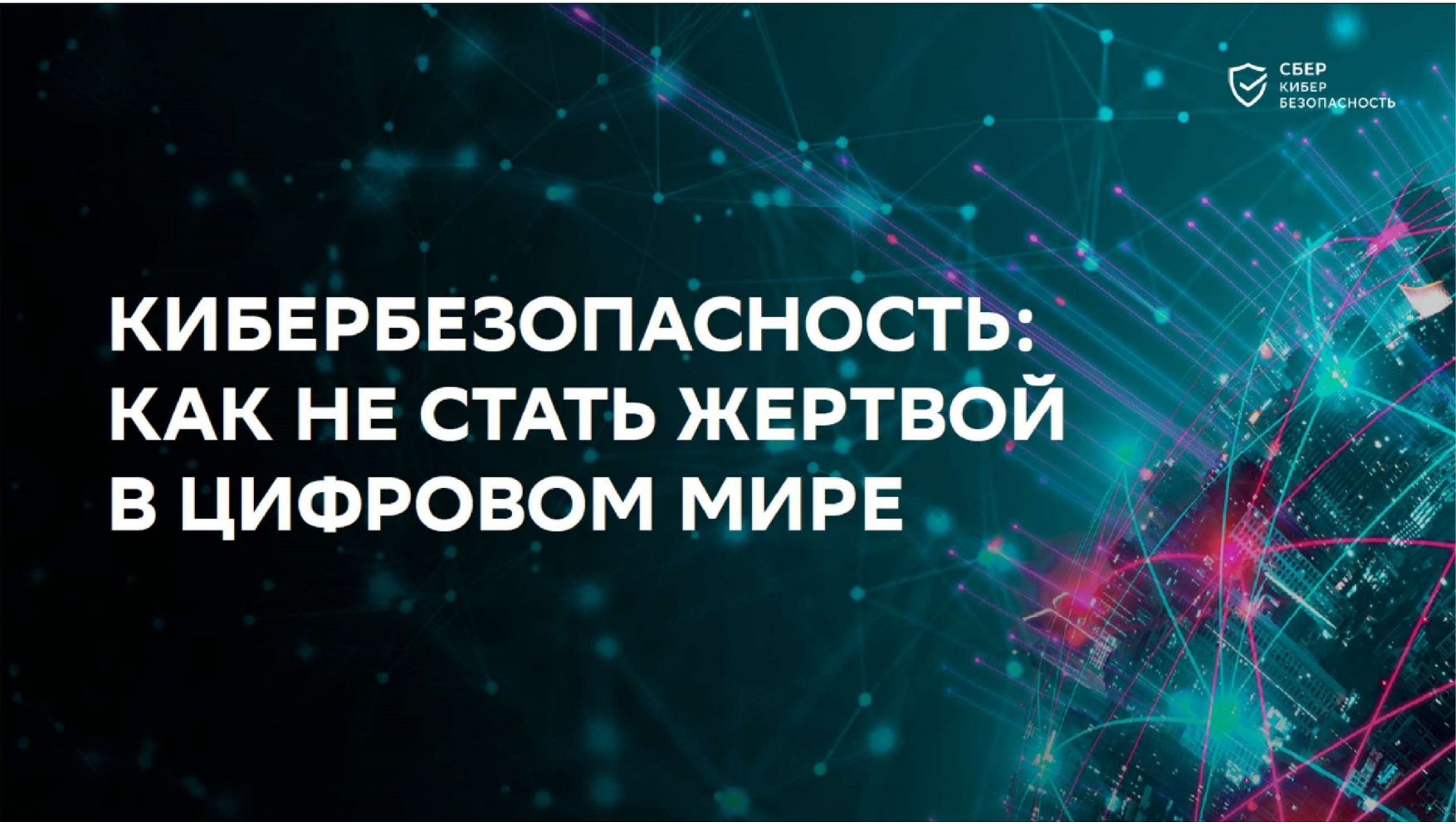

СБЕР
КИБЕР
БЕЗОПАСНОСТЬ
КИБЕРБЕЗОПАСНОСТЬ:
КАК НЕ СТАТЬ ЖЕРТВОЙ
В ЦИФРОВОМ МИРЕ

Что нужно киберпреступникам

СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

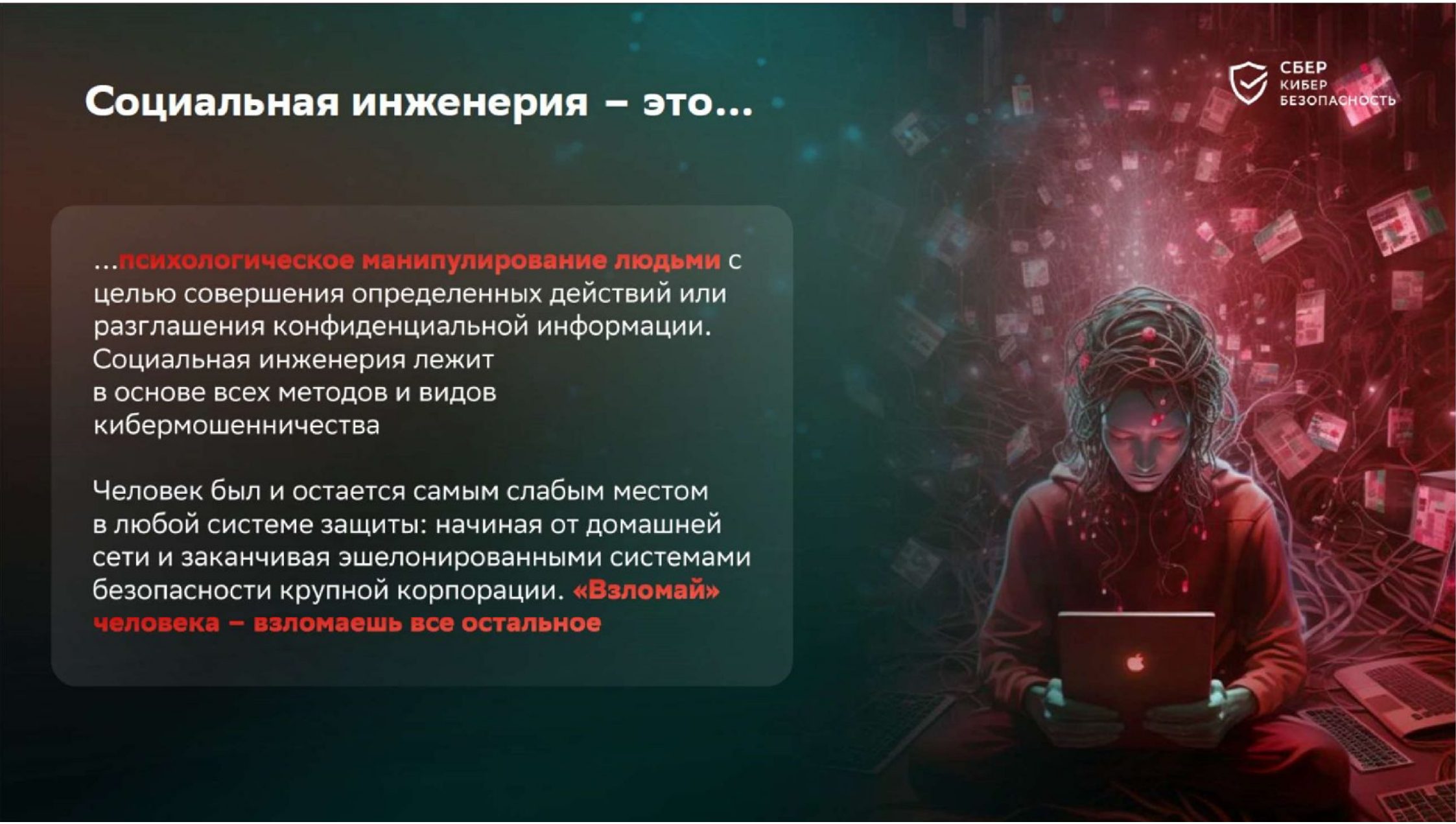
Ваши данные

Ваши деньги

Социальная инженерия – это...

