



**СБЕР
КИБЕР
БЕЗОПАСНОСТЬ**

Защита от телефонного мошенничества



Содержание



Социальная инженерия

Основные схемы телефонного мошенничества

Уловки телефонных мошенников

Как защитить себя



Социальная инженерия



Социальная инженерия – это...



...психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации

Социальная инженерия лежит в основе всех методов и видов кибермошенничества, включая телефонное

Человек был и остается самым слабым местом в любой системе защиты: начиная от домашней сети и заканчивая эшелонированными системами безопасности крупной корпорации. **«Взломай» человека – взломаешь все остальное**



На чем играют злоумышленники?

На чувствах



Страх



Доверие



Невнимательность



Жадность



Сочувствие

Какие фразы используют мошенники



Примите участие
в расследовании...

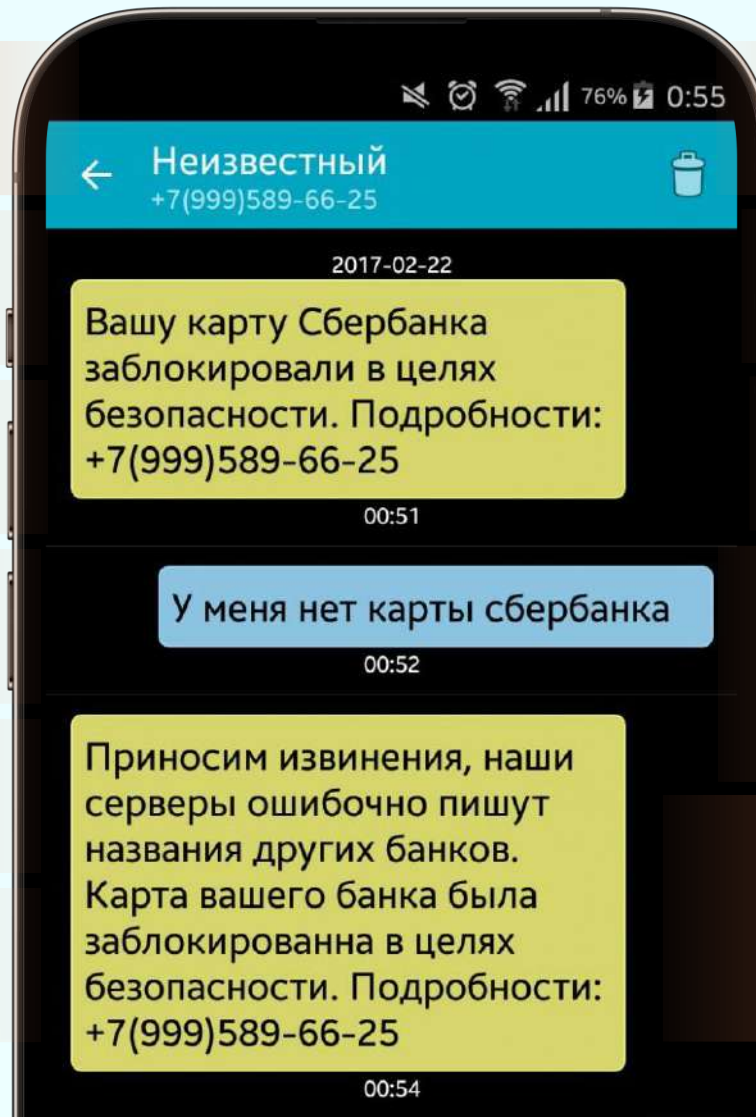
Помогите поймать
нечестного сотрудника...

На Вас оформили
кредит/доверенность...

С Вашего счета хотят перевести
деньги в другом городе...

Продиктуйте код для отмены
мошеннической операции...

Робот: Ваша карта заблокирована,
перезвоните, пожалуйста по номеру...



Голосовой помощник:
сообщите SMS-код

Давайте уточним остаток
средств на Вашей карте...

В каких ещё банках у вас
открыты счета?

По защищенной линии я
переведу Ваш звонок на
специалиста из другого
банка...

Чтобы на Вас не
оформили кредит, будем
отменять протокол Банка
России

Основные схемы телефонного мошенничества



Звонок от имени банка



Мошенник представляется сотрудником службы безопасности / технической поддержки банка

«Давайте уточним остаток средств на ваших счетах...»

