SCS SBERBANK CYBER SECURITY

КАК ЗАЩИТИТЬСЯ ОТ МОШЕННИКОВ?

БАНКОВСКАЯ КАРТА

Что важно знать:

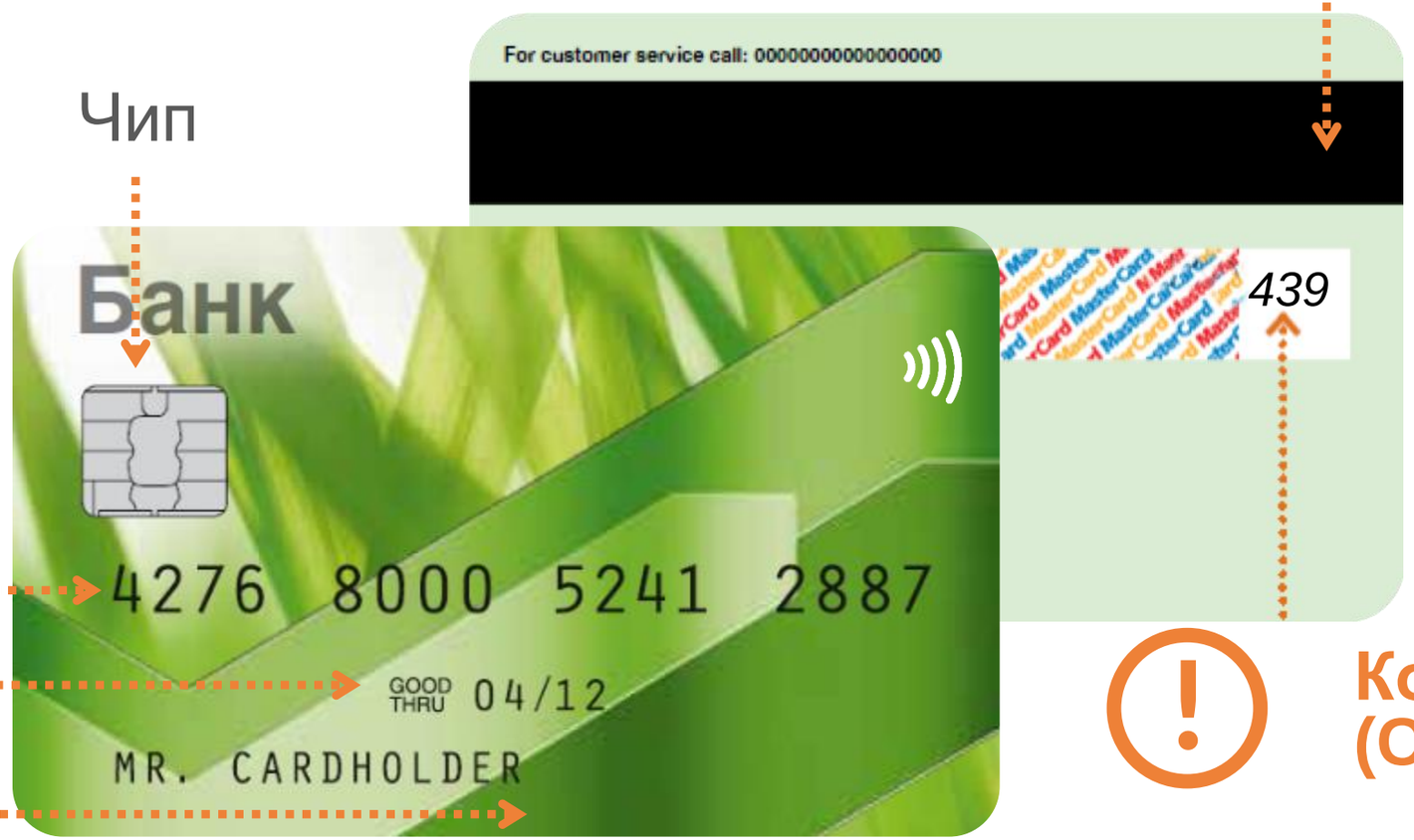
Магнитная полоса

Чип

Номер карты

Срок действия

Имя держателя



Код безопасности (CVC)