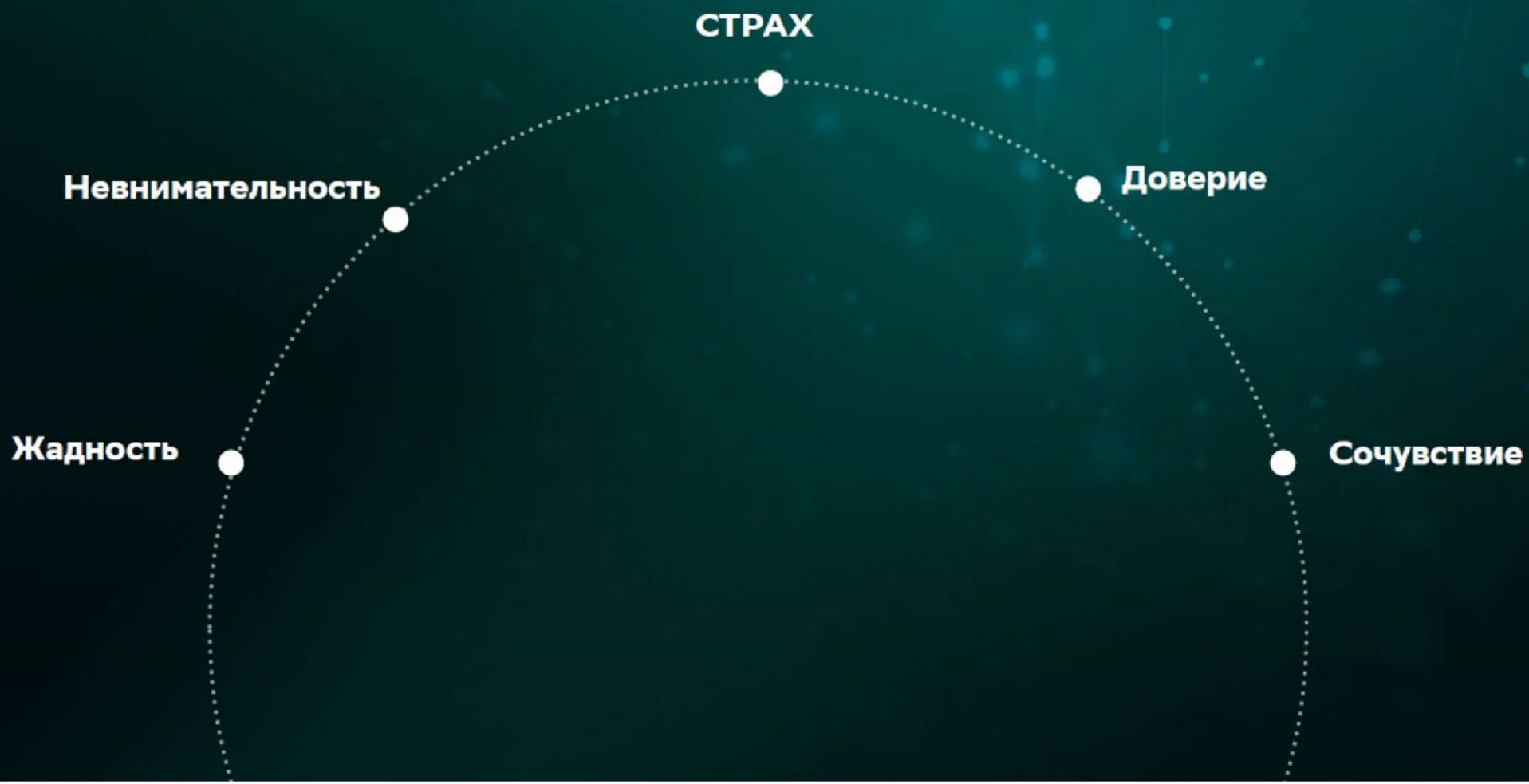
...**психологическое манипулирование людьми** с целью совершения определенных действий или разглашения конфиденциальной информации. Социальная инженерия лежит в основе всех методов и видов кибермошенничества

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**



Злоумышленники используют чувства и эмоции

СБЕР
КИБЕР
БЕЗОПАСНОСТЬ



«У меня зазвонил телефон. Кто говорит?..»

