

ПРОСТЫЕ ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ БАНКОВСКИХ ПРОДУКТОВ И УСЛУГ

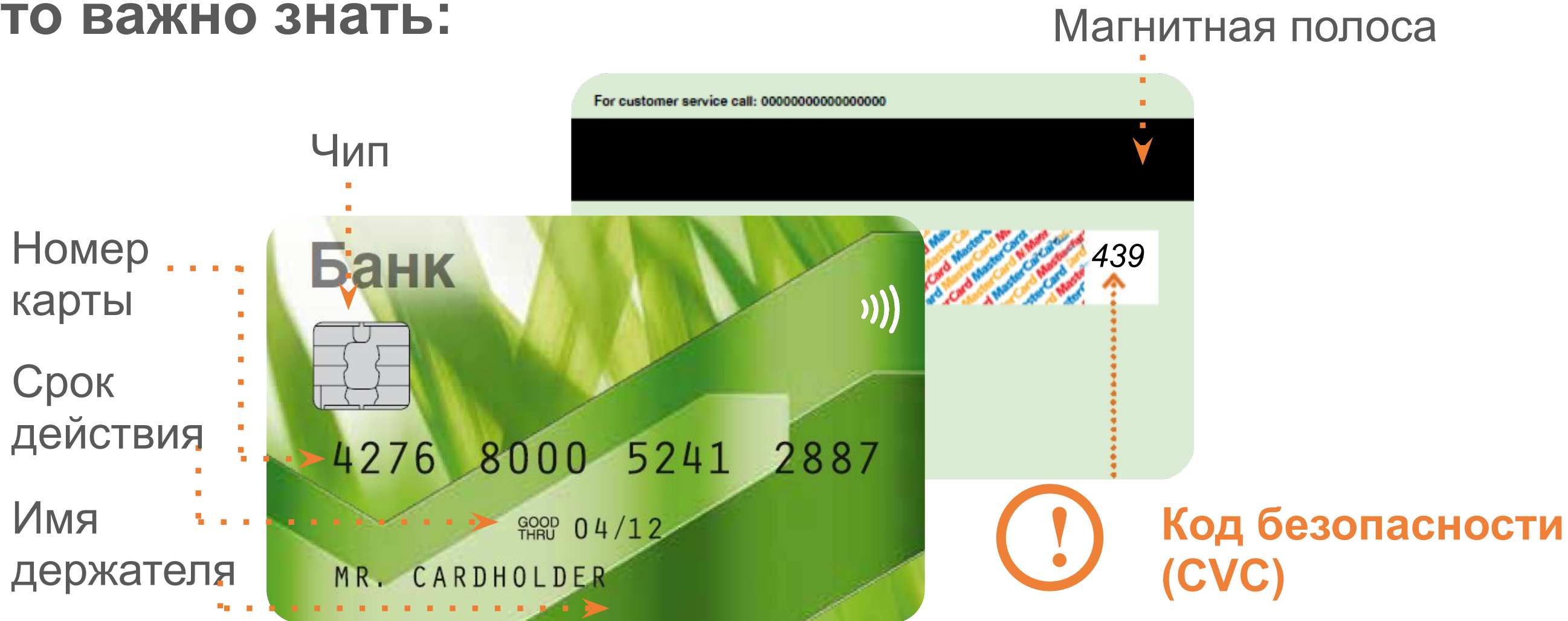


РАЗДЕЛ 1

БАНКОВСКИЕ ПРОДУКТЫ И УСЛУГИ

БАНКОВСКАЯ КАРТА

Что важно знать:

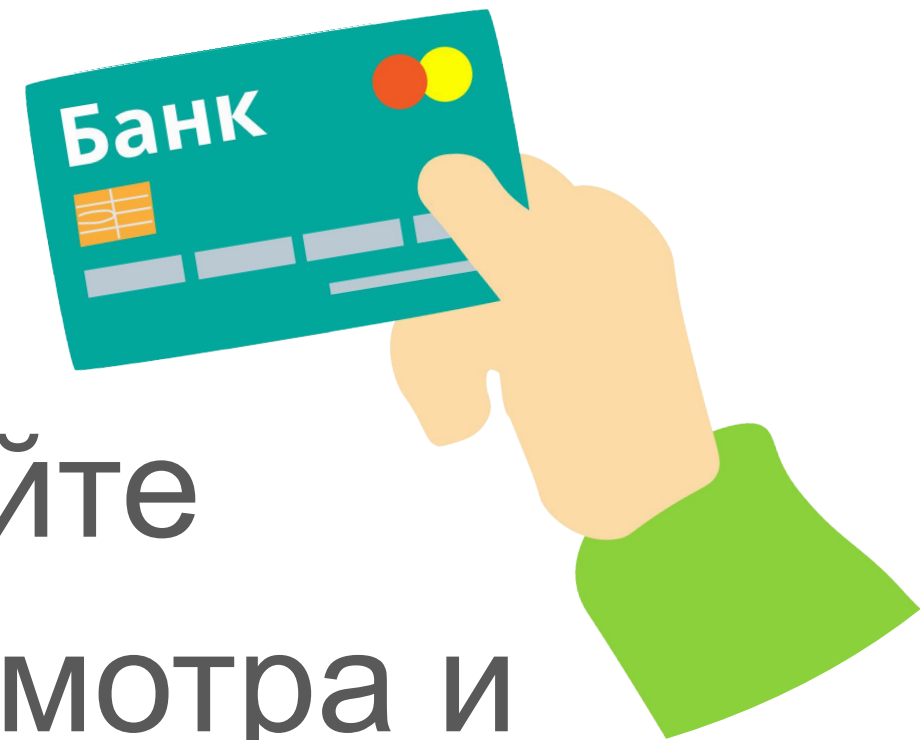


ПИН-код - пароль для работы с банкоматом, выдается банком в запечатанном конверте

