SCS SBERBANK CYBER SECURITY

СБЕРБАНК

КАК ЗАЩИТИТЬСЯ ОТ МОШЕННИКОВ?

КАКИЕ ДАННЫЕ ЕСТЬ НА БАНКОВСКОЙ КАРТЕ?

Магнитная полоса

Чип

Номер карты

Срок действия

Имя держателя

Код безопасности (CVC)

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

ЧТО ТАКОЕ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ?

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

ЧТО ТАКОЕ МОШЕННИЧЕСТВО ПО ТЕЛЕФОНУ?

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

НУЖНО ПОЛОЖИТЬ ТРУБКУ ЕСЛИ ВАМ ЗВОНЯТ ИЗ «БАНКА» И…?

A

Просят сказать номер карты, CVV-код, код из СМС

B

Спрашивают обратную связь об услуге

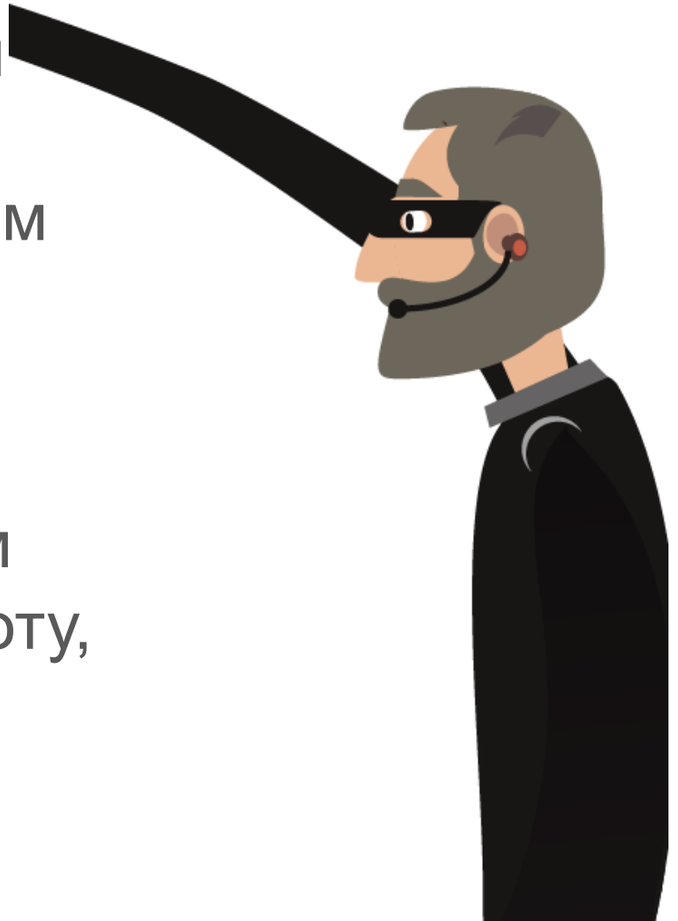
C

Говорят об угрозе мошенничества и предлагают перевести деньги на резервный счет

КЕМ МОЖЕТ ПРЕДСТАВИТЬСЯ МОШЕННИК?

СБЕРБАНК

- Сотрудником Службы безопасности, выманивающим данные карты и пароли из СМС под предлогом мошенничества по вашей карте или сбоя системы
- 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



КЕМ МОЖЕТ ПРЕДСТАВИТЬСЯ МОШЕННИК?

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

1

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Постарайтесь успокоиться и не принимать решений сразу

