СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

КИБЕРБЕЗОПАСНОСТЬ: КАК НЕ СТАТЬ ЖЕРТВОЙ В ЦИФРОВОМ МИРЕ

Содержание

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Киберпреступность сегодня

СБЕР КИБЕР БЕЗОПАСНОСТЬ

>577 тыс.

преступлений в сфере ИТ
за 1 полугодие в 2024

для сравнения: >677 тыс. в 2023[1]

44%

доля преступлений в ИТ от общего числа преступлений в 2024

для сравнения: 35% в 2023[2]

[1] Источник: МВД

Киберпреступность сегодня

СБЕР КИБЕР БЕЗОПАСНОСТЬ

91%

граждан России хотя бы раз сталкивались с мошенничеством в 2023

для сравнения: 82% в 2022[2]

59,8 тыс.

вредоносных фишинговых доменов было заблокировано в 2024[3]

[2] Источник: НАФИ, Ингосстрах

[3] Источник: Минцифры

Что нужно киберпреступникам

СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

Ваши данные

Ваши деньги

СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Социальная инженерия – это...

СБЕР КИБЕР БЕЗОПАСНОСТЬ

...**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**

Угрозы конфиденциальности

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Любое действие в сети оставляет цифровой след

Цифровой след

- Регистрация на сайтах
- Лайки в соцсетях
- Посты и репосты
- Комментарии к постам
- Фото и видео

Цифровой портрет

Кнопки Delete в Интернете нет

Что о вас могут знать мошенники

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Интернет-магазины
- Покупки
- Платёжная информация

Социальные сети
- Родственники, друзья и знакомые
- Образование
- Хобби
- Политические и религиозные убеждения
- Места пребывания

Службы доставки
- Место жительства
- Место работы

Билеты
- Данные о перелетах, поездках, попутчиках

Государственные услуги
- Паспорт и другие документы
- Состав семьи
- Имущество
- Социальные и медицинские услуги

Такси, каршеринг
- Время, маршруты и адреса поездок

Злоумышленники используют...

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Страх

Неосведомленность

Невнимательность

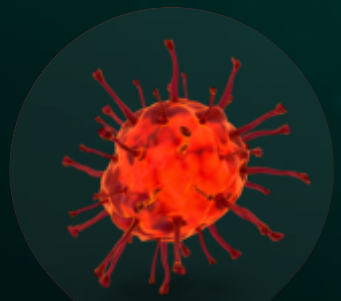
Доверие

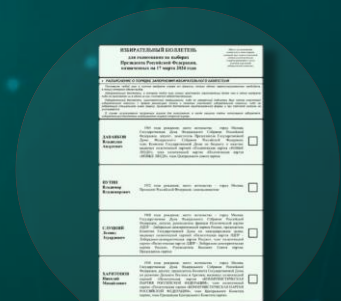
Жадность

Сочувствие

Использование новостной повестки

СБЕР КИБЕР БЕЗОПАСНОСТЬ





2020-2021

- COVID-19
- Вакцинация

2022-2023

- СВО
- Мобилизация

2024-...

- Политическая повестка
- Sim-карты

Злоумышленники всегда эксплуатируют наиболее «горячие» темы

СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Используемые «скрипты»

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Продление договора по sim-карте

Обновление полиса ОМС

Перерасчет пенсии или трудового стажа

Капитан ФСБ

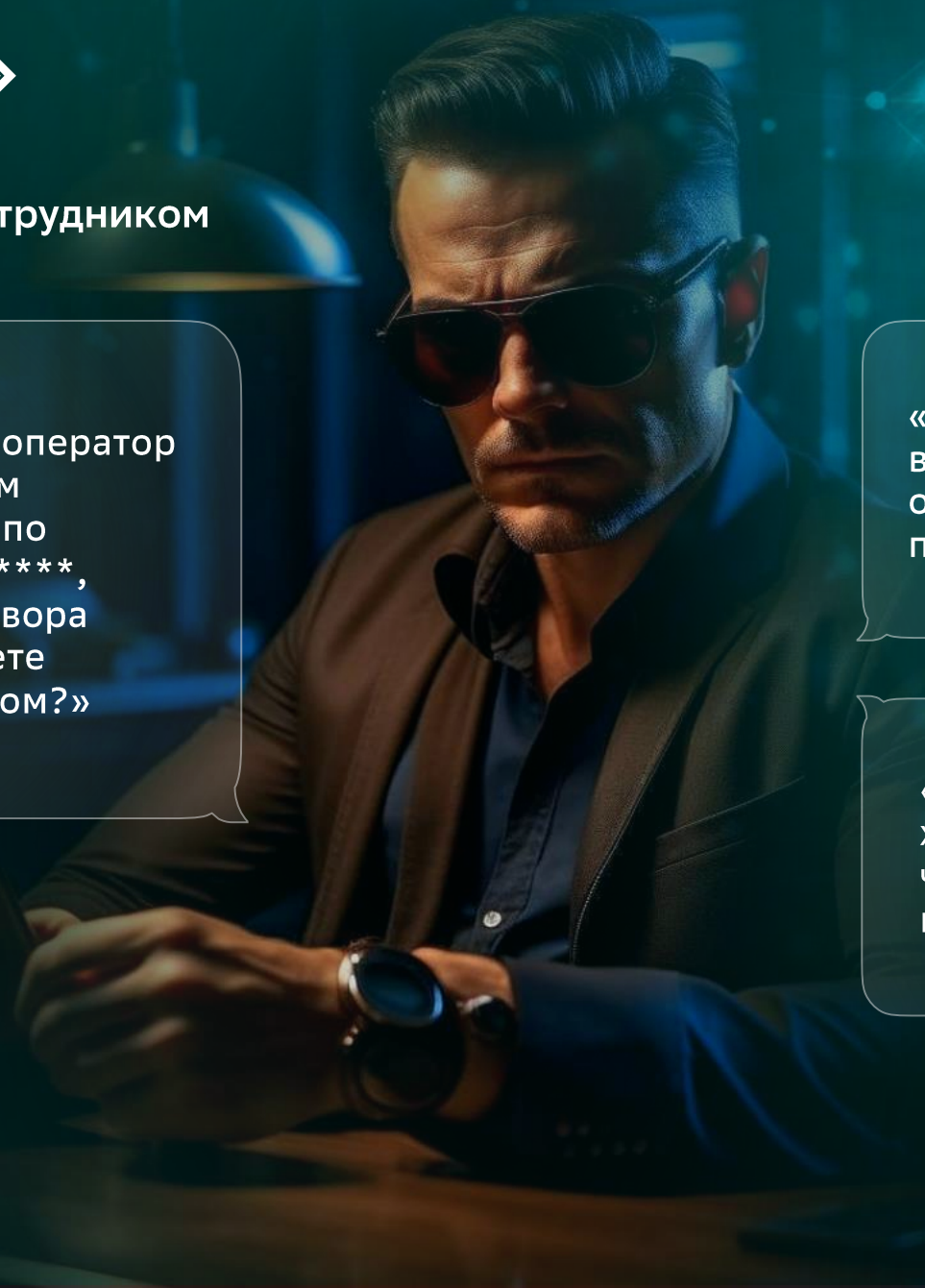
Сотрудник ЦБ

«Госуслуги»

«Здравствуйте...»