1

РЕКОМЕНДАЦИИ
ПО
БЕЗОПАСНОСТИ

Карта - доступ ко всем
электронным деньгам



Не оставляйте
ее без присмотра и
не передавайте
никому

2

РЕКОМЕНДАЦИИ
ПО
БЕЗОПАСНОСТИ

Измените
ПИН-код
в банкомате
на известный
только вам и
запомните его



3

РЕКОМЕНДАЦИИ
ПО
БЕЗОПАСНОСТИ

Никому не говорите
ПИН-код и код
безопасности

Не храните
ПИН-код рядом
с картой



Пин-
код
1068

4

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Осмотрите банкомат
перед снятием денег,
нажмите кнопку «отмена»

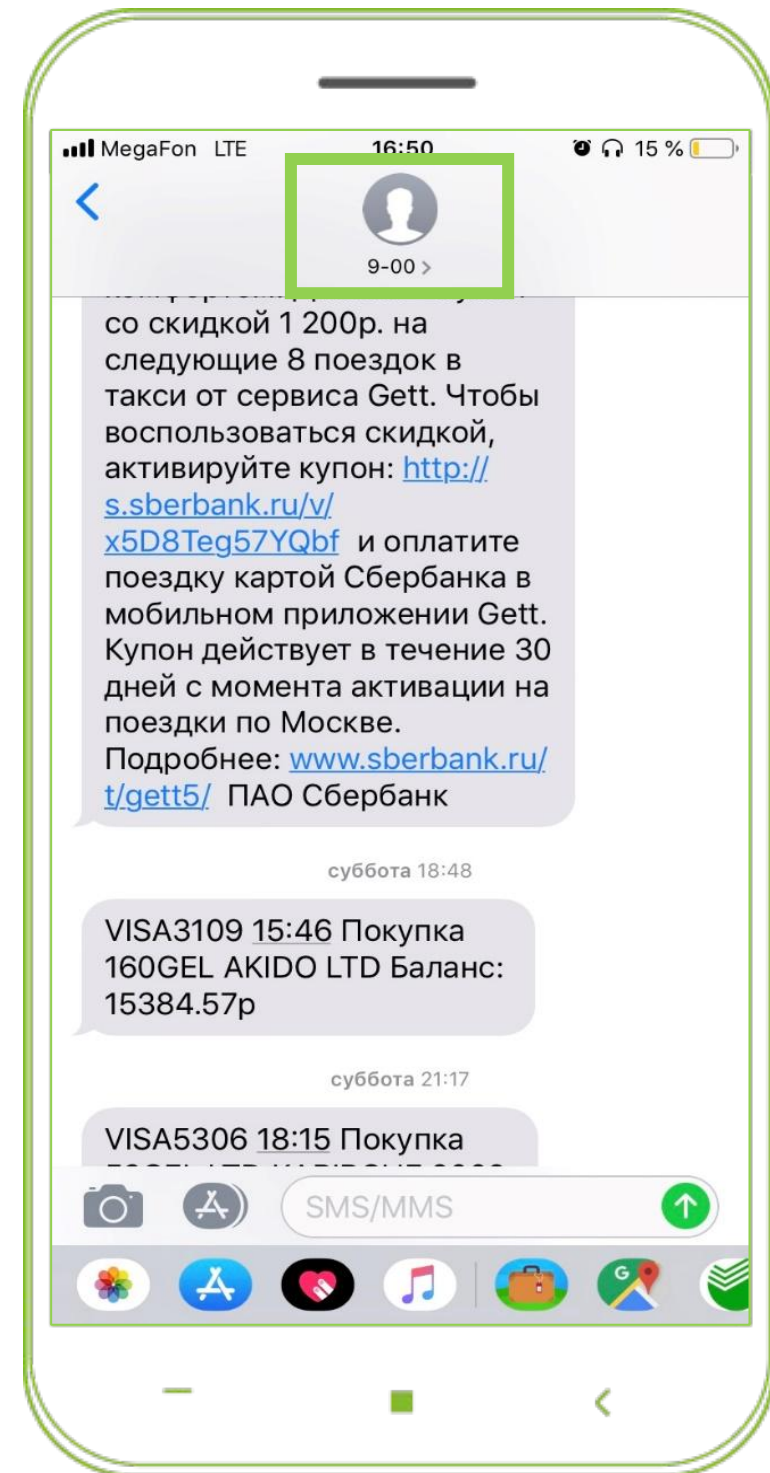


ЧТО ТАКОЕ МОБИЛЬНЫЙ БАНК

Услуга позволяет:
распоряжаться своими деньгами и
оперативно отслеживать по СМС
поступление и списание денег с карты

Для использования мобильного
банкинга нужно иметь только
ТЕЛЕФОН!