2

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

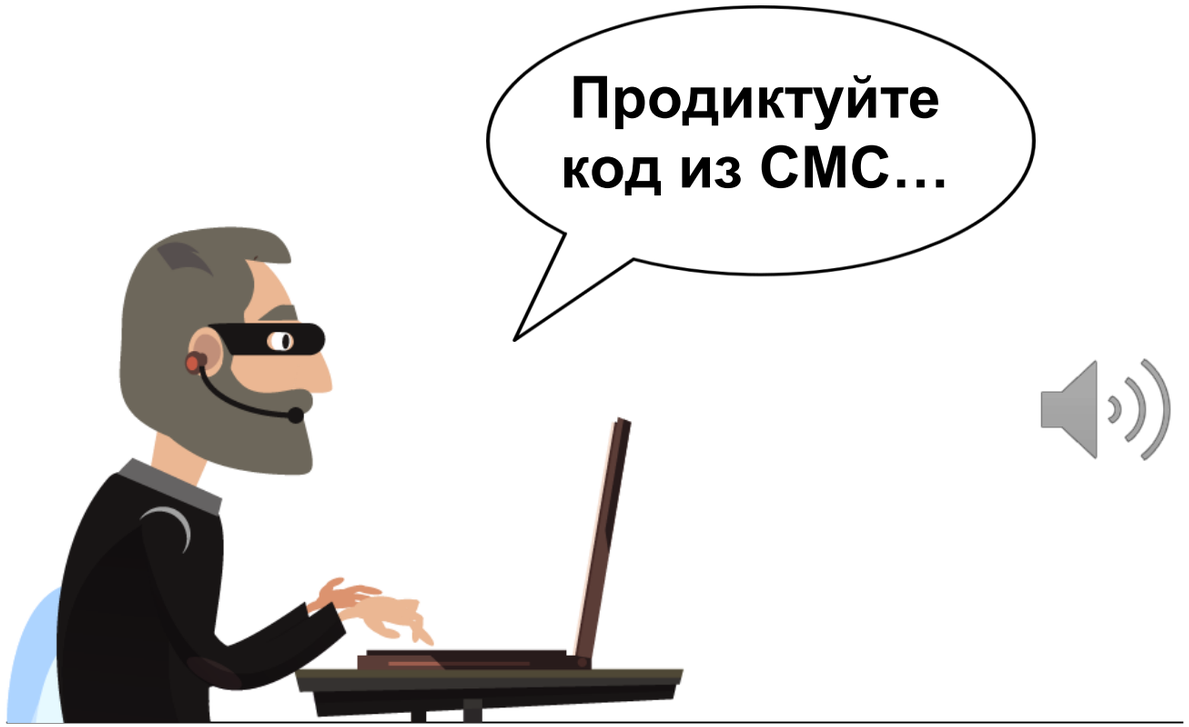
Помните – работники банка никогда не запрашивают

- код безопасности (CVV)
- логин и пароль от Сбербанк Онлайн
- код из СМС

3

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Не совершайте какие-либо операции с картой по инструкциям звонящего



4

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Положите трубку и перезвоните сами по **официальному номеру организации,** его можно узнать на сайте

SCS SBERBANK CYBER SECURITY

СБЕРБАНК

РАСПРОСТРАНЕННЫЕ СХЕМЫ МОШЕНИЧЕСТВА

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

Социальная инженерия: «Звонок из Службы безопасности»

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, пароли 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:

- перевода на карту другого клиента,
- оплаты сотовой связи,
- перевода на карту в другом банке через СБОЛ

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

СБЕРБАНК

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»

СБЕРБАНК

2

В случае общения по телефону с «представителями банков» помните - работники банка никогда не запрашивают CVV/CVC-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

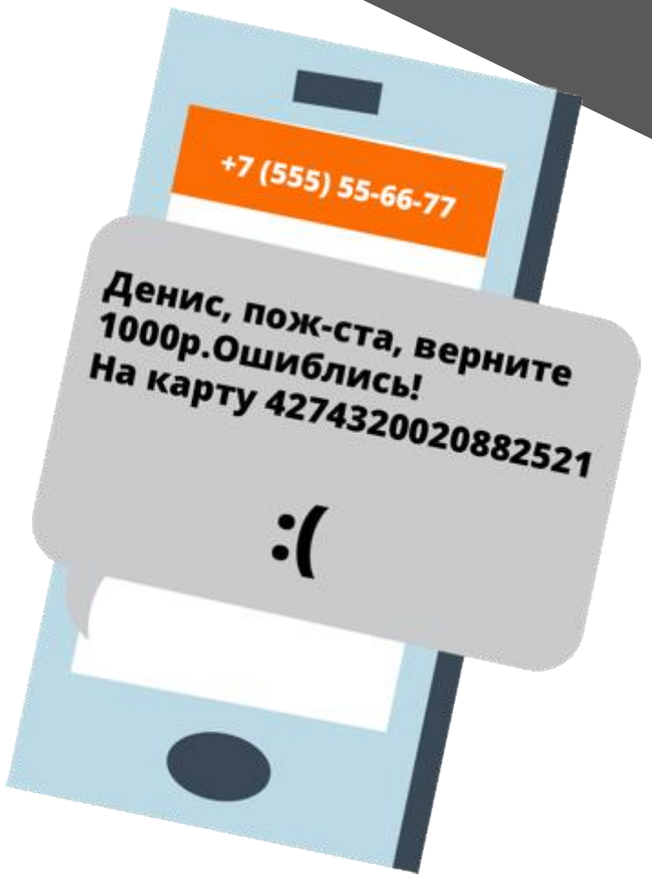
После этого с другого номера приходят сообщения следующего содержания: «Денис, пож-ста, верните 1000р.Ошиблись! На карту 4274320020882521»