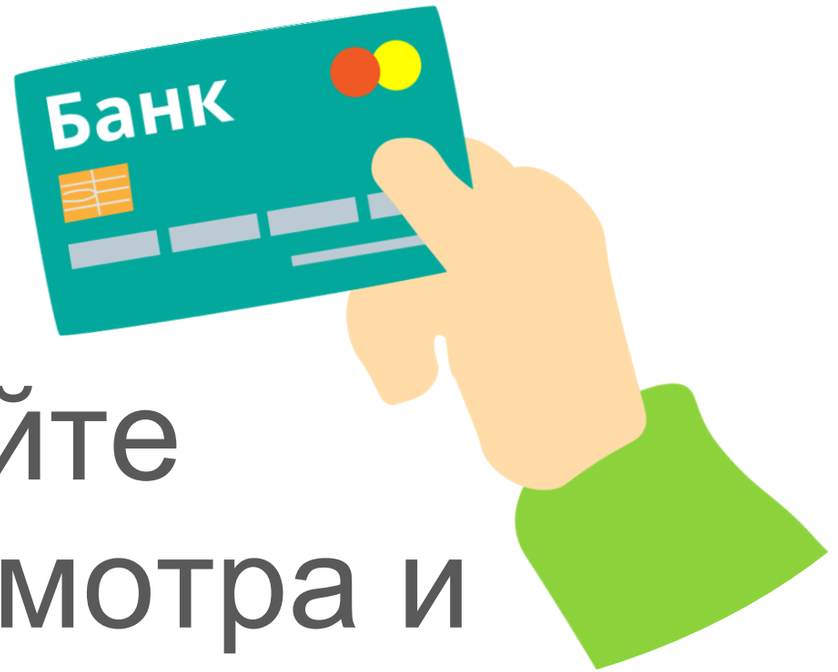
PIN-код - пароль для работы с банкоматом, выдается банком в запечатанном конверте

СБЕРБАНК

1

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Карта - доступ ко всем электронным деньгам



Не оставляйте ее без присмотра и не передавайте никому

2

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Никому не говорите ПИН-код и код безопасности

Не храните ПИН-код рядом с картой

3

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

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

4

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Осмотрите банкомат перед снятием денег, нажмите кнопку «отмена»