Уловки мошенников



«Сбережения в опасности, их могут украсть, поэтому их нужно перевести на «безопасный» счёт»



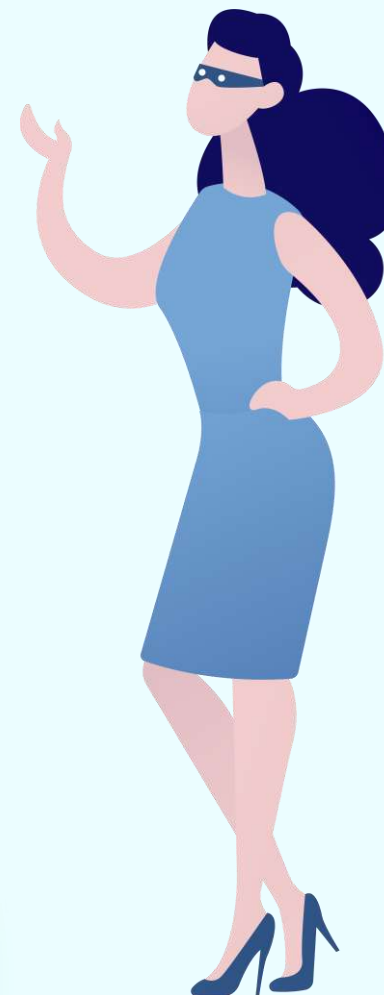
«На ваше имя пытаются оформить кредит в другом городе»



«Назовите реквизиты банковской карты, срок действия и трехзначный код для защиты средств»

Часто в схеме участвует не один человек

Например, для большей убедительности «сотрудник» банка может перевести звонок на «техническую поддержку / специалиста Центрального банка»



Звонок от имени Правоохранительных органов

Мошенник представляется сотрудником **МВД / СК / ФСБ**

Уловки мошенников



«Вам нужно вывести все деньги с банковских карт и счетов, и перевести их на «безопасный» счет»



«Вы должны исчерпать свой кредитный лимит по карте и перевести средства на «безопасный» счет для сохранности»

«По вашим поддельным документам кто-то пытается взять кредит на крупную сумму...»

Часто в схеме участвует не один человек

Например, для большей убедительности «сотрудник МВД» может перевести звонок на «службу безопасности Центрального банка»

Помимо кражи средств мошенники все чаще склоняют жертв к совершению противоправных действий в отделениях банков якобы с целью «помощи в поимке преступников» или «предотвращения общественно опасных деяний»



Звонок от имени родственников или близких



Мошенник представляется **сыном / внучкой / родственником**

Весь диалог строится с расчетом на то, что жертва не успеет опомниться, а непохожесть голос спишет на стрессовое состояние

Все фразы говорятся быстро и с максимально достоверной актерской игрой, чтобы ввести потенциальную жертву в стресс и не дать мыслить рационально

Суть всей «игры» – якобы нужна крупная сумма денег на «покрытие ущерба», «лечение», «взятку, чтобы не заводить уголовное дело»

Злоумышленники отправляют курьера по адресу жертвы, чтобы забрать деньги, после чего исчезают

«Я сбил на машине ребенке, но уже договорился о взятке, срочно нужны деньги...»



Уловки телефонных мошенников



«Единый государственный реестр»



Мошенники создают сайты, на которых якобы можно проверить, действительно ли вам звонит настоящий сотрудник банка или полиции