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Мошенник представляется сотрудником различных организаций:



«Вас приветствует мобильный оператор «МТС», меня зовут..., проводим продление действия договора по вашему номеру с окончанием ****, напоминаю, что действие договора истекает сегодня, вы планируете пользоваться данным телефоном?»

«Беспокоят из поликлиники, ваш полис ОМС обновлён, каким образом будете его получать: по почте или в электронном виде?»

«Это Социальный фонд, в ходе проверки выяснилось, что вам неправильно посчитали трудовой стаж...»

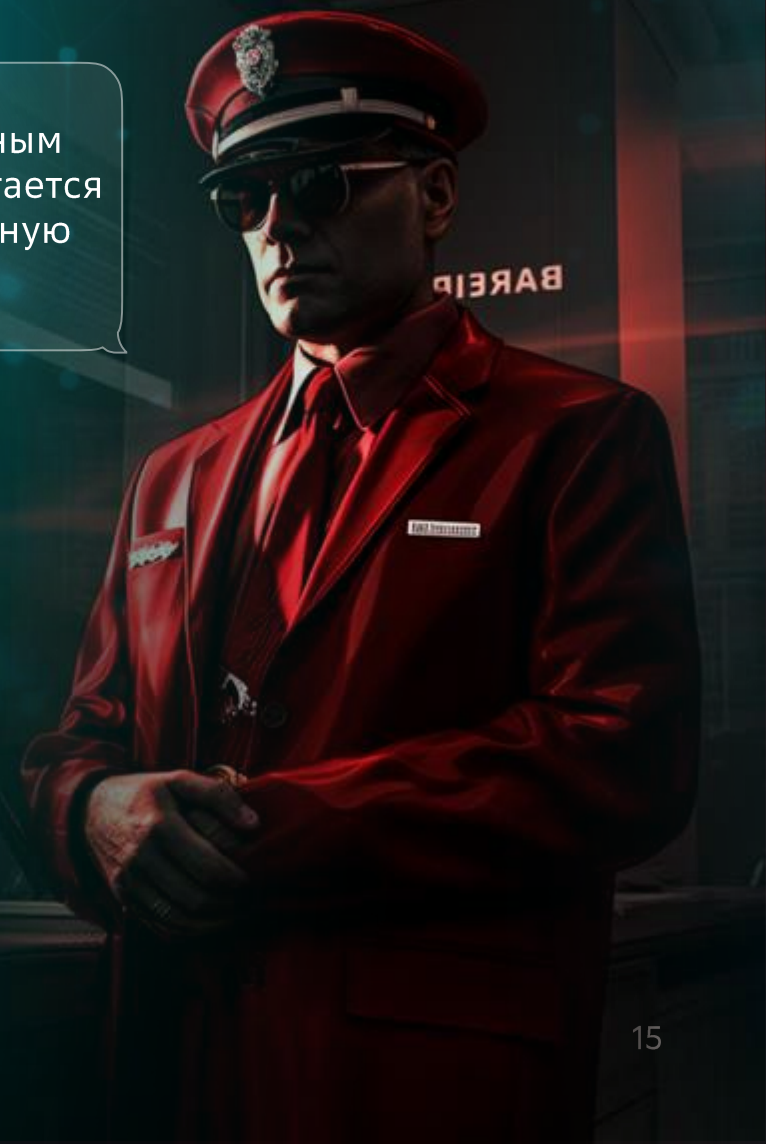
Когда звонит «товарищ майор»

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Мошенник представляется сотрудником МВД / СК / ФСБ:

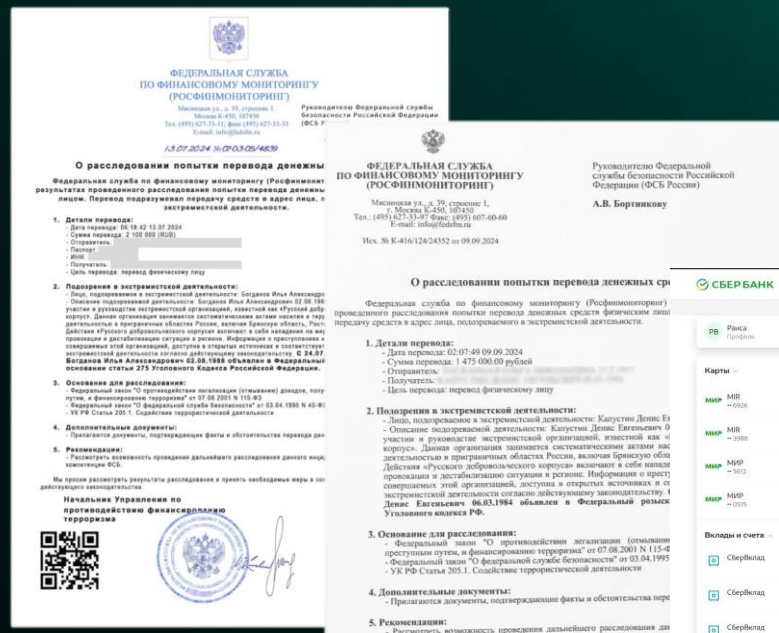
- Злоумышленник предлагает решить проблему:
  - Вывести все деньги с банковских карт жертвы и перевести их на «безопасный» счет.
  - Исчерпать лимит кредитов по карте и перевести их на «безопасный» счет.
- Часто в схеме участвует не один человек

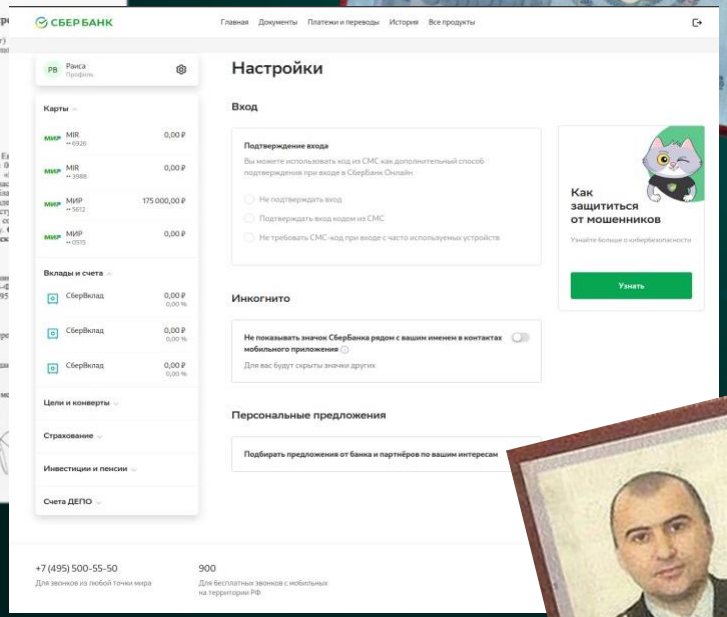
«По вашим поддельным документам кто-то пытается взять кредит на крупную сумму...»



«Можете проверить...»