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Служба безопасности

Сотрудник ЦБ

Майор ФСБ

Капитан полиции

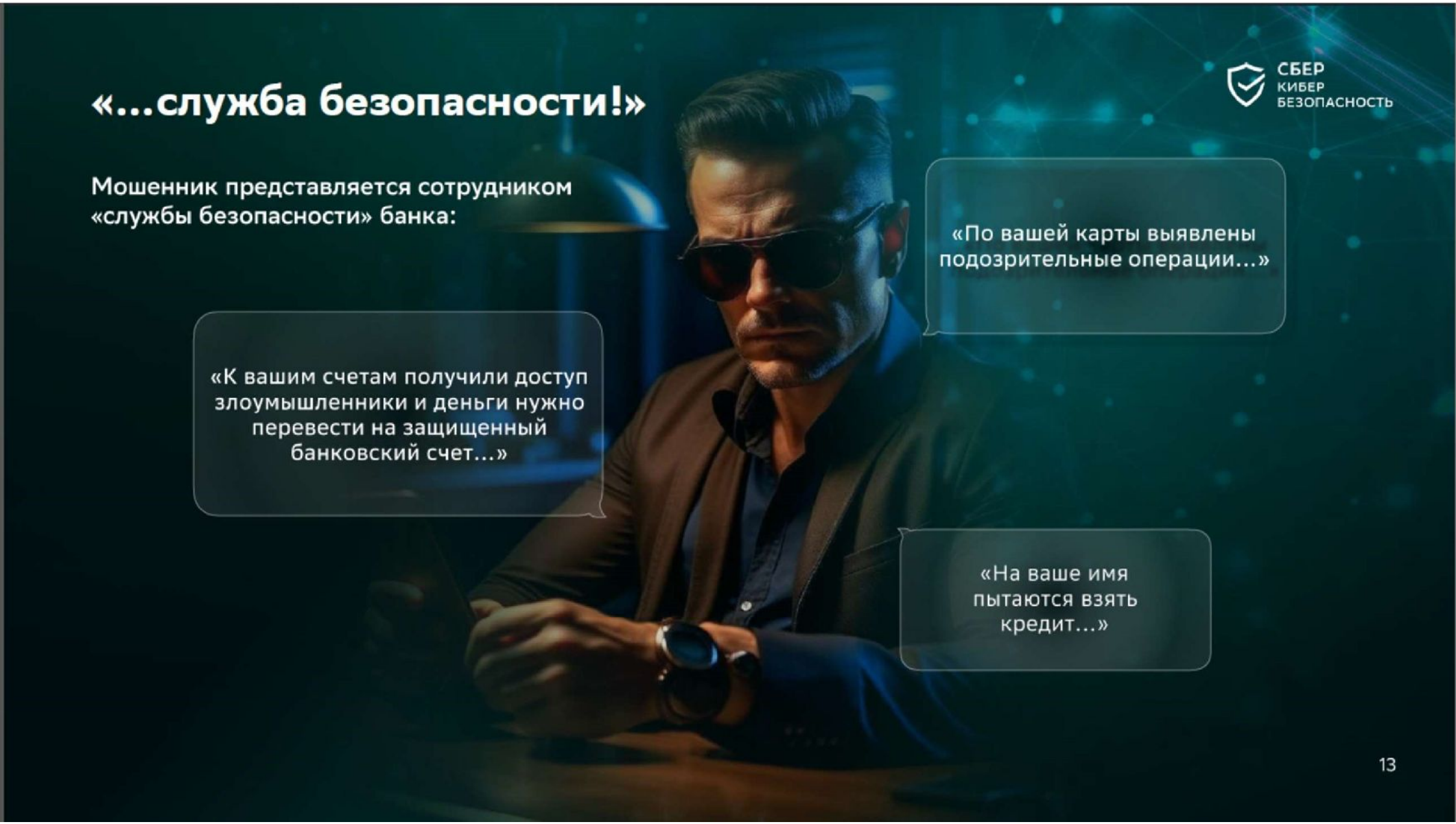
Старший следователь СК

Мама, это я

«...служба безопасности!»

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Мошенник представляется сотрудником «службы безопасности» банка:



«По вашей карты выявлены подозрительные операции...»

«К вашим счетам получили доступ злоумышленники и деньги нужно перевести на защищенный банковский счет...»

«На ваше имя пытаются взять кредит...»