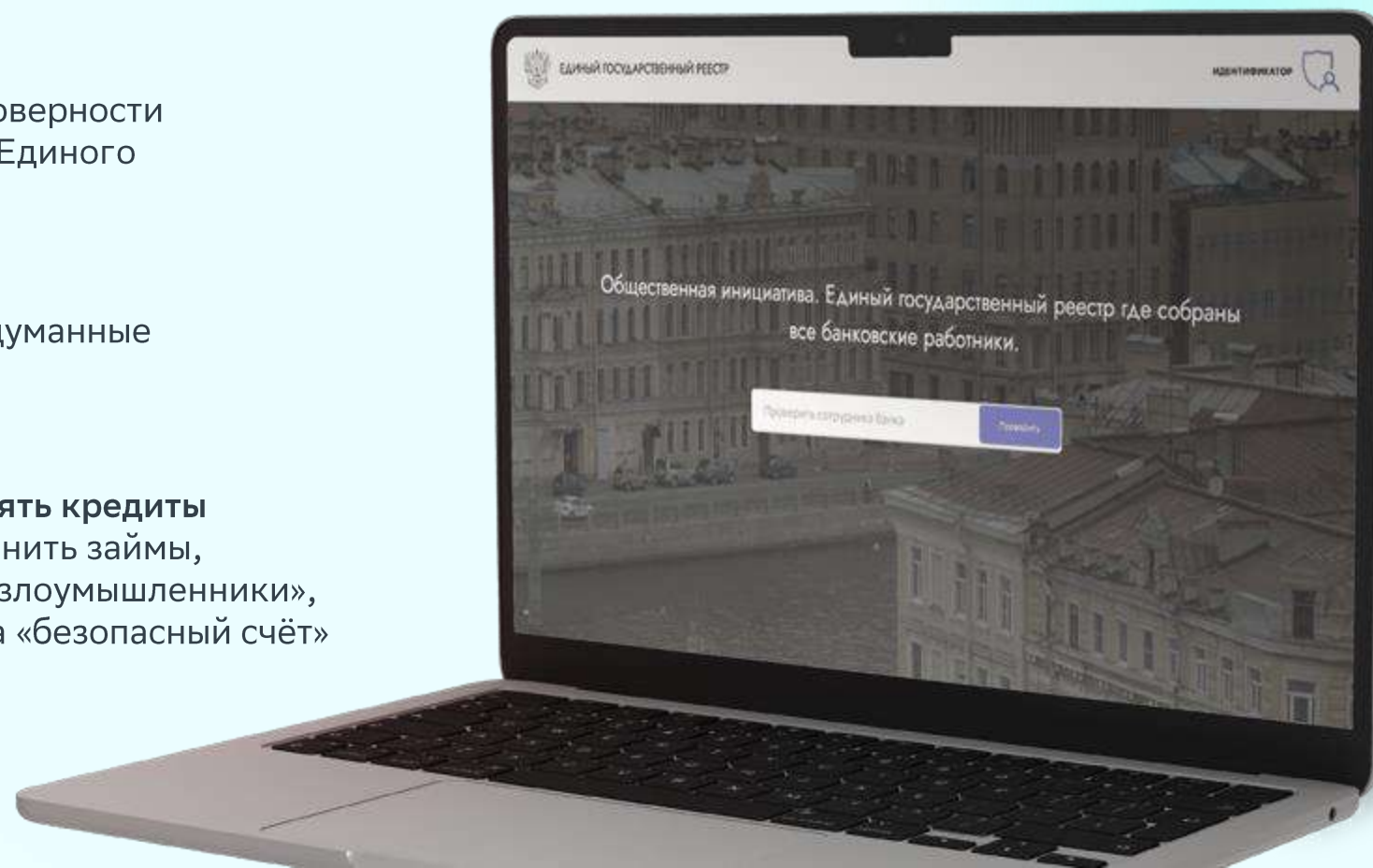
Жертве предлагают убедиться в достоверности сообщаемой информации через сайт «Единого государственного реестра»



После ввода номера жертва видит выдуманные характеристики «работника»



Мошенник убеждает клиента оформлять кредиты в разных банках для того, чтобы «отменить займы, которые пытаются взять от его имени злоумышленники», и перевести взятые в кредит деньги на «безопасный счёт»



Вредоносные мобильные приложения



Мошенники предлагают установить на смартфон приложение для якобы поиска уязвимостей



На самом деле вредоносное программное обеспечение дает злоумышленникам удаленный доступ к телефону



После установки злоумышленники предлагают запустить новое приложение



Мошенники получают удаленный доступ к устройству, к конфиденциальной информации и данным для входа в онлайн-банк, после чего пытаются украсть денежные средства жертвы



Код из СМС



Во время разговора с жертвой мошенники, используя телефонный номер жертвы, **делают запрос на регистрацию в СберБизнес**