СБЕР КИБЕР БЕЗОПАСНОСТЬ





Что делать, если звонят мошенники

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Внимательно проверяйте входящий номер

Не совершайте никаких операций по инструкциям звонящего

Сразу заканчивайте разговор и блокируйте номер при любых сомнениях

Проверьте, не было ли сомнительных операций за время разговора

Не отвечайте на подозрительные вызовы в мессенджерах

Сотрудники правоохранительных органов **не могут допрашивать по телефону. Любые следственные действия проводятся очно в отделе**

ЦБ РФ никогда не звонит физическим лицам

Поставьте приложение для фильтрации входящих вызовов

СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

ФИШИНГ

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

СБЕР КИБЕР БЕЗОПАСНОСТЬ

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

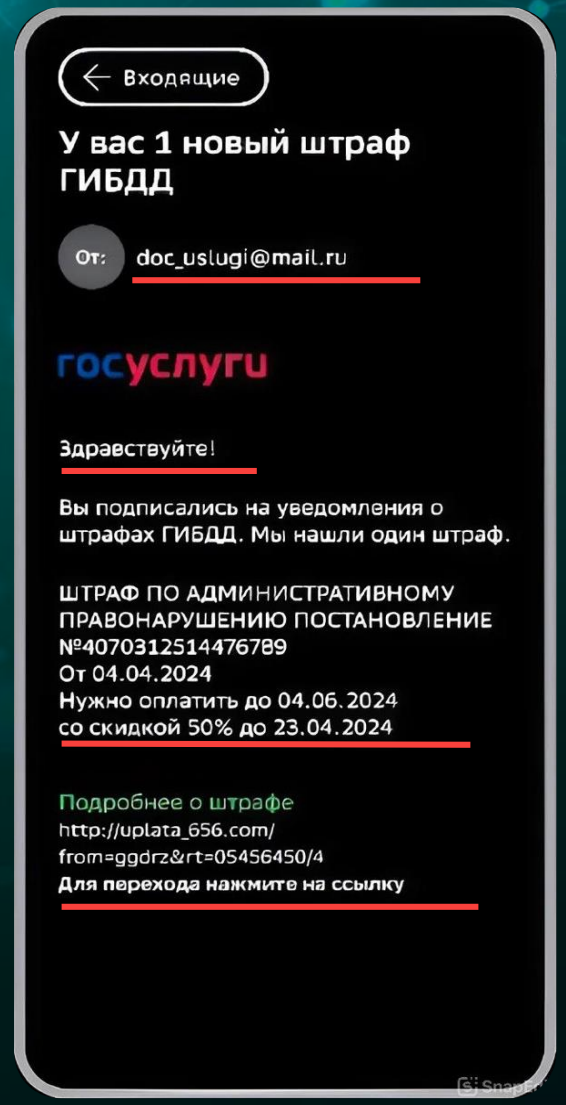
Не переходите по ссылкам, не кликайте на подозрительные объекты.

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



Какие уловки используют мошенники в письмах

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Службы доставки

Горячие новости

Подписки и онлайн-сервисы

Криптовалюта

Маркетплейсы

Туроператоры и отдых

Лотерии

Билеты на мероприятия

Дополнительный заработок и инвестиции

Что делать, если есть подозрение на фишинг

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Не переходите по ссылкам,
не кликайте на подозрительные объекты.

Не перенаправляйте письмо
другим сотрудникам

Не вводите свои данные
и не отвечайте
на подозрительные письма

Перешлите письмо в службу КБ
своего учреждения

Не открывайте
вложения

СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

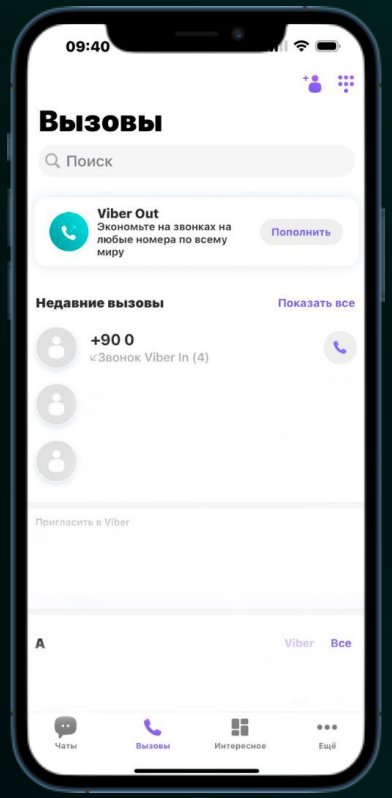
УГРОЗЫ В МЕССЕНДЖЕРАХ И СОЦИАЛЬНЫХ СЕТЯХ