СБЕР

Что важно знать о банковской карте?

Чип

Номер карты

Срок действия

Имя держателя

Магнитная полоса

Код безопасности (CVV/CVC)

Код из СМС

Код для подтверждения операции, который приходит от банка с номера 900

Значок бесконтактной оплаты

Операции по карте можно проводить бесконтактно, просто прикладывая карту к терминалу оплаты/банкомату

Поддельный реестр сотрудников

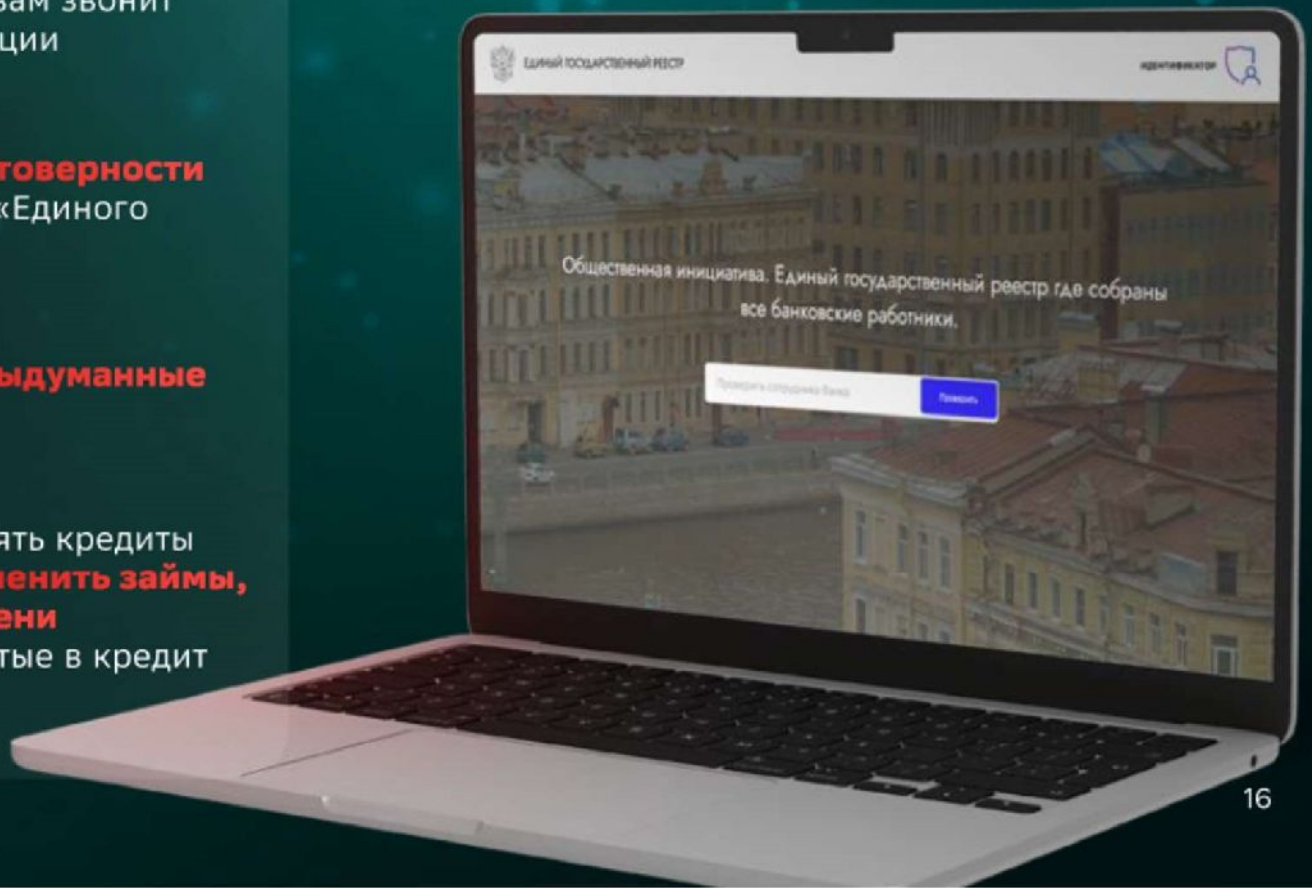
СБЕР КИБЕР БЕЗОПАСНОСТЬ

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»



«Родственник попал в беду или вы?»

СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

Мошенник представляется сыном / внучкой / родственником:

- Все это говорится быстро и с максимально достоверной актерской игрой, чтобы ввести потенциальную жертву в стресс и не дать мыслить рационально
- Злоумышленники отправляют курьера по адресу жертвы, чтобы забрать «деньги», после чего исчезают

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

Что делать, если звонят мошенники

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Внимательно проверяйте входящий номер

Не совершайте никаких операций по инструкциям звонящего

Сразу заканчивайте разговор при любых сомнениях

Проверьте, не было ли сомнительных операций за время разговора

Сотрудники правоохранительных органов **не могут допрашивать по телефону**

ЦБ РФ никогда не звонит физическим лицам

Поставьте приложение для фильтрации входящих вызовов

Фишинг – это...

...**вид мошенничества**, при котором злоумышленники рассылают письма и пытаются обманом заставить получателей совершить какое-то действие:

- перейти по вредоносной ссылке
- загрузить зараженное вложение
- сообщить персональные данные и иную конфиденциальную информацию

С английского «phishing» – созвучно с «fishing» (рыбалка)

Фишинговое письмо — письмо, которое содержит вредоносное вложение или ссылку на мошеннический сайт

Основные признаки фишингового письма

СБЕР КИБЕР БЕЗОПАСНОСТЬ

1

Обращайте внимание на почтовый домен

Мошенники обычно используют общедоступные домены gmail.com, mail.ru и т.п., или домены, похожие на официальные имена компаний (напр. sberbankc[.]ru, 1c-sberbank[.]com и т.д.)

2

Изучите тему. Контент письма и название файлов

Побуждают вас к немедленному действию. Обращайте внимание на грамотность письма

3

Будьте осторожны с вложениями

Открывайте только те, которые ждали. Проверьте расширение вложения.

4

Обращайте внимание на обращение и подпись

Если они являются безличными, или есть признак автоподстановки в обращении, то высока вероятность фишинга

5

Не переходите по ссылкам, не кликайте на подозрительные объекты.

Наведите курсор мыши на подозрительную ссылку/объект и вы увидите, куда она ведёт на самом деле. Сравните её с официальным сайтом компании