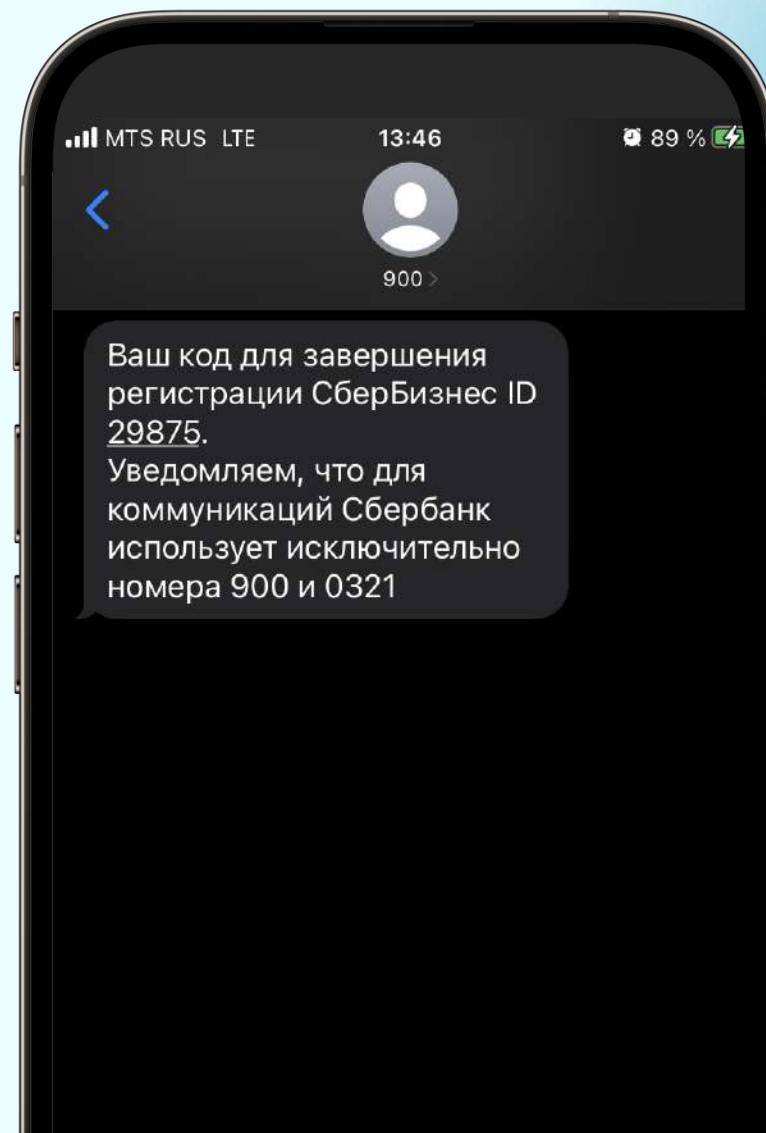
Мошенники предупреждают жертву о том, что им направлен код в СМС якобы для «подтверждения» легитимности звонка



Злоумышленники говорят жертве, что им сообщать код не нужно и предупреждают жертву, что код из СМС никогда никому называть нельзя



Все это делается, чтобы **максимально усыпить бдительность потенциальной жертвы** и создать видимость того, что ей звонит настоящий сотрудник банка. После чего убедить жертву вывести средства на «безопасный» счет становится значительно легче



Как защитить себя





ОСНОВА – ЗДРАВЫЙ СМЫСЛ

Что делать для защиты от мошенничества



Внимательно проверяйте входящий номер



Поставьте приложение для фильтрации входящих вызовов



Не совершайте никаких операций по инструкциям звонящего

ПОМНИТЕ!



Сразу заканчивайте разговор при любых сомнениях



Сотрудники правоохранительных органов не могут допрашивать по телефону



Проверьте, не было ли сомнительных операций за время разговора



ЦБ РФ никогда не звонит физическим лицам



Что делать для защиты от мошенничества



Помните о том, что бесплатный сыр бывает только в мышеловке. Соблюдая это правило, вы обезопасите себя от большинства видов мошенничества



Всегда сомневайтесь в том, что вам предлагают и на какие действия вас мотивируют. Будьте скептиком



Всегда лучше положить трубку и самому перезвонить в банк / своему родственнику для уточнения информации



Обновляйте операционную систему и приложения



Создавайте надежные и уникальные пароли для всех ресурсов



Настройте двухфакторную аутентификацию везде, где это возможно



Создавайте резервные копии важной информации



Устанавливайте только лицензионное ПО и приложения из надежных источников



Не переходите по подозрительным ссылкам

Наши сервисы



«Кибрарий»
Библиотека знаний
по кибербезопасности



МП «Сбербанк Онлайн»
Раздел
«Не дайте себя обмануть»



МП «Сбербанк Онлайн»
«Осторожно, мошенники!»
Канал об актуальных схемах
мошенничества



МП «Сбербанк Онлайн»
Настройки безопасности