Мошенничество с использованием мессенджеров

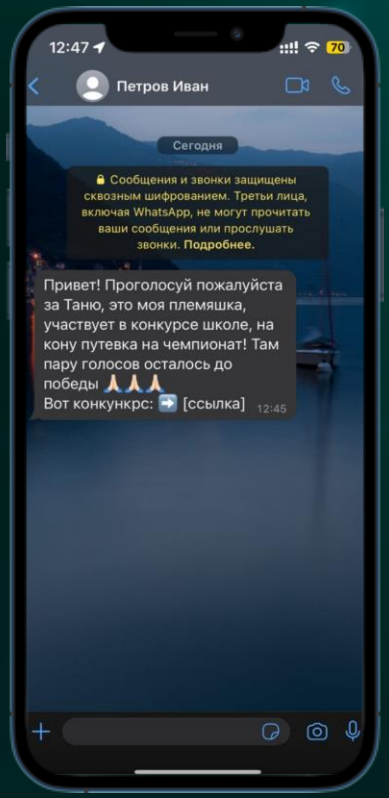
СБЕР КИБЕР БЕЗОПАСНОСТЬ

Злоумышленники стали активно использовать мессенджеры для социальной инженерии

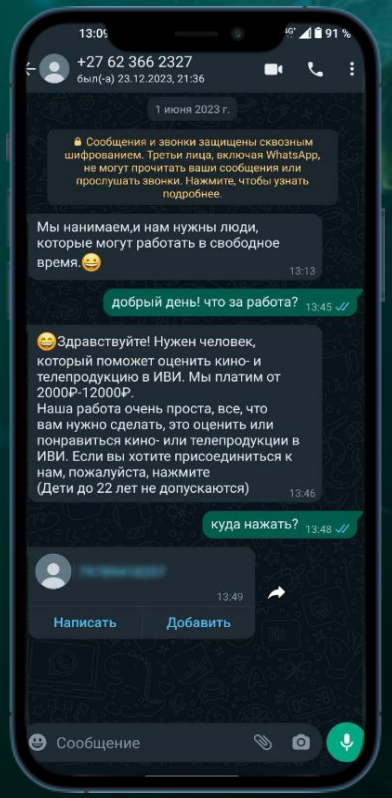
Звонок с «+900», «+90 0» и подобных



Предложение проголосовать за родственника



Предложение о работе



Причины использования мессенджеров мошенниками

Сложность определения мошенников

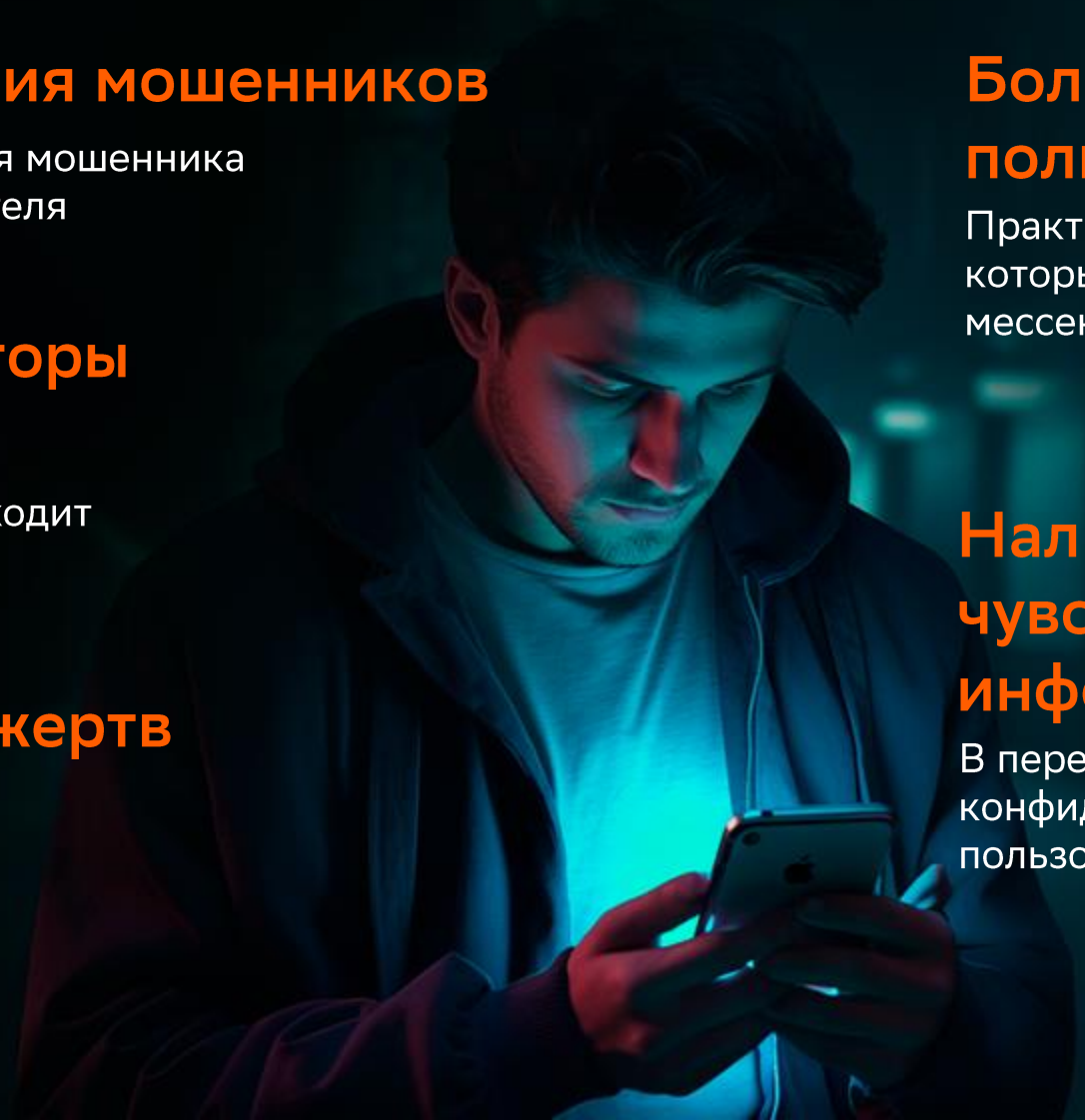
Человеку сложно отличить действия мошенника от действий легитимного пользователя

Дополнительные факторы доверия

Как правило мошенничество происходит от имени лица, которого вы знаете

Неподготовленность жертв

Это новое явление с которым еще не все знакомы



Большой охват пользователей

Практически не осталось людей, которые не используют мессенджеры для общения

Наличие чувствительной информации

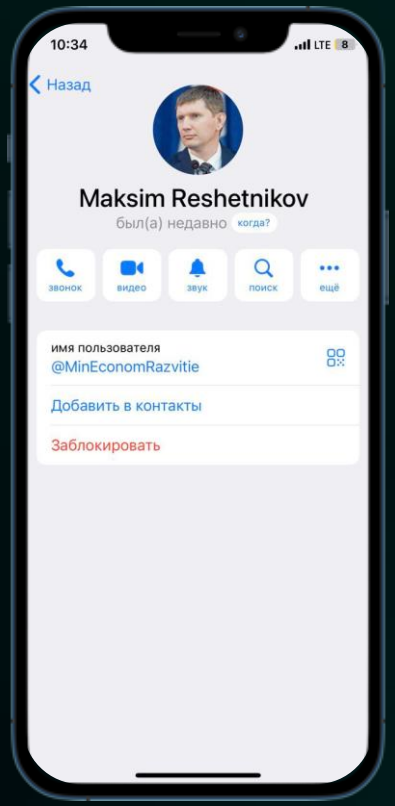
В переписке могут хранится конфиденциальные данные пользователей

Мошенники маскируются под руководство организации

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Создание профиля

Мошенники создают профиль от лица «руководителя организации»

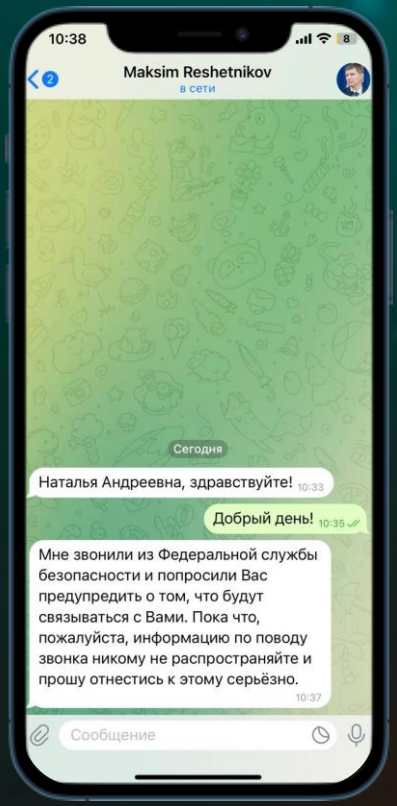


Контакт мошенников с жертвой

Мошенники связываются с вами от лица «руководителя»

Манипуляции мошенников

«С вами свяжутся, никому не сообщайте о нашем разговоре»



Мошеннический звонок

Сотрудник «ФСБ» в ходе телефонного разговора сообщает вам о необходимости перевести ваши ДС на «безопасный счет»