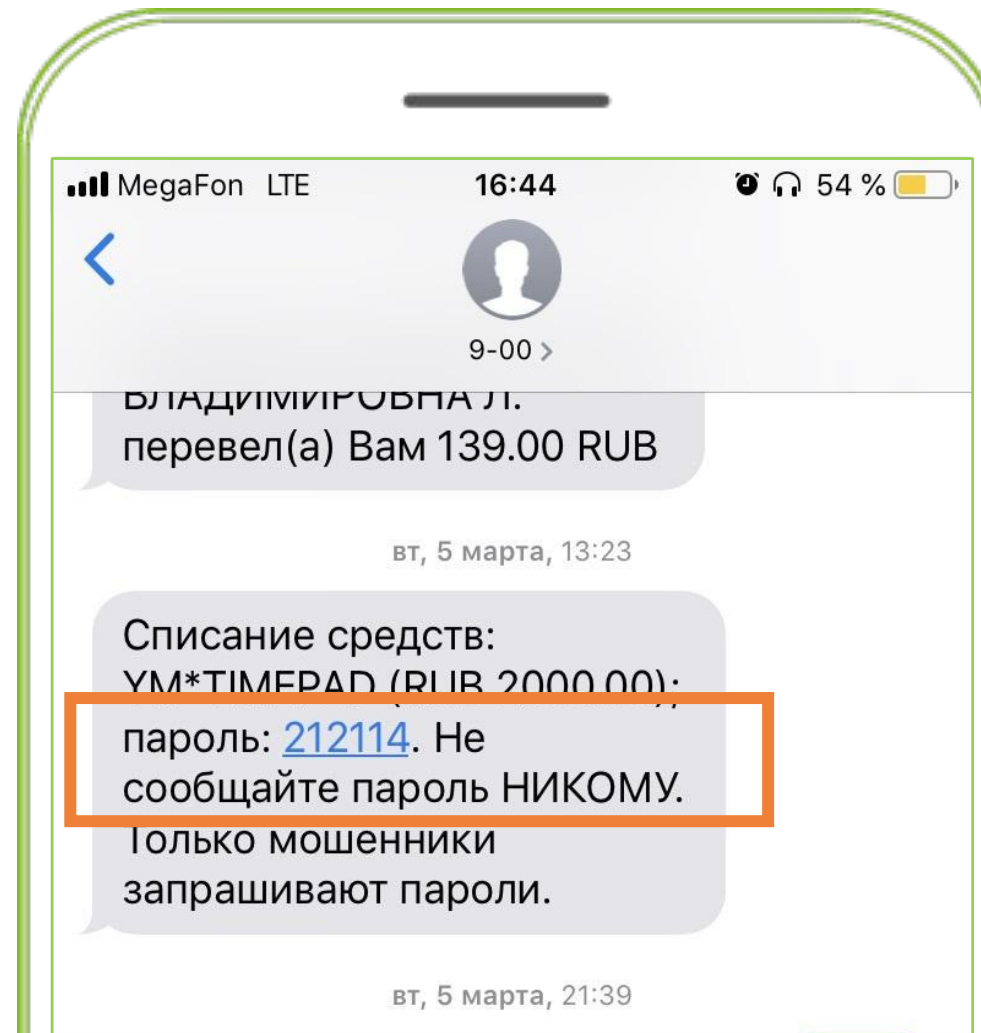
Сбербанк отправляет СМС
только с номеров 900 и 9000



1

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Не сообщайте никому коды из SMS



2

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Если потеряли телефон или сменили номер мобильного, обратитесь в банк и к оператору



3

РЕКОМЕНДАЦИИ
ПО
БЕЗОПАСНОСТИ

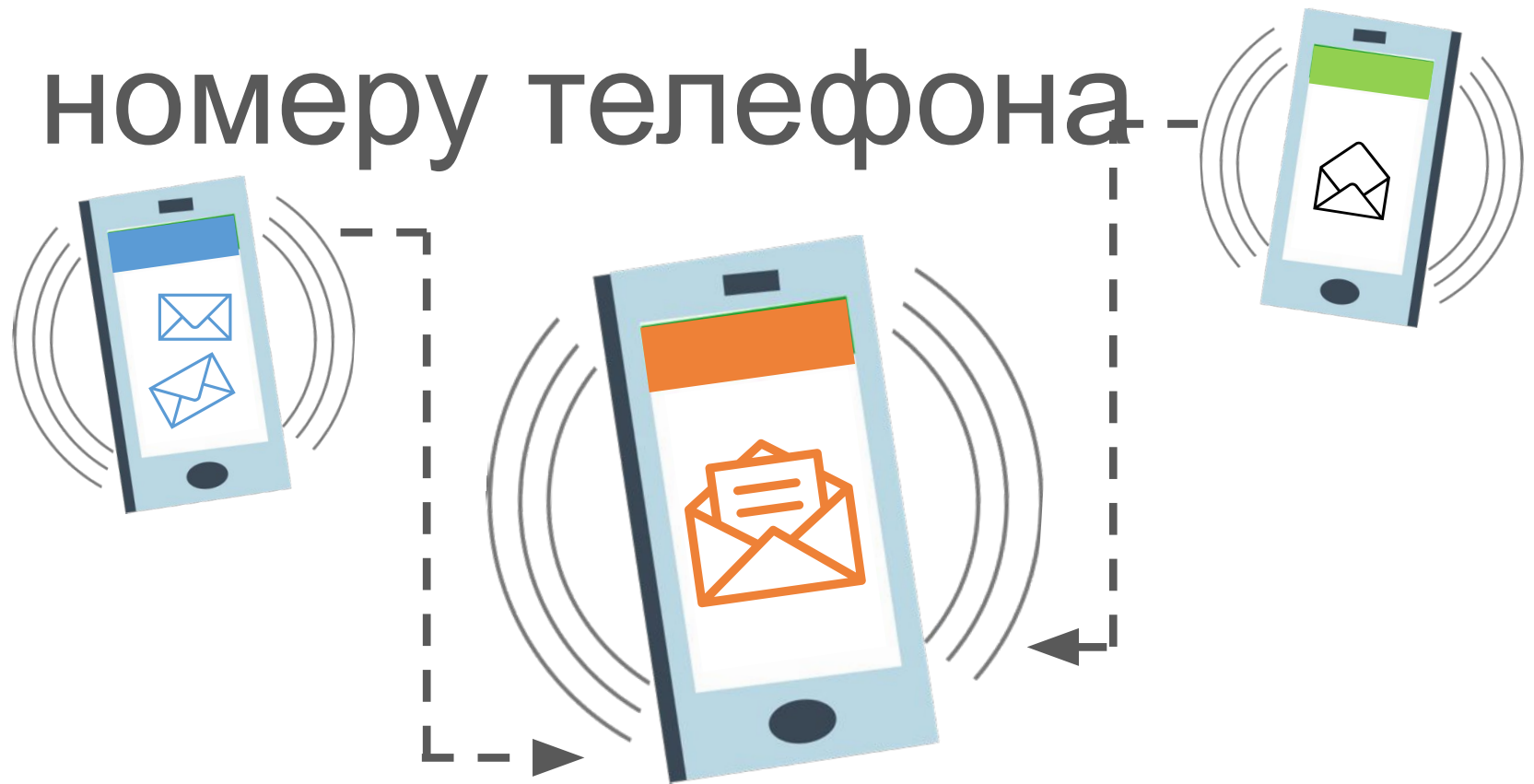
Не подключайте к мобильному банку чужие телефоны