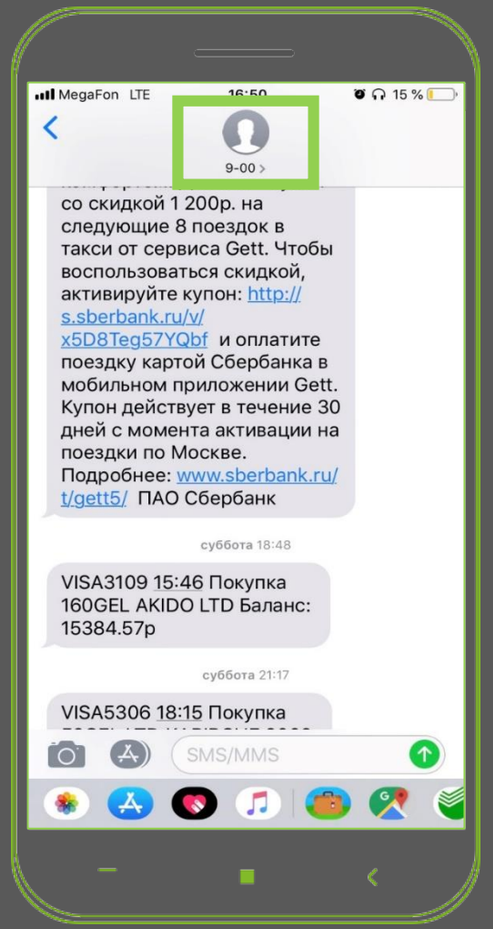
5

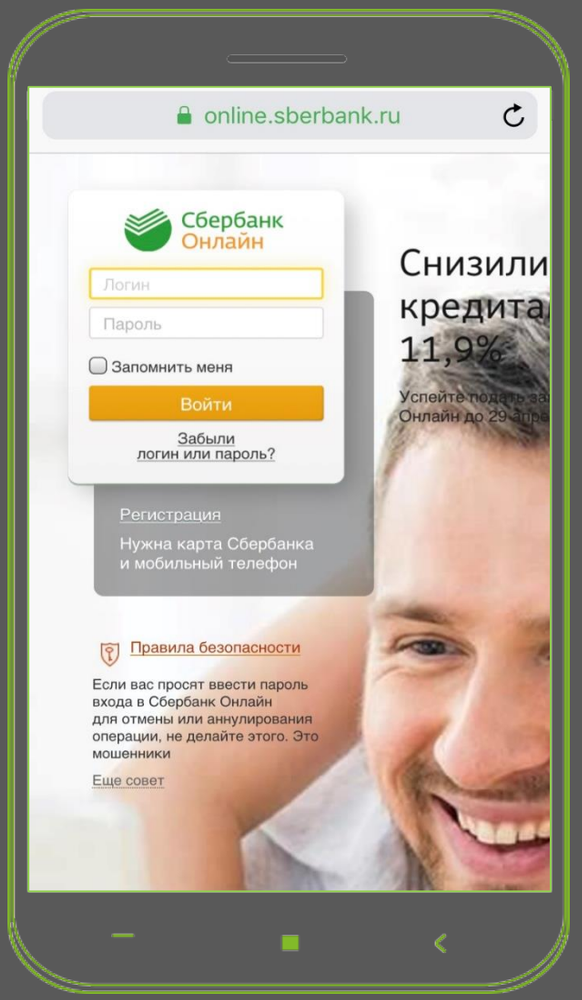
РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Не выбрасывайте в урну чек, который печатает банкомат

SCS SBERBANK CYBER SECURITY

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНОГО И ОНЛАЙН-БАНКА





1

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Если потеряли телефон или сменили номер мобильного, обратитесь в банк

2

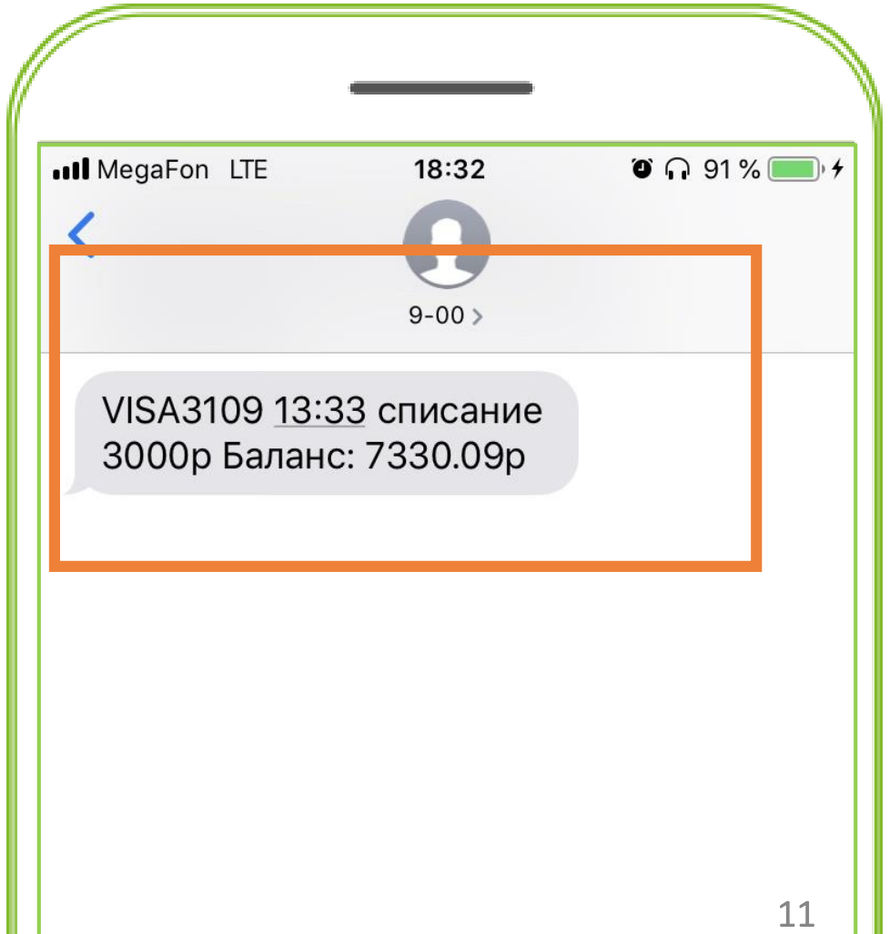
РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Не подключайте к СМС-сервису чужие телефоны

3

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

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



4

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Скачивайте мобильное приложение в официальных магазинах

Загрузите в App Store

Загрузите в Google Play

Установите Сбербанк Онлайн с встроенным антивирусом

5

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Разработчики постоянно исправляют уязвимости и добавляют функции, повышающие безопасность

Своевременно обновляйте программное обеспечение и антивирус

SCS SBERBANK CYBER SECURITY

КАК НЕ ПОПАСТЬСЯ НА УЛОВКИ МОШЕННИКОВ?