Мошенничество в мессенджерах/социальных сетях

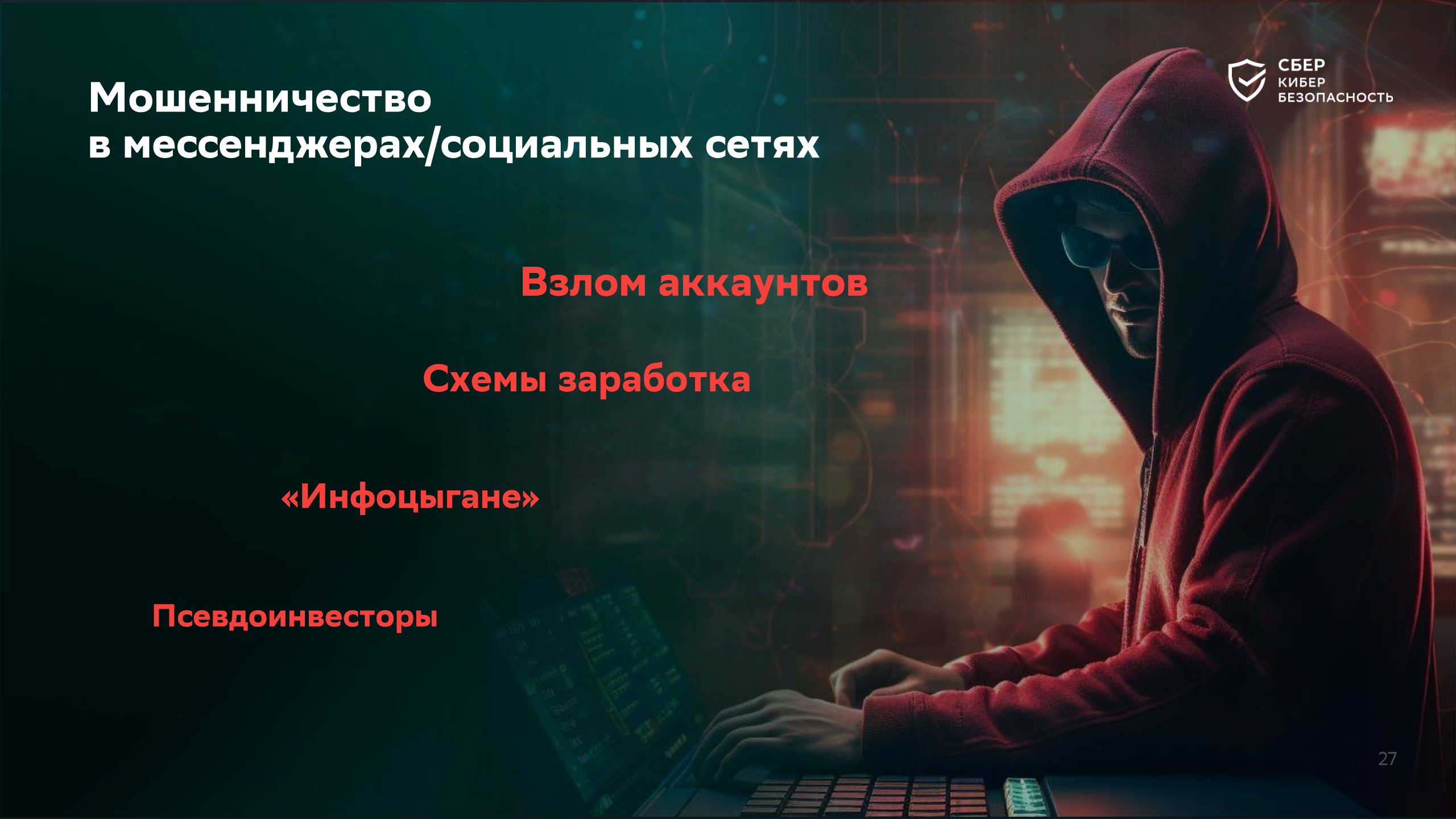
СБЕР КИБЕР БЕЗОПАСНОСТЬ

Взлом аккаунтов

Схемы заработка

«Инфоцыгане»

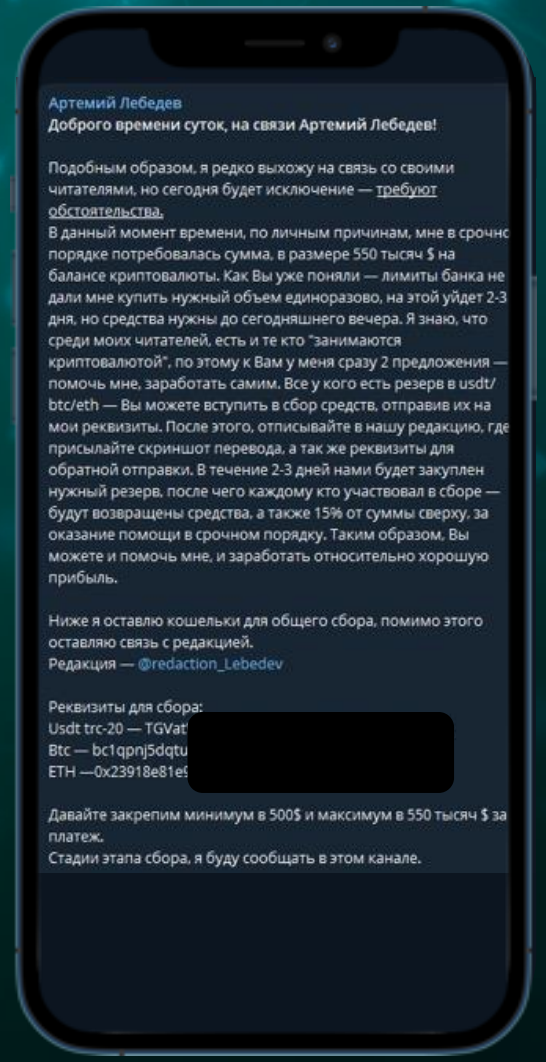
Псевдоинвесторы



Взлом аккаунтов в мессенджерах/социальных сетях

СБЕР КИБЕР БЕЗОПАСНОСТЬ

- Схемы мошенничества для мессенджеров актуальны и для социальных сетей
- Злоумышленники могут взломать аккаунты владельцев различных групп и каналов
- Взломав учетную запись владельца популярного канала, злоумышленники размещают сообщение о «срочном» сборе средств на благотворительность, помощь и т.д. от имени владельца
- Ничего не подозревающая аудитория канала переводит на карту / криптокошелек мошенника денежные средства

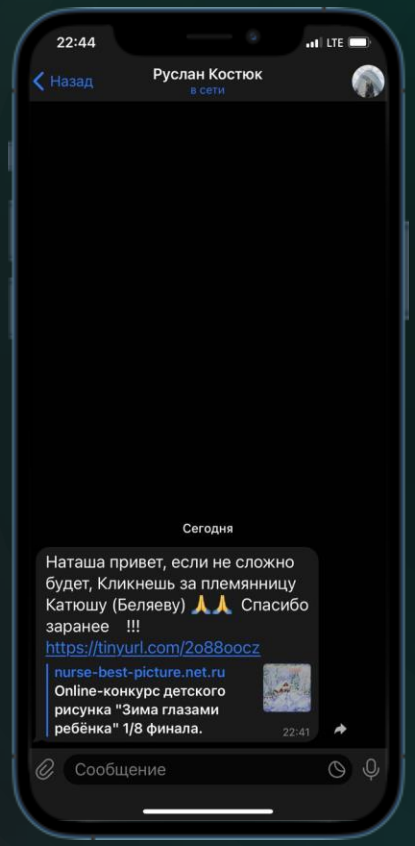


«Привет, проголосуй пожалуйста за мою племянницу!»