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»

СБЕРБАНК

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 позвоните в контактный центр по номеру **900**

Социальная инженерия: «Опрос от Сбербанка»

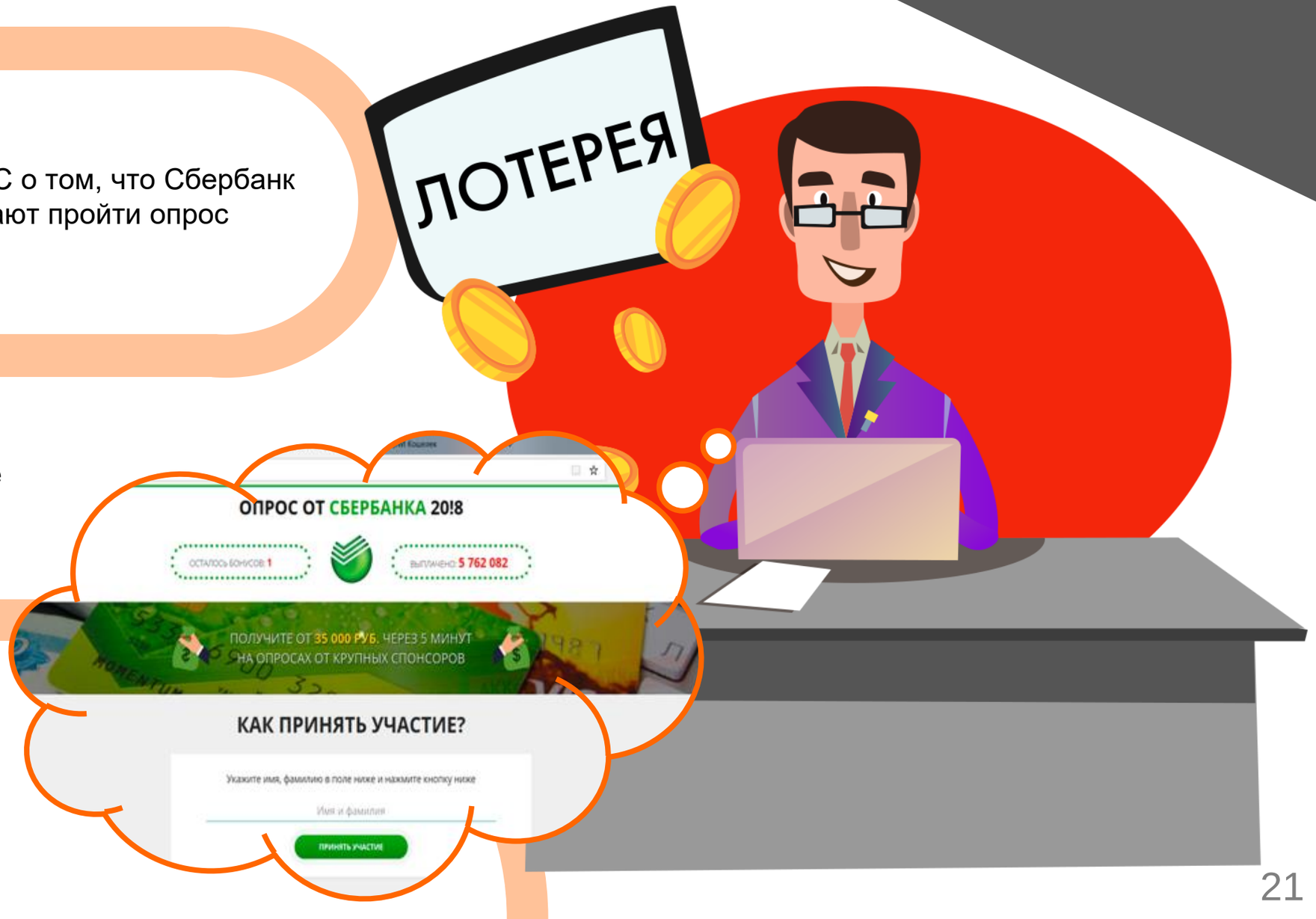
СБЕРБАНК

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»

СБЕРБАНК

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»

