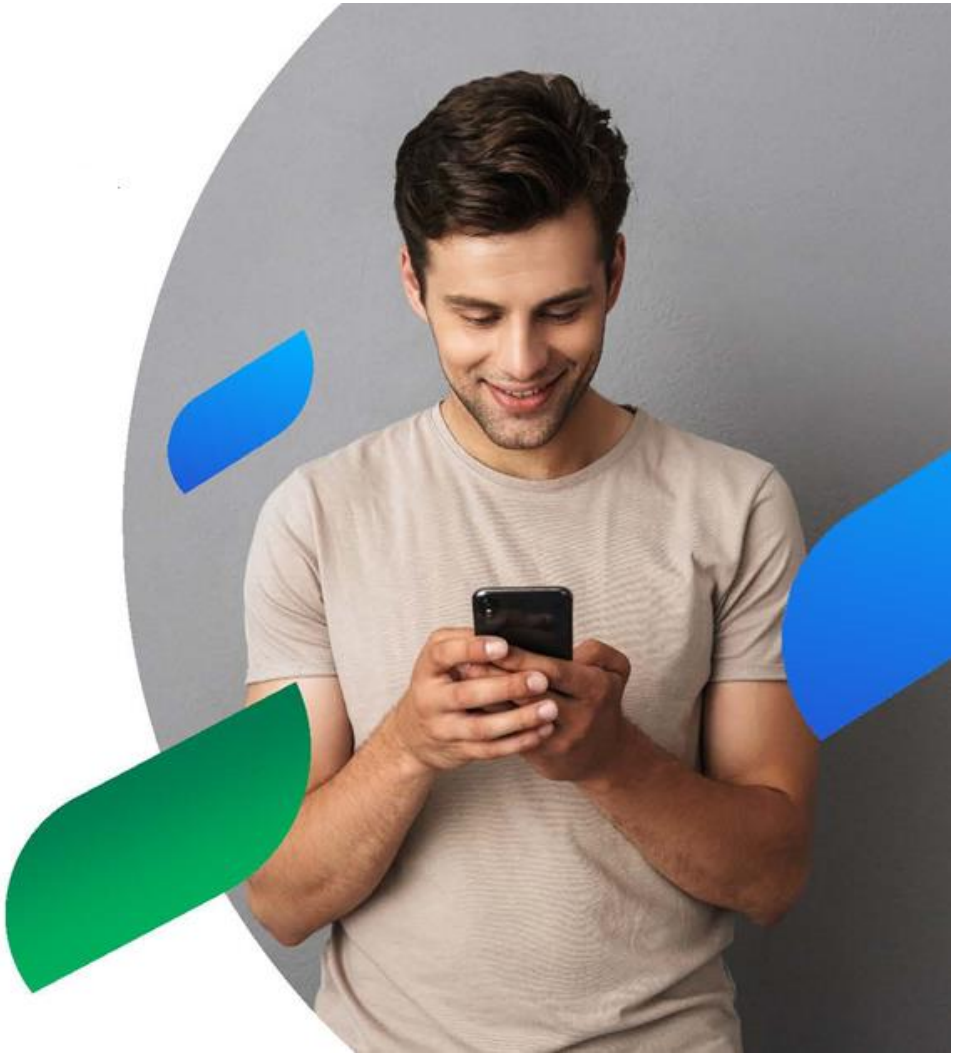
Берегите от чужих глаз CVC/CVV/ППК код -
расположен на оборотной стороне платежной карты

Не передавайте Вашу карту в руки посторонним людям!

Общие правила использования карт

Используйте сервис смс-информирования при совершении операций по карте

Надежный способ контролировать расходы, совершаемые по банковской карте



ВАЖНО!

- ✓ Помните, что Банк России присылает СМС и e-mail только в ответ на ваше обращение через Интернет-приемную
- ✓ Не храните крупные суммы денег на карте, которую вы носите с собой и используете для повседневных трат
- ✓ Если с вашей банковской карты списали деньги без вашего ведома, НЕМЕДЛЕНО свяжитесь с банком и заблокируйте карту, но не позднее следующего дня
- ✓ Банк рассмотрит заявление в течение 30 дней. Если операция была международной – в течение 60 дней
- ✓ Обратитесь в правоохранительные органы с заявлением о хищении

Банк России

СПАСИБО
ЗА ВНИМАНИЕ

Почтовый адрес: 443099, Самара, ул. Куйбышева, д. 112
Тел.: (846) 332-03-25
Факс: (846) 332-08-62
Сайт: www.cbr.ru