СБЕР КИБЕР БЕЗОПАСНОСТЬ

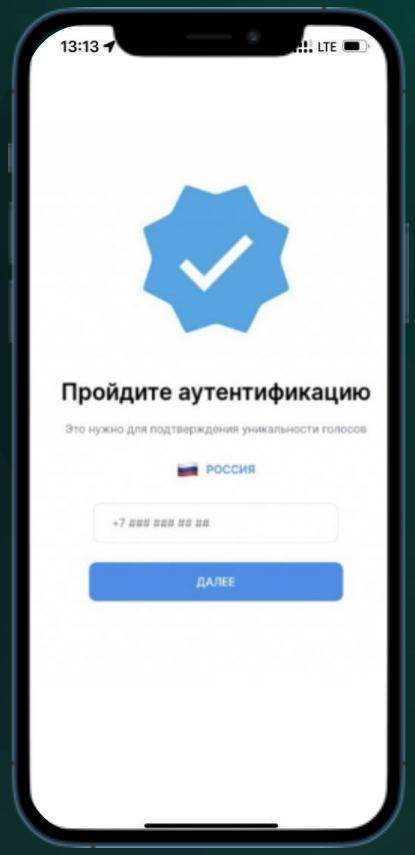
Первоначальная рассылка

- Мошенники присылают сообщение с фишинговой ссылкой



Взлом аккаунта

- Переходя по фишинговой ссылке вы передаете данные от своего аккаунта мошенникам

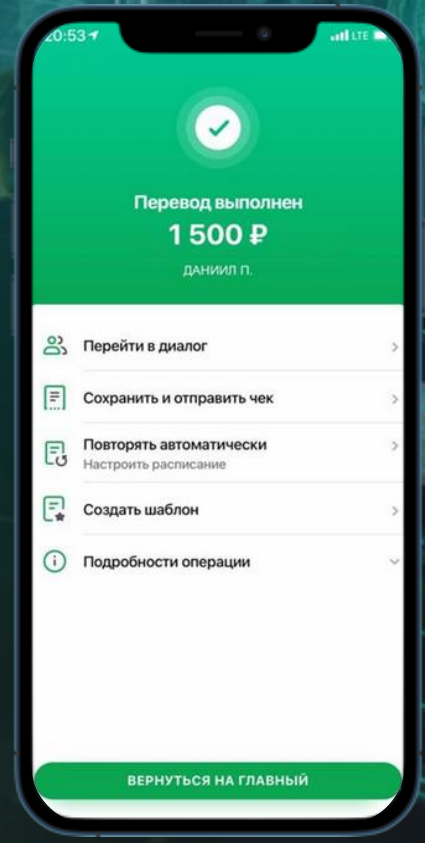


«Займи пожалуйста»

- Получив доступ, мошенники осуществляют рассылку вашим контактам с просьбой «занять небольшую сумму»

Перевод денежных средств мошенникам

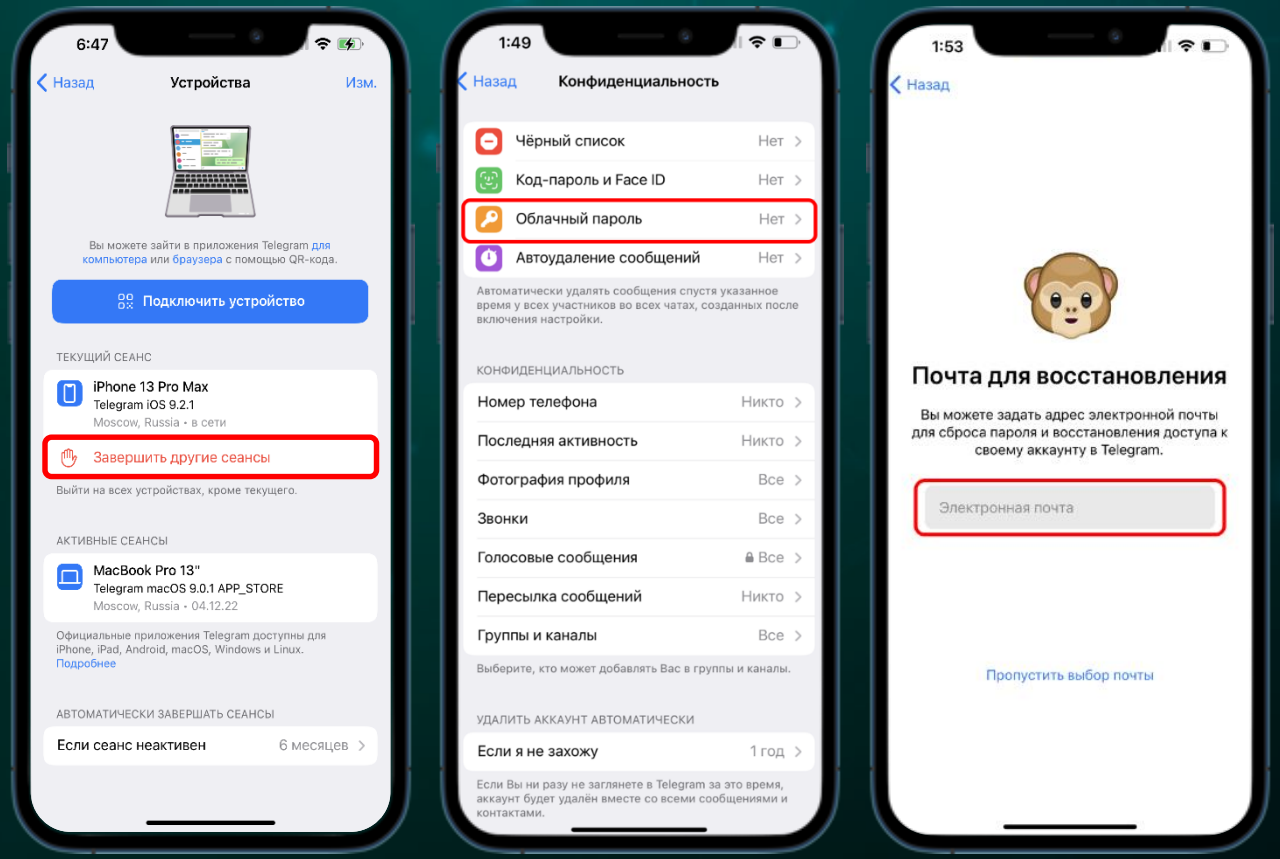
- Ваши знакомые переводят денежные средства мошенникам!