4

РЕКОМЕНДАЦИИ
ПО
БЕЗОПАСНОСТИ

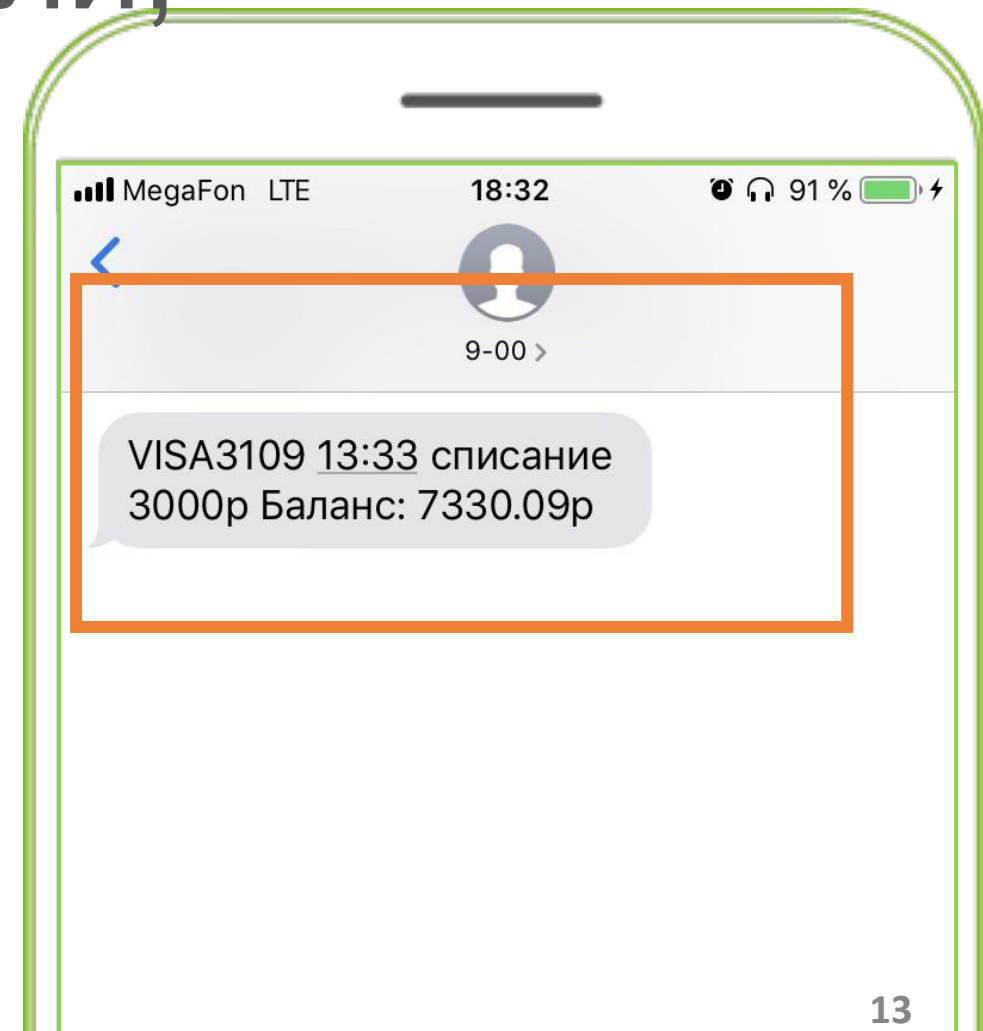
Подключайте
мобильный банк только
к оформленному на Вас
номеру телефона -



5

РЕКОМЕНДАЦИИ
ПО
БЕЗОПАСНОСТИ

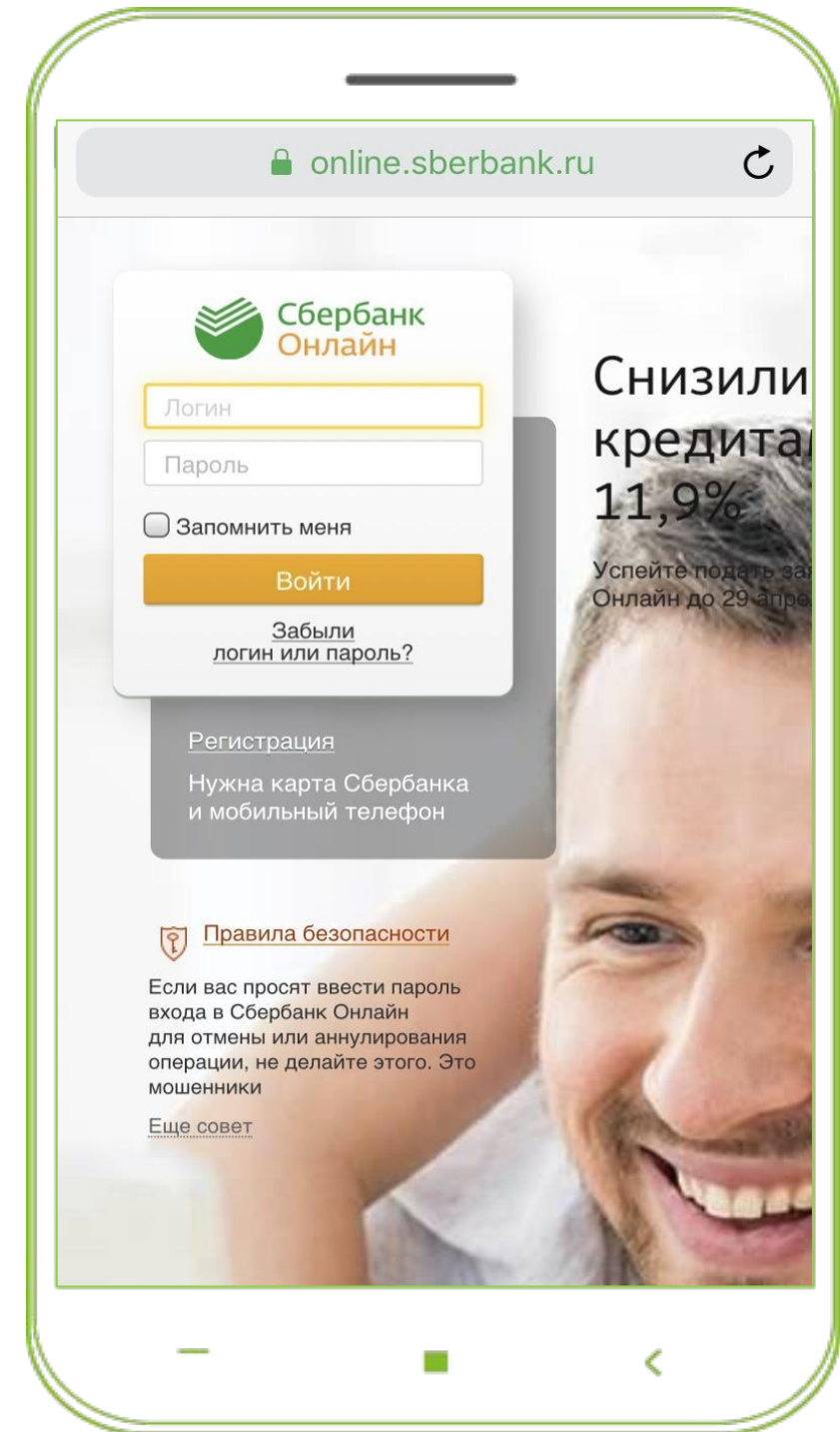
Если получили СМС
о переводе, который
не совершали,
обратитесь
в банк