ЧТО НУЖНО ЗНАТЬ О МОШЕННИЧЕСТВЕ?

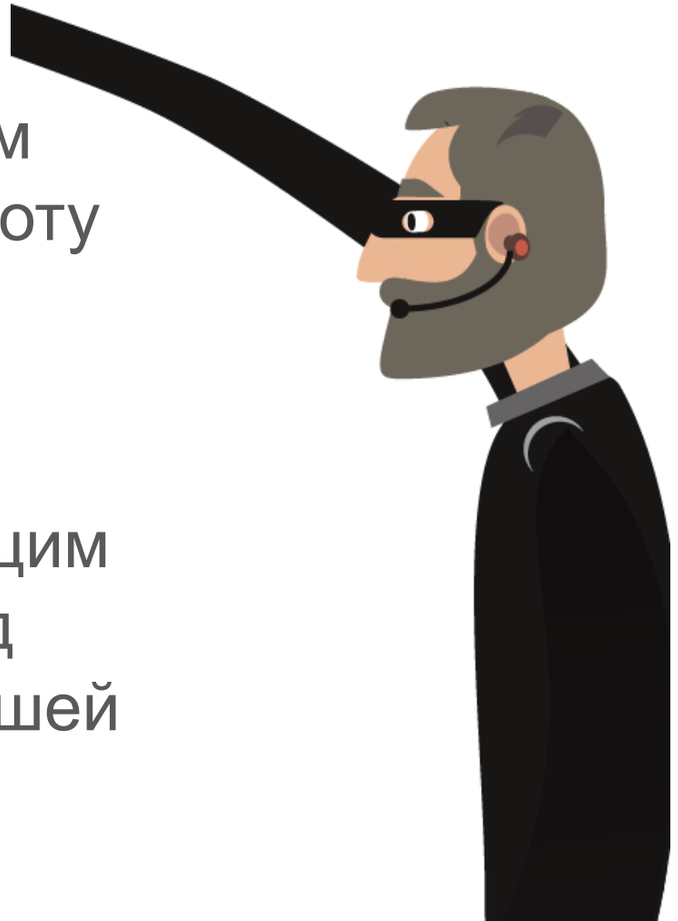
Социальная инженерия – воздействие мошенников на людей, при котором люди собственными руками отдают свои деньги или сообщают данные

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

КЕМ МОЖЕТ ПРЕДСТАВИТЬСЯ МОШЕННИК?

СБЕРБАНК

- Вашим родственником, «попавшим в беду», в связи с чем он просит перевести деньги
- Сотрудником ПФР, предлагающим льготы и путевки, удаленную работу при этом просит оплатить регистрационный взнос
- Сотрудником банка, выманивающим данные карты и коды из СМС под предлогом мошенничества по вашей карте или сбоя системы



КЕМ МОЖЕТ ПРЕДСТАВИТЬСЯ МОШЕННИК?

- Сотрудником социальных служб, предлагающим компенсации
- Сотрудником ПХО/прокуратуры/иных организаций, рассказывающим о мошенничестве, выгодном вложении денег, брокерских или дилерских услугах
- Покупателем Вашего товара с сайта, выманивающим данные карты и коды из СМС, под предлогом перевода Вам аванса

КАК РАСПОЗНАТЬ МОШЕННИКА ПО ТЕЛЕФОНУ?