Рекомендуемые настройки безопасности в мессенджерах и социальных сетях

СБЕР КИБЕР БЕЗОПАСНОСТЬ

- **Проверьте активные сеансы на вашем устройстве**
  если вы заметили что в активных сеансах мессенджера присутствуют не ваши устройства, завершите эти сеансы
- **Установите двухфакторную аутентификацию в (SMS-подтверждение, облачный пароль, двухшаговая проверка, pin-код)**
  злоумышленники не смогут попасть в ваш аккаунт, даже если вы сообщите им код из SMS или PUSH-уведомления
- **Свяжите учетную запись с электронной почтой**
  у вас появится дополнительная возможность восстановления доступа к аккаунту



Как быстро ~~заработать~~ потерять деньги

СБЕР КИБЕР БЕЗОПАСНОСТЬ

1. Злоумышленники создают группу в мессенджерах или отправляют сообщения, в которых предлагают за несколько минут выполнить простую работу и заработать хорошую сумму денег.

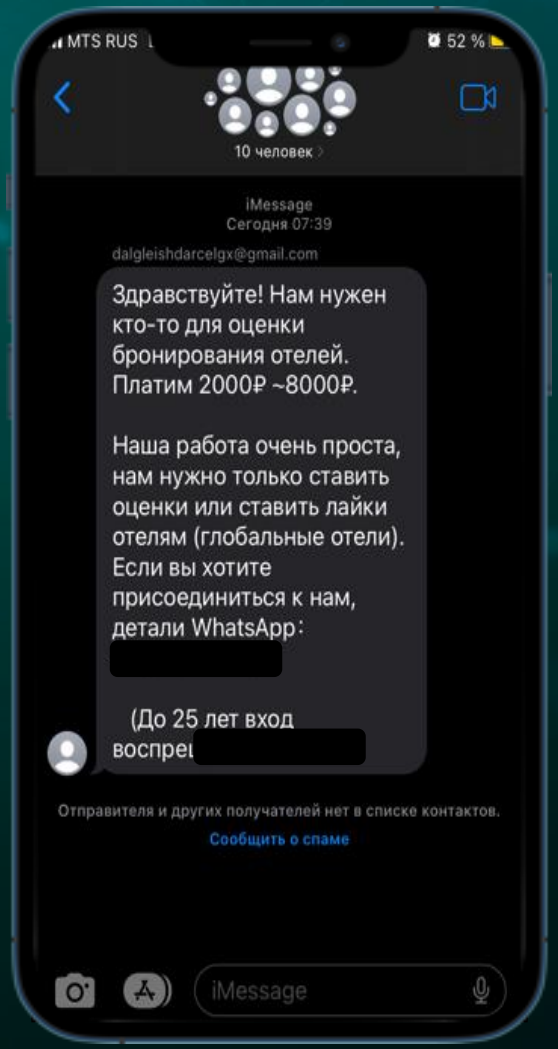
2. Пользователю предлагается связаться с персональным «менеджером» для обсуждения «сотрудничества».

3. Злоумышленники отправляют клиенту ссылку на мошеннический сайт, где нужно пройти регистрацию для выполнения работы.

4. После регистрации клиенту необходимо внести определённую сумму на указанный счет, чтобы подтвердить учетную запись или купить «подписку».

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.



Успешный успех

Инфоцыгане в мессенджерах/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

Псевдоинвесторы/брокеры – это...

...**мошенники, которые выдают себя за профессиональных участников фондового рынка или криптоинвесторов.** Они регулярно предлагают клиентам брокерские, дилерские и инвестиционные услуги с помощью которых якобы можно преумножить свой капитал.

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Как действуют псевдоинвесторы/брокеры

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Псевдоинвесторы/брокеры представляются сотрудниками крупных брокерских компаний и предлагают вложиться в очень прибыльный проект, который «гарантированно принесёт большие дивиденды»

Мошенники призывают «инвесторов» зачислять настолько большие суммы, насколько это возможно

Будущим «инвесторам» обещают внушительный доход

Если жертва захочет вывести деньги, этого не дадут это сделать по различным вымышленным причинам

Псевдоинвесторы/брокеры заманивают человека на поддельный инвестиционный сайт. Дизайн сайта может полностью повторять облик сайта известной компании. Затем убеждают создать свой личный кабинет, ввести персональные данные и пополнить «брокерский счет»

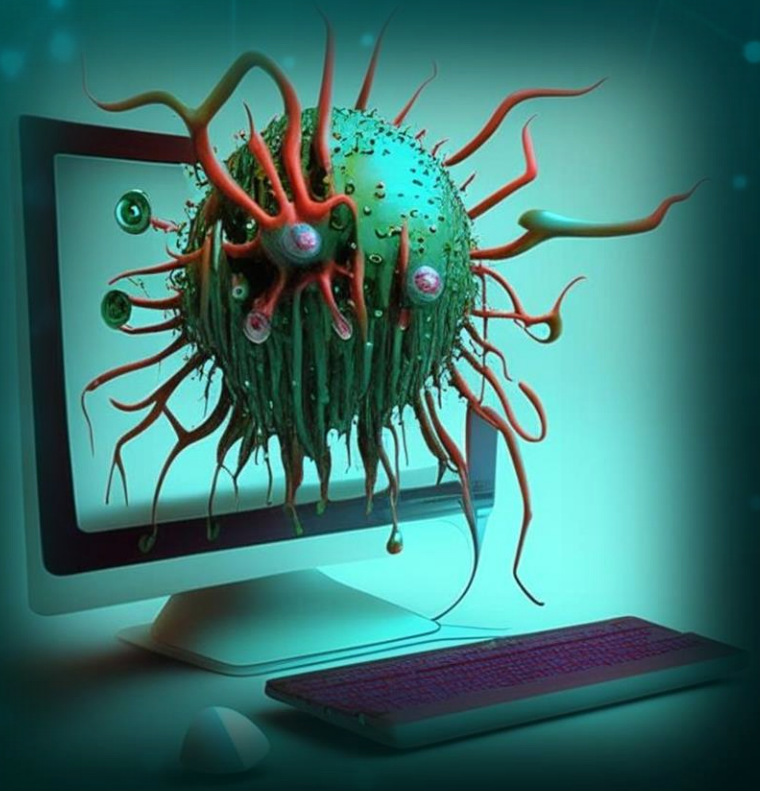
Как обезопасить себя от псевдоинвесторов/брокеров

- Убедитесь, что у вас достаточно знаний о том, как устроен фондовый рынок
- Изучите отзывы о брокерской компании и её первых лицах в интернете
- Проверьте брокера на сайте Банка России
- Внимательно изучите договор, который вам предлагают заключить
- Для пополнения настоящего брокерского счёта не нужно переводить деньги по номеру карты или телефона, реквизитам счета (в сообщениях) или электронным кошелькам

Распространение вредоносного ПО в мессенджерах

СБЕР КИБЕР БЕЗОПАСНОСТЬ

- Для заражения Android-устройства злоумышленники распространяют файлы с расширением .apk. Достаточно открыть его и запустить, чтобы началась распаковка и установка приложения на мобильное устройство.
- Киберграмотность населения растёт, вследствие чего злоумышленникам сложнее попасть в круг доверия потенциальной жертвы. Они постоянно придумывают новые способы заставить человека установить вредоносное приложение.