СБЕРБАНК

1

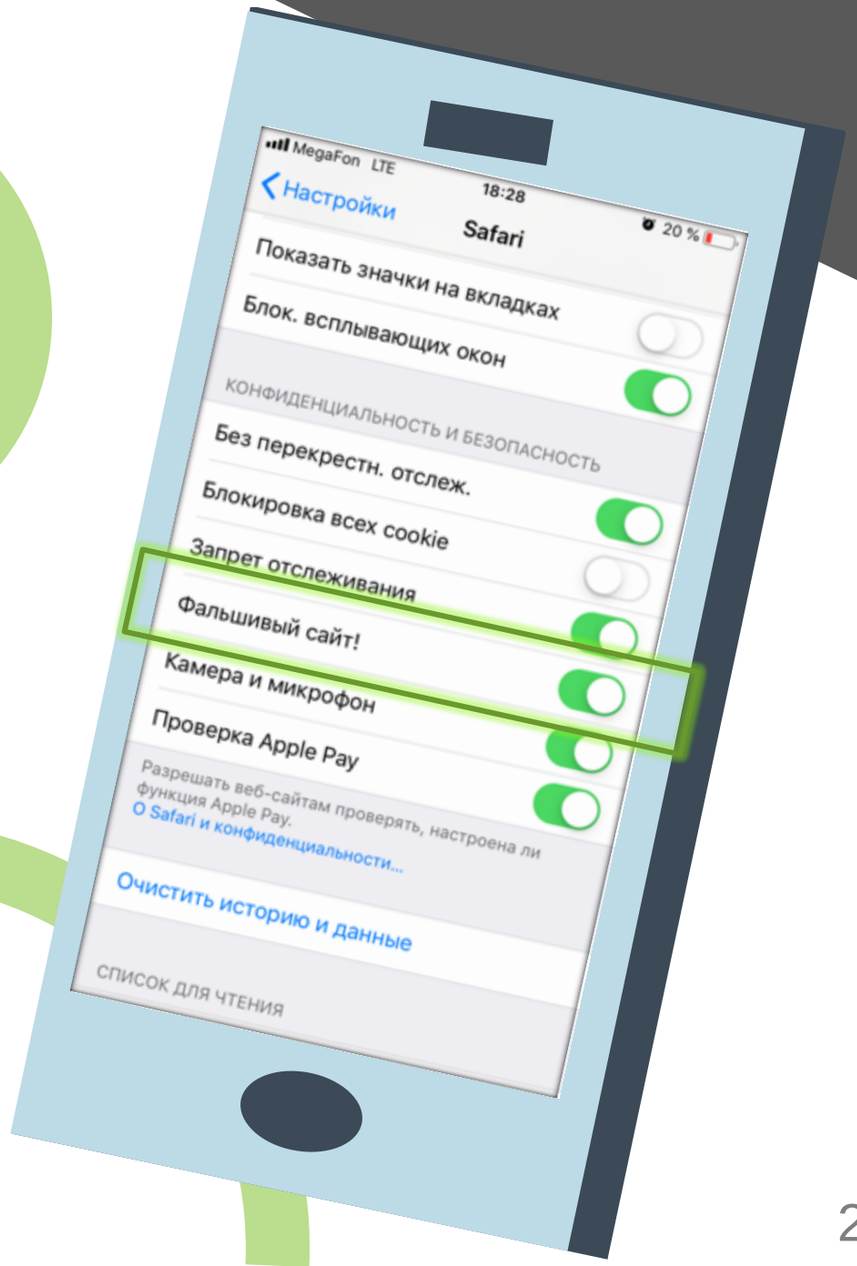
- При оплате проверяйте адрес сайта и вводите данные только если домен точно совпадает с официальным названием сайта

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 подтверждения платежа паролем от банка
- При подозрении на фишинговый сайт вы можете проверить домен на специализированных сайтах (например, VirusTotal)



СБЕРБАНК

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

ПРОВЕРЬТЕ СЕБЯ

1.

Вы потеряли телефон, к которому подключена услуга «Мобильный банк», куда следует обратиться?

A

К оператору сотовой связи

B

В контактный центр банка

C

И к оператору, и в банк

2.

Вы получили новую банковскую карту. Как хранить ПИН-код?

A

В заметках на смартфоне,
чтобы всегда был рядом

B

В ежедневнике,
чтоб посмотреть, когда нужно

C

ПИН-код надо запомнить

3.

Кажется, вы случайно сообщили мошенникам важную информацию. Как теперь быть?

A

Срочно им перезвонить

B

Срочно в банк

C

Будь что будет, в следующий раз буду внимательнее