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, код из СМС)

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

СБЕРБАНК

1

Постарайся успокоиться и не принимать решений сразу

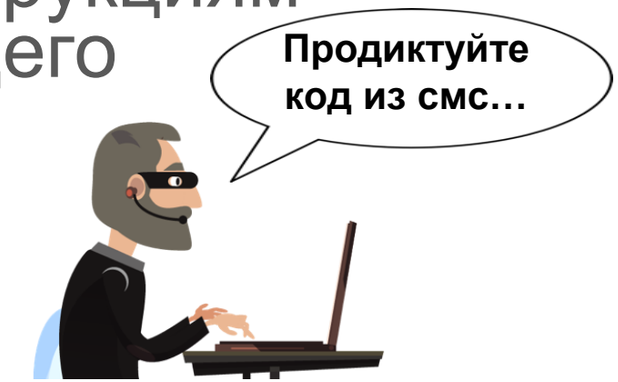
2

Помни – работники банка никогда не запрашивают:

- CVV-код,
- логин и пароль от Сбербанк Онлайн,
- код из СМС

3

Не совершайте какие-либо операции с картой по инструкциям звонящего



4

Положите трубку и перезвоните сами по **официальному номеру организации**

SCS SBERBANK CYBER SECURITY

РАСПРОСТРАНЕННЫЕ КЕЙСЫ МОШЕННИЧЕСТВА

Социальная инженерия: «Звонок из Службы безопасности»

1

На телефон клиента поступает звонок с номера похожего или неотличимого от номера Банка.

ВНИМАНИЕ!

У мошенников есть возможность позвонить клиенту с номера, который может выглядеть, например так:

+7900, +90 0

они могут использовать номера банка, меняя в них одну цифру, которую клиент может не заметить и подумать, что это банковский номер*

- Злоумышленники покупают у сотовых операторов виртуальные АТС и оформляют их на одноразовые СИМ-карты. При помощи специального веб-интерфейса, номера станций меняются на любые. При звонке клиентам они подставляют официальный номер Банка, номер **900**, будет выглядеть, например так **+7900, +90 0, 4995005550 или 4955055550**

Социальная инженерия: «Звонок из Службы безопасности»

SCS SBERBANK CYBER SECURITY

2

Мошенник представляется сотрудником, например, «безопасности» и говорит:

а банк выявил подозрительную операцию, в целях сохранности средств нужно провести некоторые манипуляции. Для этого у клиента запрашивают конфиденциальную информацию: полные данные карты, включая **CVV-код**, **коды из смс**, логин и пароль от Сбербанк Онлайн

б к счетам клиента доступ получили злоумышленники и деньги нужно перевести на защищенный банковской счет, который закреплен за персональным менеджером. Клиент соглашается, ему дают реквизиты по которым клиент сам переводит деньги при чем **ФИО** получателя совпадает с **ФИО** персонального менеджера

Социальная инженерия: «Звонок из Службы безопасности»

3

При возражении со стороны клиента в предоставлении данной информации мошенники

а говорят, что они звонят с официального номера и предлагают проверить этот номер на сайте банка

б говорят, что в целях конфиденциальности они включат программу-робот, которая сможет расшифровать сказанное клиентом и не позволит разгласить конфиденциальную информацию. После этого в разговоре мошенники включают аудиозапись, в ходе прослушивания которой клиент слышит негромкий шелест

в для убедительности называют персональные данные клиента, и просят клиента самостоятельно сделать перевод своих денег на защищенный банковской счет, который закреплен за персональным менеджером, а потом их можно будет вернуть назад после проведения всех необходимых мероприятий

Социальная инженерия: «Звонок из Службы безопасности»

4

Клиент соглашается и предоставляет все необходимые данные

5

Происходит хищение денежных средств посредством:

- p2p-сервисов сторонних банков или других ресурсов*,
- перевода на карту другого клиента Сбербанка,
- оплаты сотовой связи,
- перевода на карту в другом банке через СБОЛ

*Peer-to-Peer - от человека к человеку - это переводы денег между двумя владельцами банковских карт. Сервисы P2P-платежей позволяют выполнить перевод денежных средств в течение нескольких секунд, даже в том случае, если денежные счета принадлежат двум разным банкам или платёжным системам. Для перевода денег достаточно знать номер банковской карты получателя и его ФИО

Как защитить себя. Социальная инженерия: «Звонок из Службы безопасности»

1

Запишите номера банка в телефонную книгу: **900**, **8800555-55-50**
Если звонок будет с другого номера, он отобразится как неизвестный

Как защитить себя. Социальная инженерия: «Звонок из Службы безопасности»

2

В случае общения по телефону с «представителями банков» помните - работники банка никогда не запрашивают ПИН- или CVV2/CVC2-код, логин, пароль от Сбербанк Онлайн или код из СМС

3

Не совершайте какие-либо операции с картой по инструкциям звонящего, сотрудник банка все операции для защиты карты делает сам

4

Сразу прекратите разговор и завершите вызов. Проверьте, не было ли сомнительных операций за время разговора. Если сообщили мошенникам финансовую или личную информацию, сразу обратитесь к своему персональному менеджеру или позвоните

в контактный центр по номеру 900 и сообщите о случившемся

Социальная инженерия: «Перевод «по ошибке»

1

Клиент оставляет объявление с именем и номером телефона на сайтах бесплатных объявлений

2

На телефон клиента поступает **СМС** с частного мобильного номера:

Sberbank Онлайн. ДАНИЛ АЛЕКСАНДРОВИЧ Б. перевел(а) Вам 1000.00 RUB.