Основные схемы распространения вредоносного ПО в мессенджерах

СБЕР КИБЕР БЕЗОПАСНОСТЬ

1 **Схема 1. Подарок подписки «Telegram Premium»**

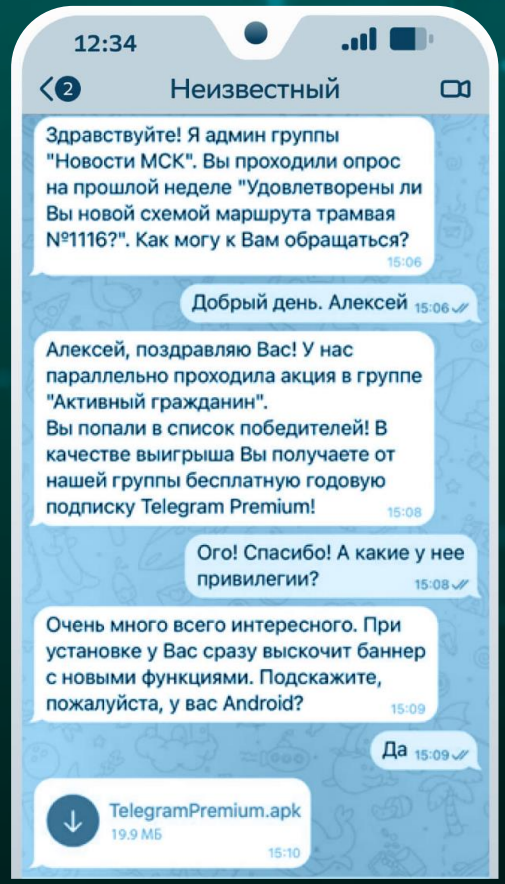
Мошенники рассылают вредоносное ПО под видом подписки Telegram Premium.

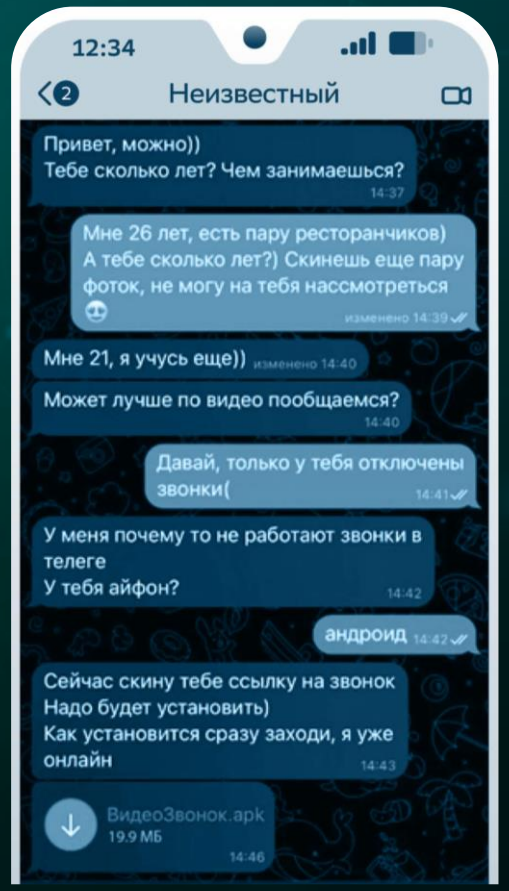
Важно: Подписка не является приложением. Устанавливать ее не надо.

2 **Схема 2. Знакомства**

Мошенники рассылают вредоносное ПО под видом видеозвонка/приложений для звонков/фото-архивов

Важно: Для звонков не нужно устанавливать отдельные приложения. Архивы с фотографиями не могут иметь расширение .apk.





СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

КАК ЗАЩИТИТЬ СЕБЯ

Обновления ОС и приложений

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Важный процесс, необходимый для обеспечения безопасности, стабильности и надежности.

Своевременные обновления позволяют исправлять уязвимости, улучшать производительность, получать новые функции и исправление ошибок в работе устройства.

Базовые правила

СБЕР КИБЕР БЕЗОПАСНОСТЬ

- Создавайте надежные и уникальные пароли для всех ресурсов
- Настройте двухфакторную аутентификацию везде, где это возможно
- Настройте резервные адреса и телефоны для восстановления доступа
- Анализируйте авторизованные сессии
- Не устанавливайте подозрительные приложения из непроверенных источников
- Не переходите по подозрительным ссылкам
- Повышайте свой уровень киберграмотности и держите руку на пульсе

Не забывайте:

Сотрудники «Службы безопасности», МВД, ФСБ России, Центрального Банка никогда не будет звонить вам через мессенджеры

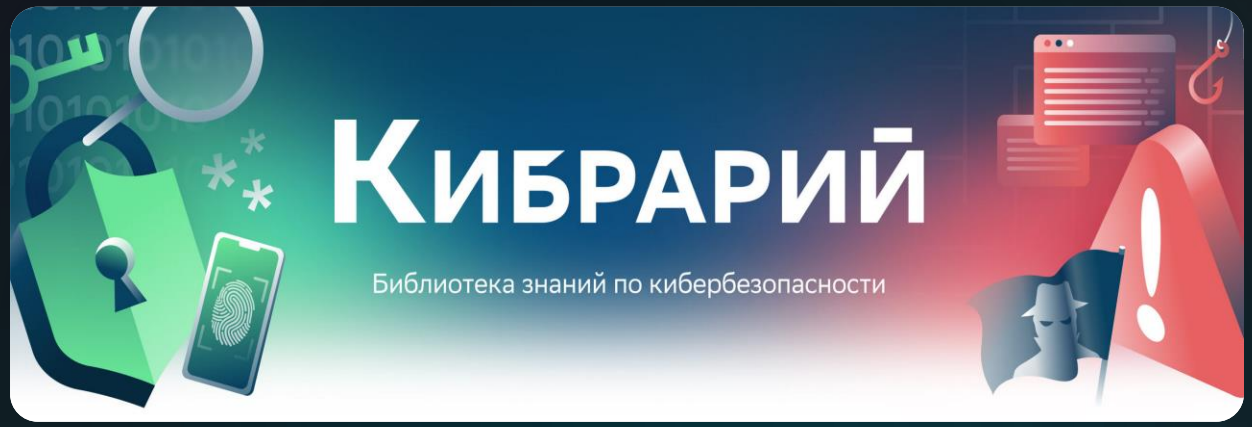
Как обезопасить не только себя, но и своих близких

СБЕР КИБЕР БЕЗОПАСНОСТЬ

Рекомендации:

- Если вы сомневаетесь в своих действиях, возьмите паузу, соберите как можно больше информации из проверенных источников и всё тщательно взвесьте
- Если вам кажется что с вами общается не ваш коллега, а мошенник, просто позвоните ему на рабочий телефон
- Если ваш аккаунт или аккаунт близкого человека все таки взломали, немедленно сообщите ему об этом по телефону
- Рассказывайте об известных случаях мошенничества своим близким: бабушкам и дедушкам, родителям и детям

Информационная поддержка от Сбера:



Спасибо
за внимание!

Правила кибербезопасности коротко, но точно отражены в наших памятках
и инструкциях. Изучайте, скачивайте, делитесь со всеми своими друзьями и близкими