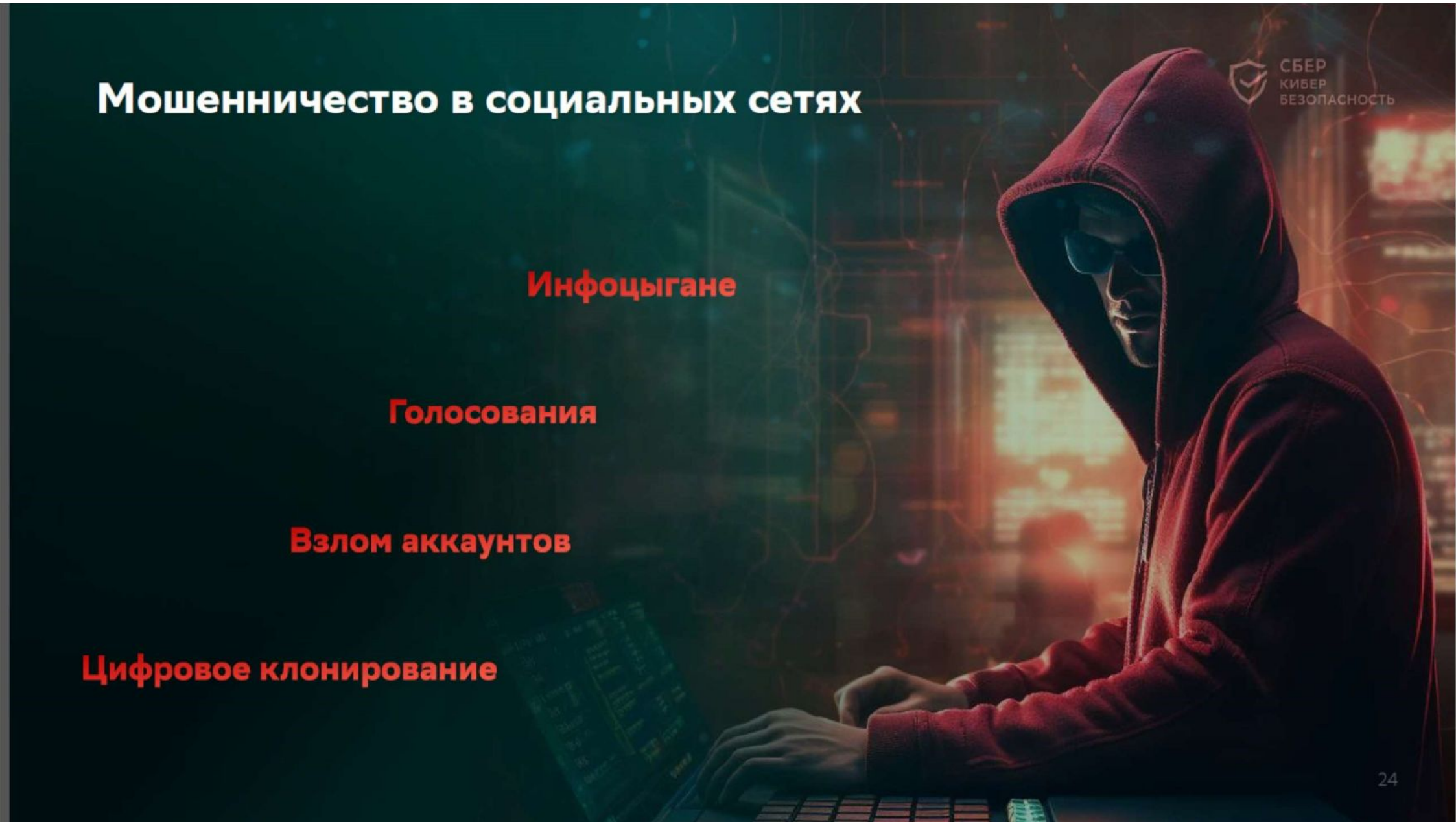
6

Письмо требует ввода данных

(логина, пароля) на подозрительных сайтах или в анкетных формах

5 мм

Мошенничество в социальных сетях



Инфоцыгане

Голосования

Взлом аккаунтов

Цифровое клонирование

Цифровое «клонирование»

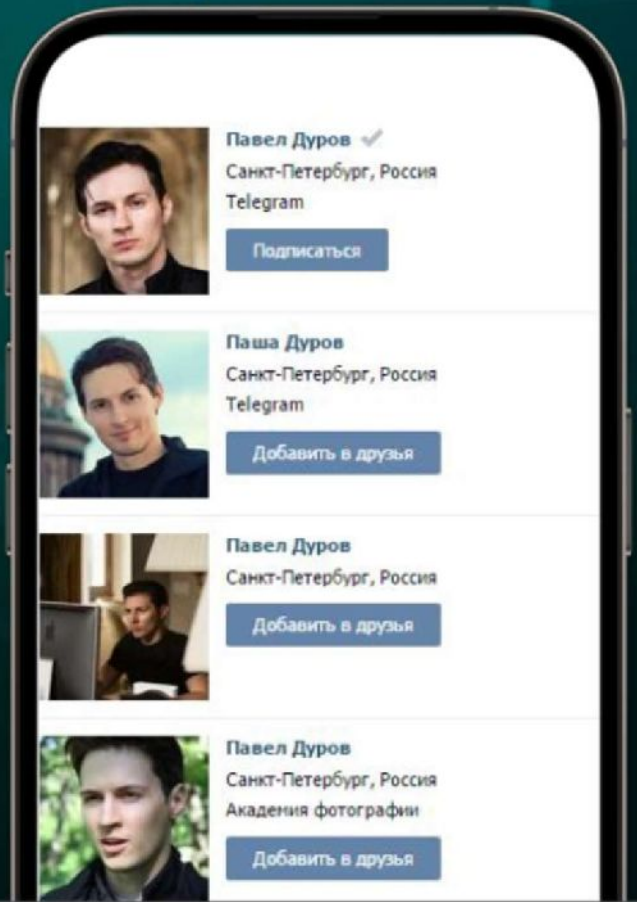
СБЕР КИБЕР БЕЗОПАСНОСТЬ

Кража цифровой личности - незаконное использование чужих персональных данных в социальных сетях для получения личной выгоды. Пользователи сами выкладывают о себе всю необходимую информацию в открытый доступ: ФИО, место жительства и работы, фотографии и т.д. Злоумышленникам остается только создать новый аккаунт и использовать в нем все собранные данные

Писать сообщения родным и знакомым от вашего имени

Используя ваши данные (ФИО, фото) рассылать спам, вымогать деньги, оскорблять, угрожать и совершать иные противоправные действия в интернете