ЧТО ТАКОЕ ИНТЕРНЕТ-БАНКИНГ

Услуга позволяет:
самостоятельно и в любое
время пользоваться услугами
банка через Интернет

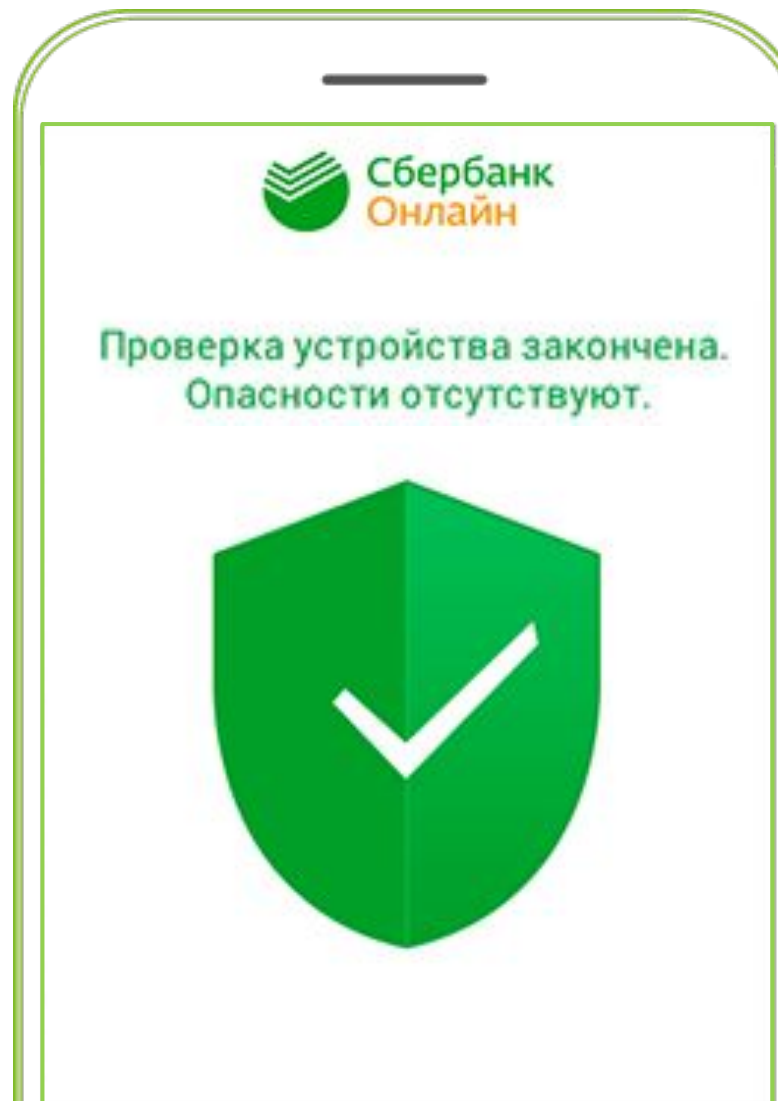
Решать вопросы
безопасности



1

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Скачивайте
мобильное приложение
в официальных магазинах