Социальная инженерия: «Перевод «по ошибке»

3

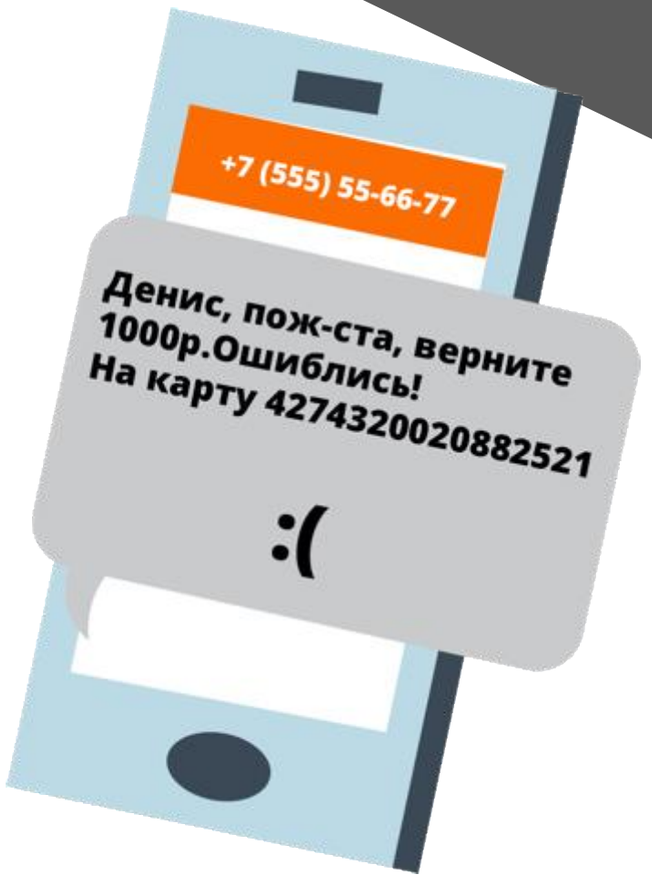
После этого с другого номера приходят сообщения следующего содержания: «Денис, пож-ста, верните 1000р.Ошиблись! На карту 4274320020882521»

4

Клиент самостоятельно осуществляет перевод со своей карты на карту мошенника

5

Мошенники пропадают, клиент не может связаться с мошенниками и жалуется в Банк на несанкционированный перевод



Как защитить себя. Социальная инженерия: «Перевод «по ошибке»

1

Помните - Сбербанк отправляет СМС

только с номера 900 или 9000

2

Перед тем, как подтвердить платежную операцию, убедитесь, что все реквизиты указаны верно