Погубить вашу репутацию или навредить репутации знакомого вам человека

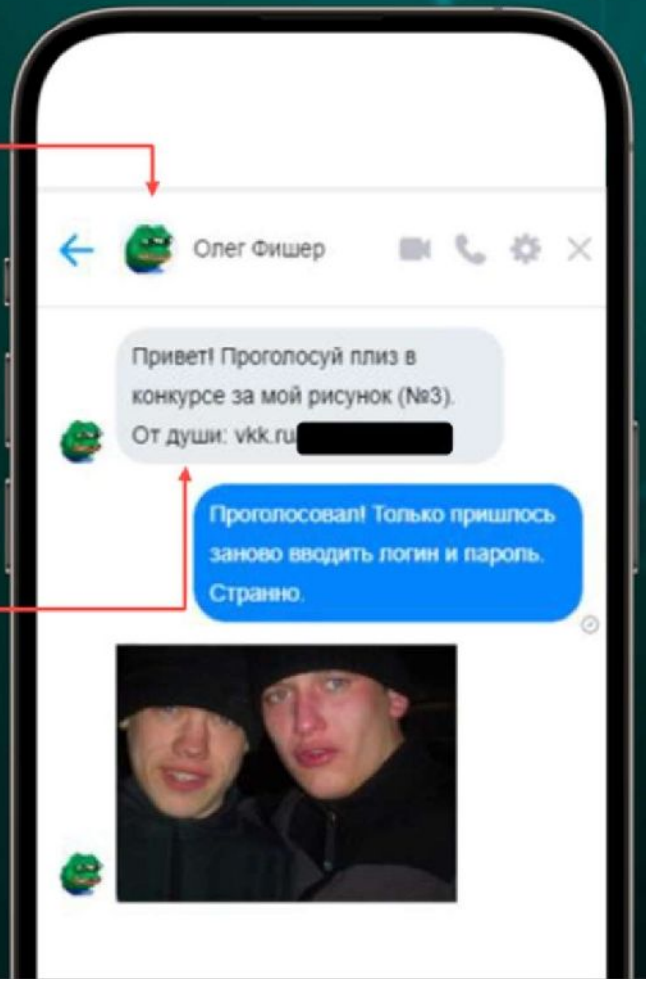


«Голосуй или проиграешь!»

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Неизвестный контакт или ваш знакомый (которого взломали)

Просьба совершить деиствие и ссылка на внешний ресурс



СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

Успешный успех

Инфоцыгане в социальных сетях — это особая категория коучей и бизнес-тренеров, которые обещают научить вас всем своим секретам, благодаря которым вы тут же разбогатеете. Такие курсы, разумеется, платные.

- Вам гарантируют результат
- Человек является супер-экспертом во всех областях сразу
- Основной фокус в рекламе сосредоточен на эмоциях, а не на конкретных знаниях
- Возраст бизнес-тренера
- Навязчивая и «кричащая» реклама курсов и тренингов
- Инфоцыгане не любят заключать договор об обучении

Что делать для защиты в социальных сетях

СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

Установите надежный пароль
Пароль должен состоять из 12 или более знаков, а также содержать строчные и прописные буквы, цифры и символы.

Проверьте настройки конфиденциальности и приватности
Каждая социальная сеть имеет свой набор настроек для усиления безопасности вашей страницы.

Используйте только официальные приложения социальных сетей.

Не указывайте в профиле больше личных данных, чем это нужно.

Включите двухфакторную аутентификацию
Второй фактор защиты вашего аккаунта (одноразовый пароль, биометрические данные) позволяет защитить ваши данные надёжнее, чем только пароль.

Проведите чистку
Удаляйте контакты, с которыми вы давно не поддерживаете связь и не добавляйте незнакомцев.

Не переходите по подозрительным ссылкам в сообщениях и комментариях, даже если они отправлены от ваших друзей.

Ведя переписку с кем-либо убедитесь в том, что адресат – действительно тот, за кого себя выдает.

Что делать, чтобы обезопасить себя в мессенджерах

СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

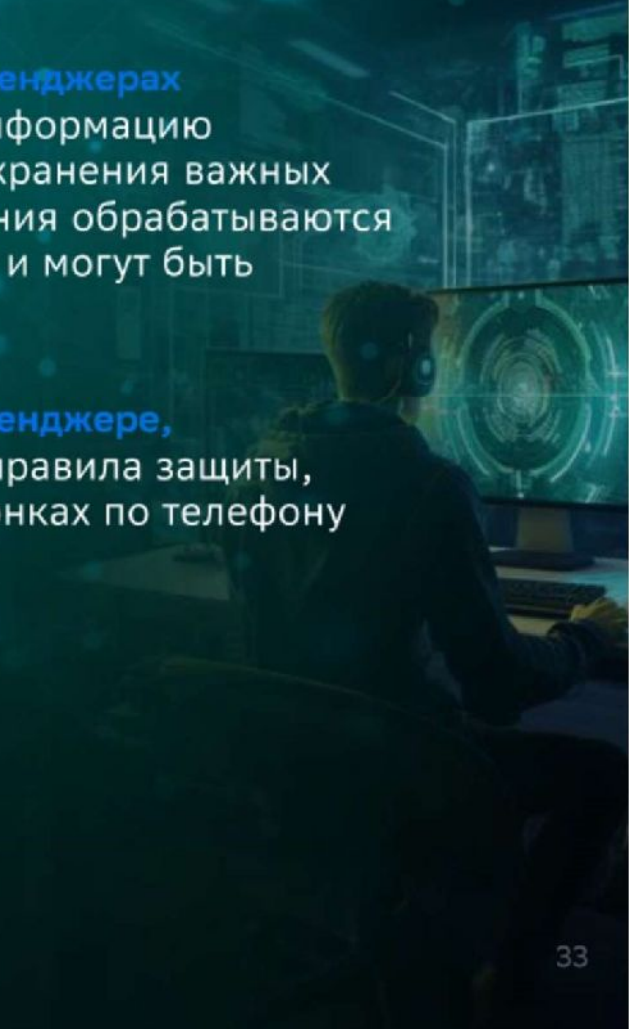
Не переходите по подозрительным ссылкам в сообщениях, даже если они отправлены от ваших друзей. Ваших знакомых могли взломать, а вы рискуете утратить доступ к вашему аккаунту.