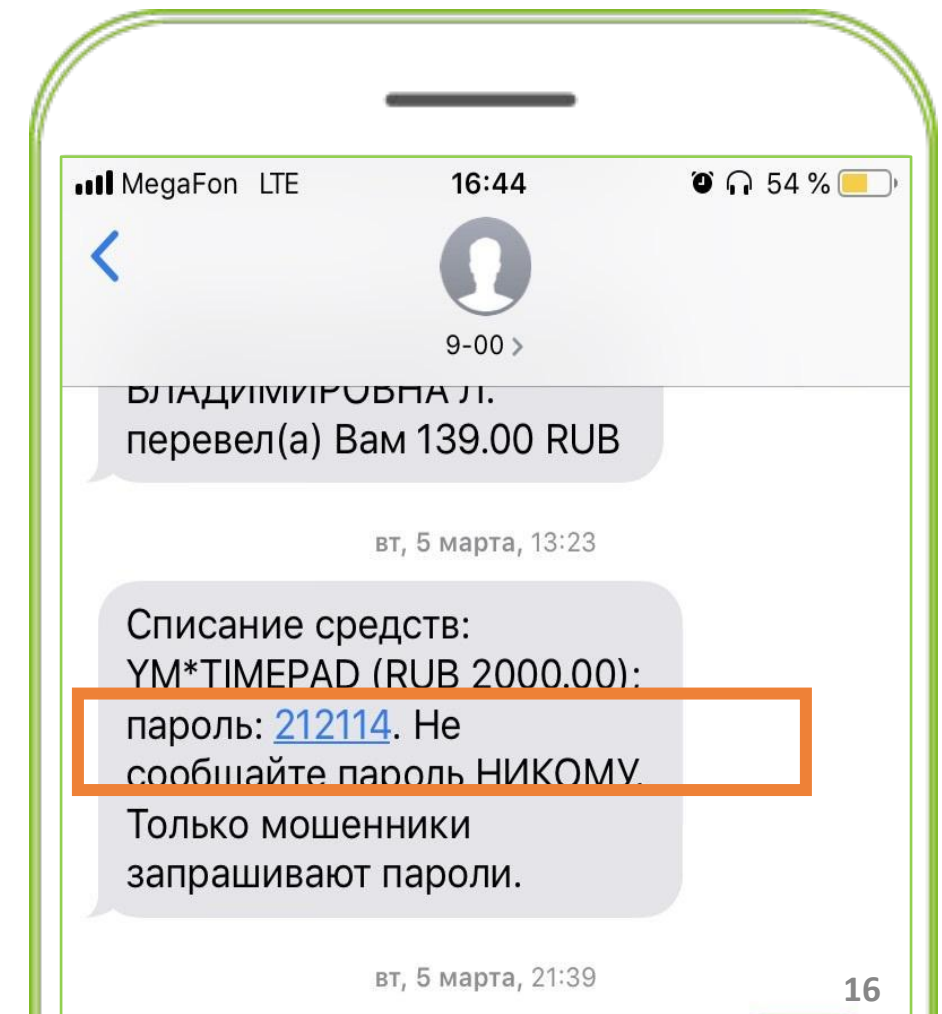
 Загрузите в
App Store Загрузите в
Google Play

2

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Не сообщайте никому:

- Логин и пароль от Сбербанк Онлайн
- Пароли из SMS

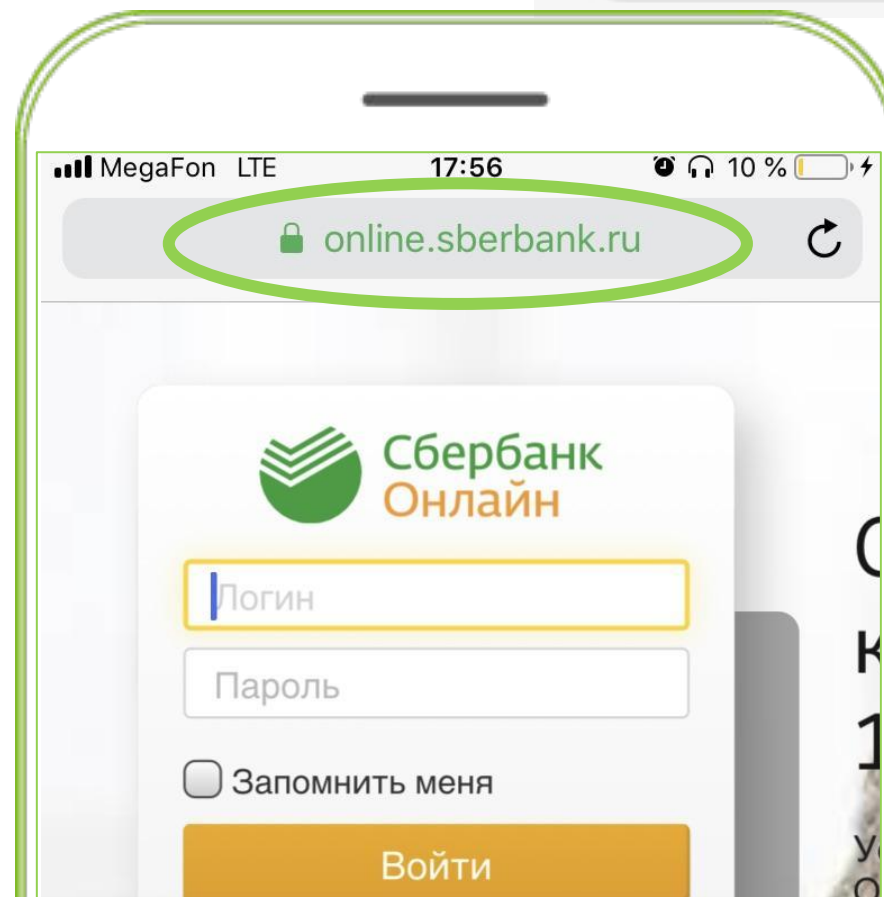


3

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

В веб-версии вводите данные только если **домен** точно совпадает с **названием сайта**

<https://online.sberbank.ru/CSAF> ✕



и сайт
начинается
с **httpS**:

4

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Разработчики постоянно исправляют уязвимости и добавляют функции, повышающие безопасность

Своевременно обновляйте программное обеспечение и антивирус



РАЗДЕЛ 2

КАК НЕ ПОПАСТЬСЯ НА УЛОВКИ МОШЕННИКОВ?

ЧТО НУЖНО ЗНАТЬ О МОШЕННИЧЕСТВЕ?