3

Если заподозрили СМС-мошенничество,

сразу обратитесь к своему персональному менеджеру или позвоните

в контактный центр по номеру 900

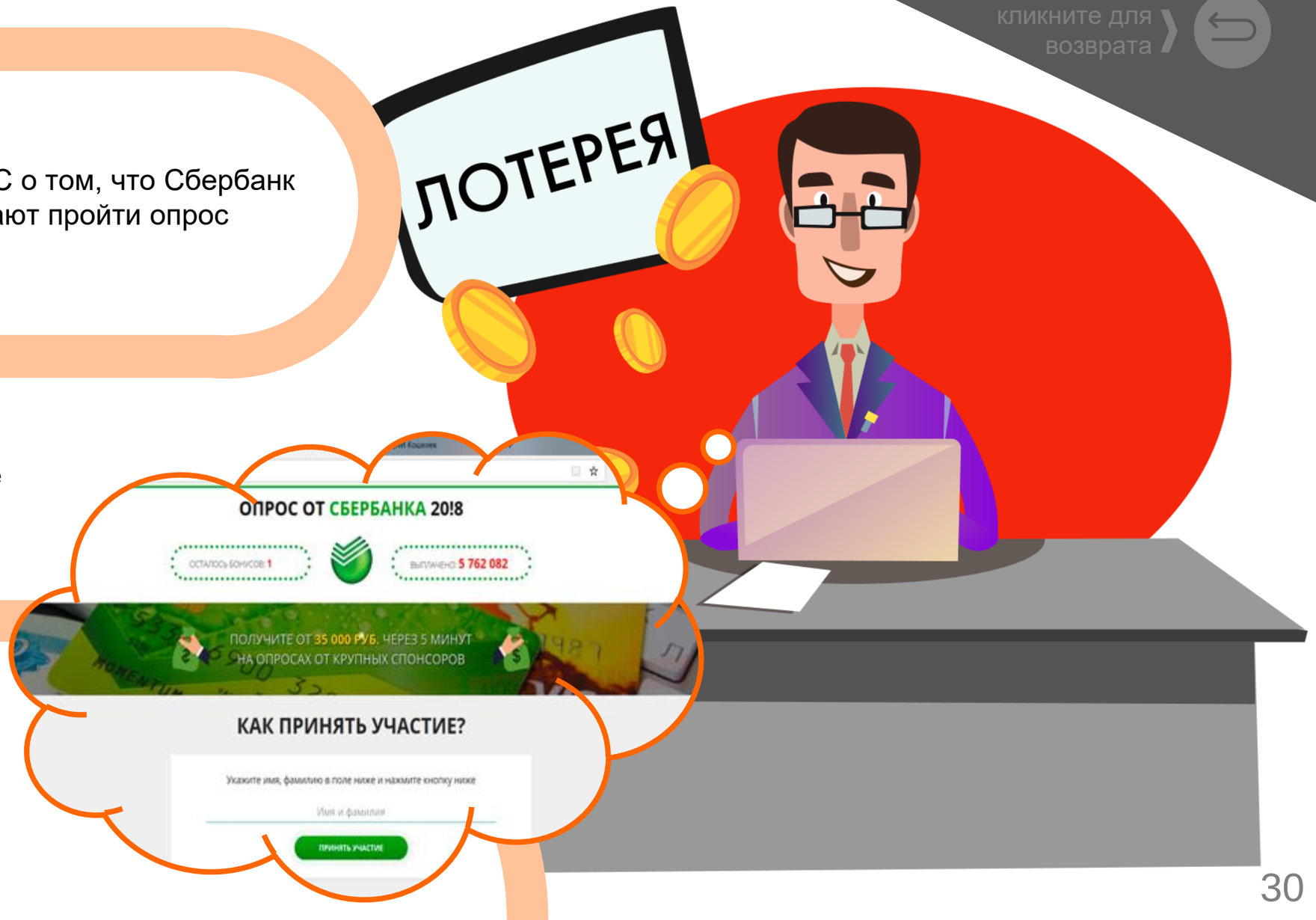
Социальная инженерия: «Опрос от Сбербанка»

1

Клиент получает письмо, СМС о том, что Сбербанк проводит лотерею и предлагают пройти опрос

2

Клиент переходит по ссылке на фишинговый сайт



Социальная инженерия: «Опрос от Сбербанка»

3

После шести вопросов, которые начинаются с того, пользуется ли клиент мобильным банком, ему сообщают, что за участие в опросе ему начислено вознаграждение 153015 руб.

4

Для подтверждения карты и перечисления бонусов на баланс клиента просят произвести «закрепительный платеж» в размере 150 руб.

5

Клиент самостоятельно переводит (иногда несколько раз) «закрепительный платеж». Клиент не может связаться с мошенниками и жалуется в Банк на несанкционированный перевод

Как защитить себя. Социальная инженерия: «Опрос от Сбербанка»