Не видитесь на фейковые новости, рассылаемые в мессенджерах. Включайте критическое мышление и не распространяйте сомнительную информацию, если не уверены в ее правдивости.

Не вступайте в переписку с незнакомцами и не принимайте приглашений в неизвестные вам группы.

Не пересылайте в мессенджерах конфиденциальную информацию и не используйте для хранения важных данных. Ваши сообщения обрабатываются на стороннем сервере и могут быть перехвачены.

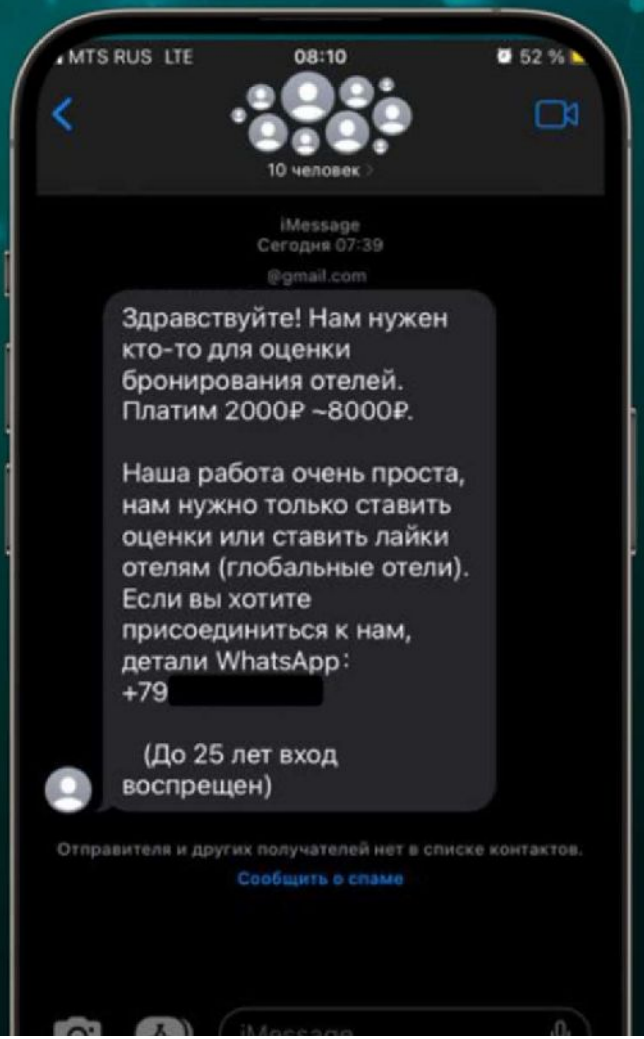
Если вам звонят в мессенджере, то используйте те же правила защиты, что и при обычных звонках по телефону



Как ~~заработать~~ потерять более 15 000₽ за день

СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

1. Злоумышленники создают группу в мессенджерах или отправляют сообщения, в которых предлагают оценивать сервис бронирования отелей / выкупать товары.
2. Пользователю предлагается связаться с персональным «менеджером» для обсуждения «сотрудничества».
3. Злоумышленники отправляют клиенту ссылку на мошеннический сайт, где нужно пройти регистрацию.
4. После регистрации клиенту необходимо внести определённую сумму на указанный счет, чтобы начать выполнять задания по оценке различных отелей или выкупе товаров за низкую цену.
5. В конце каждого «рабочего» дня на счете клиента первоначально «инвестированная» сумма увеличивается.
6. Вывести «заработанные» деньги не получится, а попытки связаться с «менеджером» ни к чему не приведут.



Сервисы кибербезопасности в «СберБанк Онлайн»

СБЕР КИБЕР БЕЗОПАСНОСТЬ

65 млн
пользователей

Сервисы кибербезопасности

- Проверка входящих звонков
- Проверка номера и почты на утечки
- Закрытие доступа к картам и вкладам
- Передача информации о мошеннике в Банк

Повышение киберграмотности клиентов

- Комиксы-статьи и видеоролики об актуальных схемах мошенничества
- Тестирование клиентов на уровень киберграмотности

Продукт на главном экране!

Настройки кибербезопасности

- Управление доступностью продуктов
- Настройка ограничения оплаты в интернете
- Управление доверенными устройствами
- Установка лимитов на снятие наличных
- Изменение суточного лимита
- Настройка способа входа в личный кабинет СБОЛ
- Проверка операций близкого