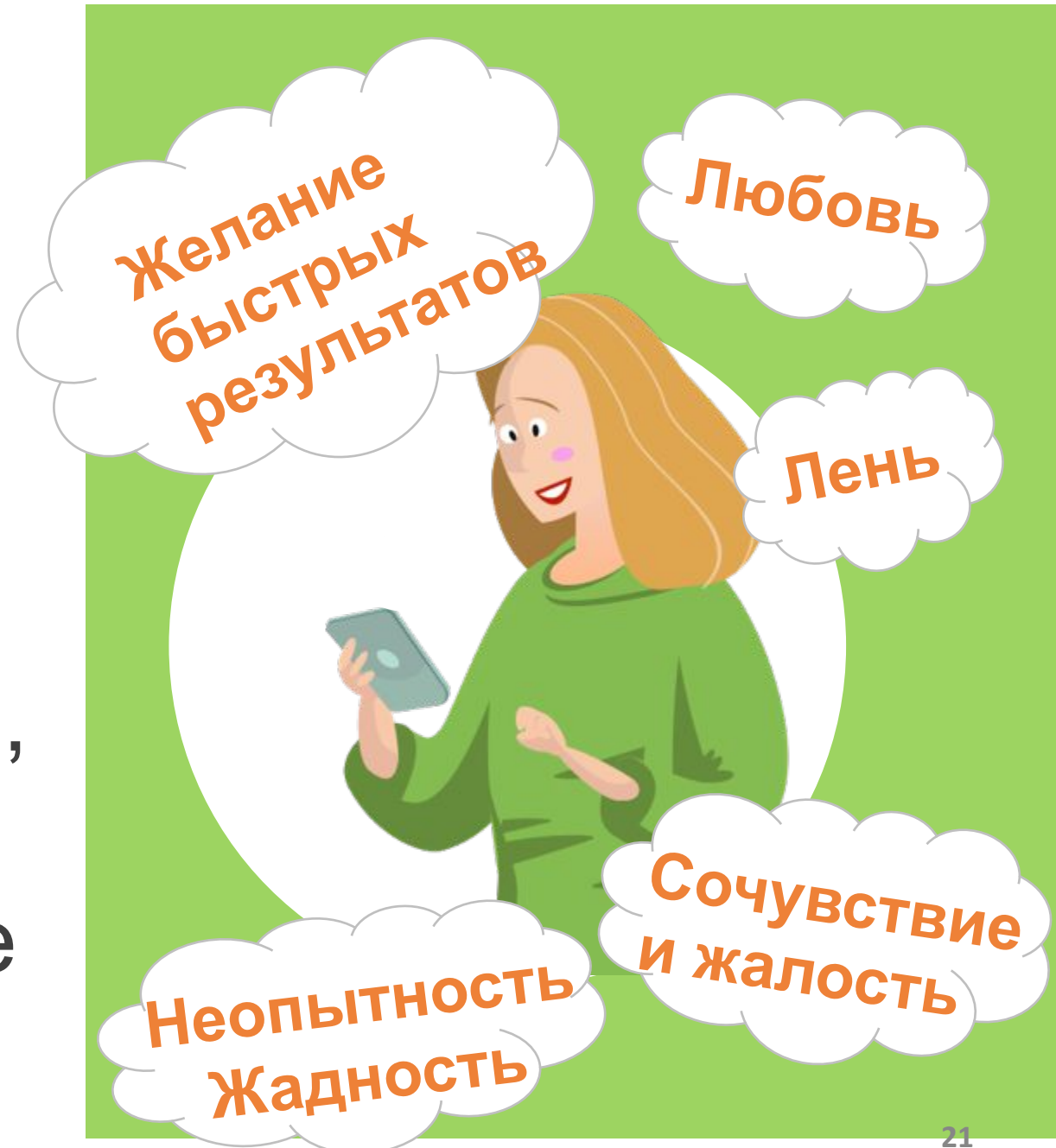
Социальная инженерия –
воздействие мошенников на людей,
при котором люди собственными
руками отдают свои деньги или
сообщают данные

Мошенничество по телефону –
вид социальной инженерии, при
котором злоумышленники звонят
Вам или просят им позвонить

МОШЕННИЧЕСТВО ПО ТЕЛЕФОНУ

Общий принцип всех атак – введение в заблуждение и требование срочного решения

Злоумышленники могут применять различные техники, направленные на эмоции, слабости или иные особенности личности



КАК ПОНЯТЬ, ЧТО ЗВОНИТ МОШЕННИК?



- 1 Незнакомый или скрытый номер телефона
- 2 Внезапность и требование быстрого принятия решения
- 3 Чрезмерная настойчивость или заискивание/уговаривание
- 4 Невнятность и нечеткость ответов на Ваши вопросы
- 5 Интерес к Вашим данным под предлогом помощи (данные карты, пароль из СМС)

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ

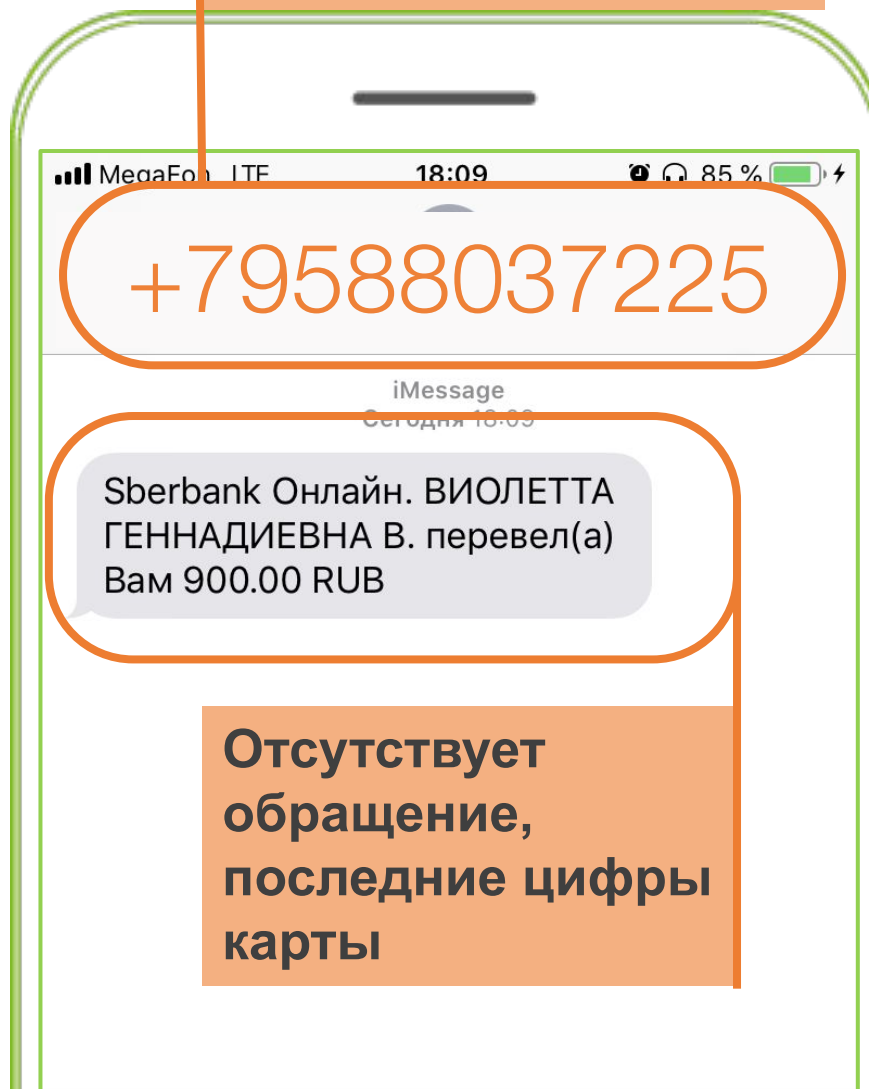
Чтобы отличить сотрудника банка, запишите номера банка в телефонную книгу, например, номер Сбербанка: **900, 8800555-55-50**