SBERBANK CYBER SECURITY

1

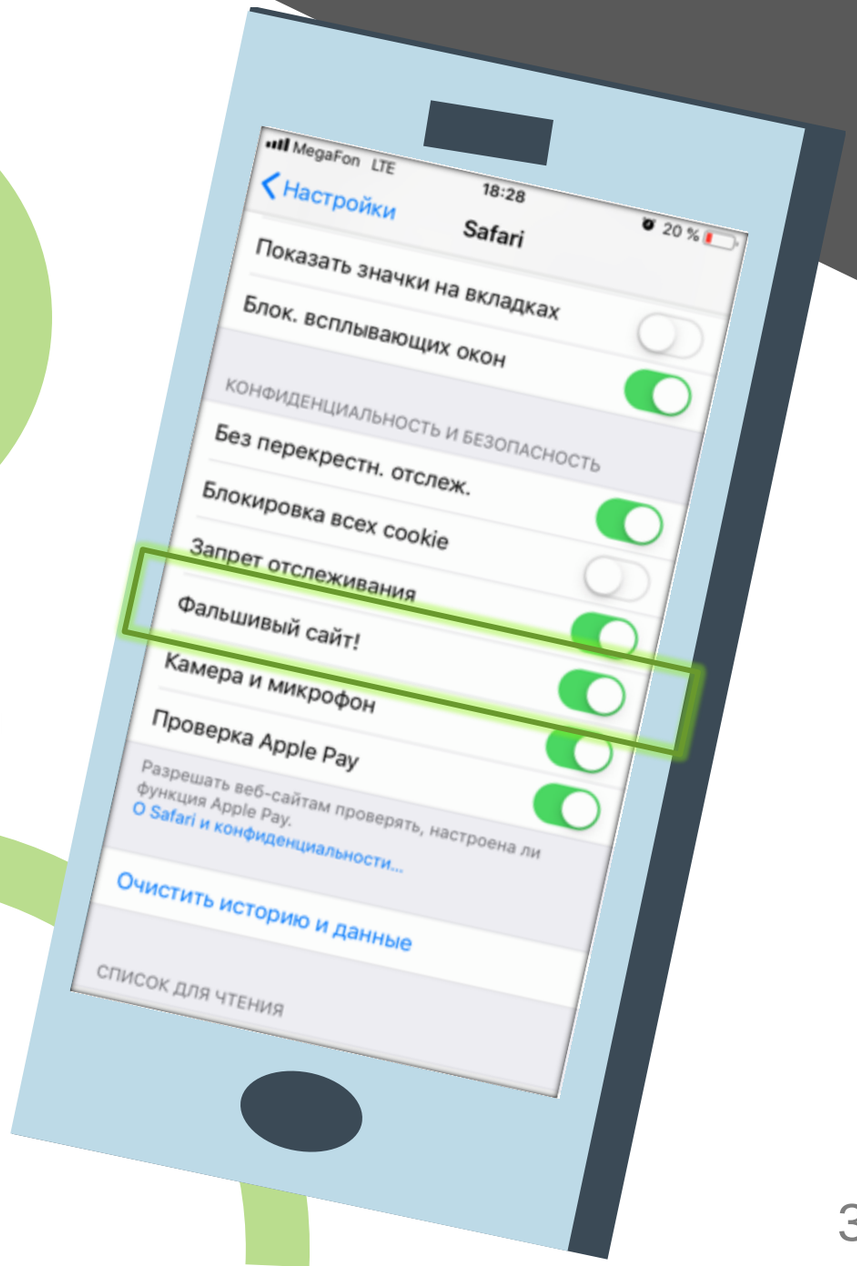
- Настройте блокировку фальшивых сайтов в Safari
- При оплате проверяйте адрес сайта и вводите данные только если домен точно совпадает с официальным названием сайта

2

- Выбирайте защищённое интернет-соединение – это повышает вероятность легитимности сайта. Адрес сайта должен начинаться с букв https, а не с http, а в адресной строке должен отображаться значок в виде закрытого замка

3

- Подключите Мобильный банк, он понадобится для работы системы 3-D Secure (технология подтверждения платежа паролем от банка)
- При подозрении на фишинговый сайт вы можете проверить домен на специализированных сайтах (например, VirusTotal)



SCS SBERBANK CYBER SECURITY

ЧТО ДЕЛАТЬ, ЕСЛИ СТОЛКНУЛИСЬ С МОШЕННИКАМИ?

SCS SBERBANK CYBER SECURITY

Мы всегда на связи

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

SCS SBERBANK CYBER SECURITY

Мы всегда на связи

ИЛИ

1. Зайдите в интернет-банк
или мобильное приложение Сбербанк Онлайн
2. Выберете карту
3. Нажмите «Заблокировать карту»
4. После чего позвоните в банк

SCS SBERBANK CYBER SECURITY

Сбербанк отправляет СМС только с номеров 900 и 9000

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

36