Если звонок будет с другого номера, он отобразится как неизвестный



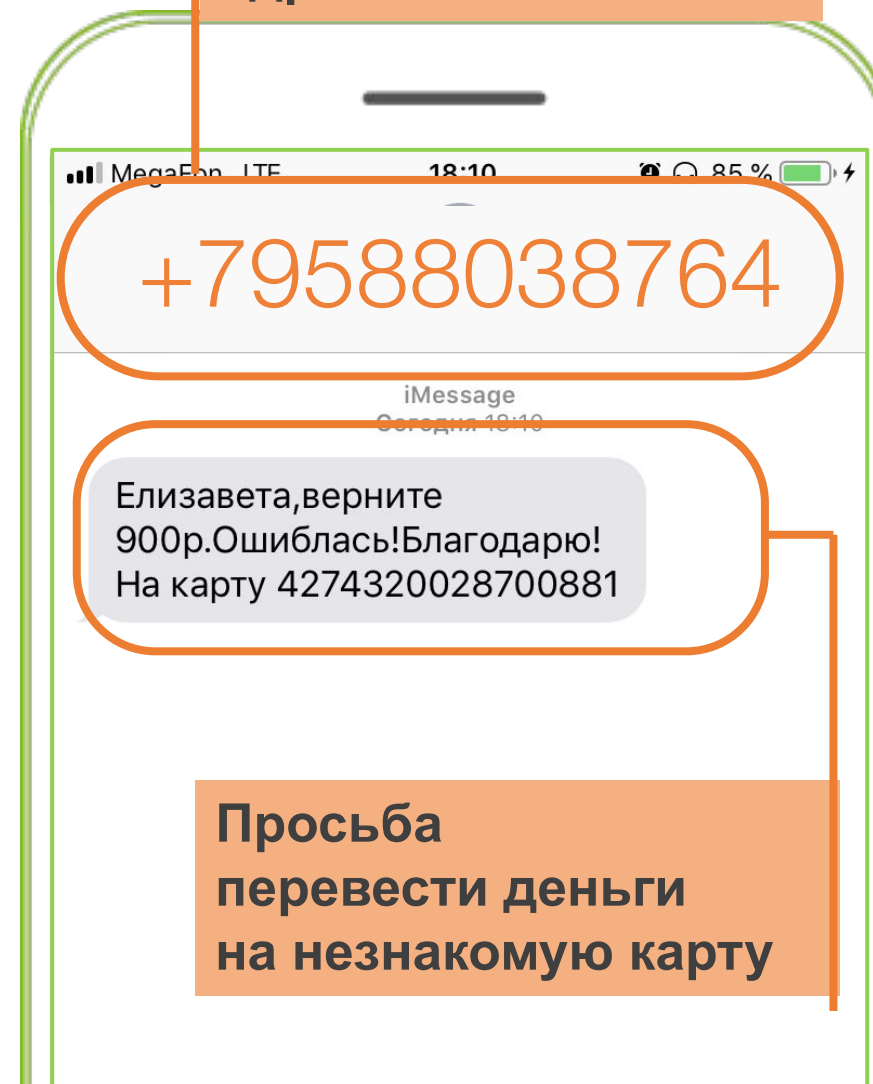
ПРИМЕРЫ МОШЕННИЧЕСКИХ СООБЩЕНИЙ

Сообщение от
незнакомца
адресата



Отсутствует
обращение,
последние цифры
карты

Сообщение от
незнакомца
адресата



Просьба
перевести деньги
на незнакомую карту

РАЗДЕЛ 3

ЧТО ДЕЛАТЬ, ЕСЛИ ВАС ОБМАНУЛИ

ДЕЙСТВИЯ ПРИ МОШЕННИЧЕСТВЕ



Позвоните в банк по официальным номерам, например, в Сбербанке:



В мобильном приложении

Нажмите иконку телефона в левом верхнем углу



900

С мобильного телефона, звонки по России бесплатные



+7 495 500-55-50

Для звонков из любой точки мира, по тарифам оператора

ОСНОВНЫЕ ПРАВИЛА

- 1 Нельзя сообщать никому: логины, пароли, CVV-коды от банковских карт, подтверждающие пароли из СМС
- 2 Не совершайте операции по просьбе незнакомцев
- 3 Не переходите по ссылкам с неизвестных номеров
- 4 Используйте антивирус

1.

Вам позвонили
из Службы
безопасности банка,
говорят, что
зафиксировано
мошенничество и для
защиты средств, срочно
скажите ваши данные
карты и код из СМС.
Как поступите?



А

Диктую, записывайте...

В

Не скажу свои данные

С

Расскажу об этом соседке

2.

Вам у метро
предлагают взять
SIM-карту
с выгодным тарифом
и сразу установить
на нее услугу
«мобильный банк»?



А

Возьму только SIM-карту

В

Подключу

С

Откажусь

3.

Как понять,
что звонит
сотрудник банка,
а не мошенник?



А

У сотрудника вежливый и
хорошо поставленный голос

В

Слышен шум колл-центра

С

Банк не запрашивает коды и
пароли из СМС