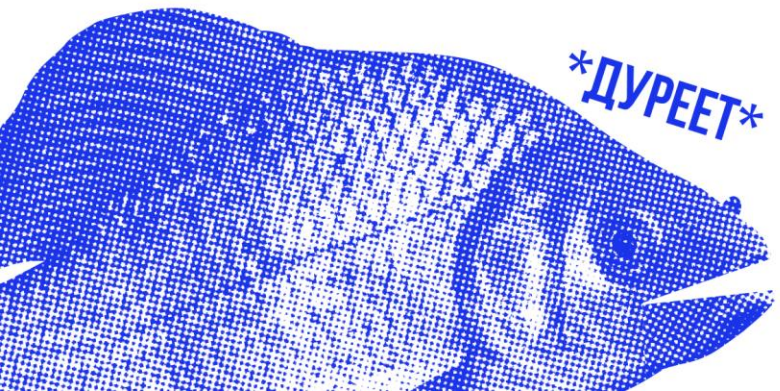
КАК НЕ ПОПАСТЬСЯ НА УЛОВКИ МОШЕННИКОВ

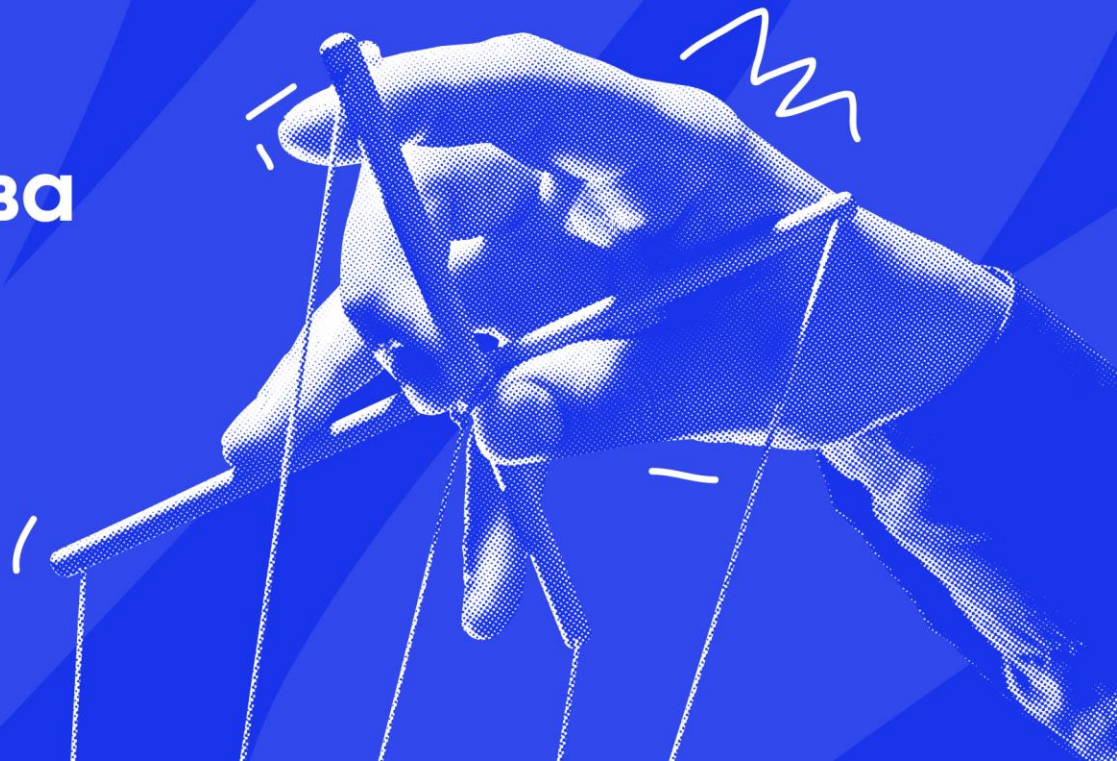


ЧТО ТАКОЕ МОШЕННИЧЕСТВО?

Мошенничество — это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием (ст. 159 УК РФ).

Инструменты мошенничества

- Мошеннические схемы
- Манипулятивное влияние



ЧТО МОЖЕТ БЫТЬ ЦЕЛЬЮ МОШЕННИКОВ?

1. Имущество (движимое/недвижимое, наличные деньги, криптовалюта и т. п.).
2. Права на чужое имущество (ценные бумаги, доверенности, наследство и т. д.).
3. Информационные активы (игровые аккаунты, социальные сети, e-mail и т. д.).
4. Персональные данные (логины и пороли, реквизиты карт, номера телефонов и т. д.).

СОВРЕМЕННЫЕ ВИДЫ МОШЕННИЧЕСТВА

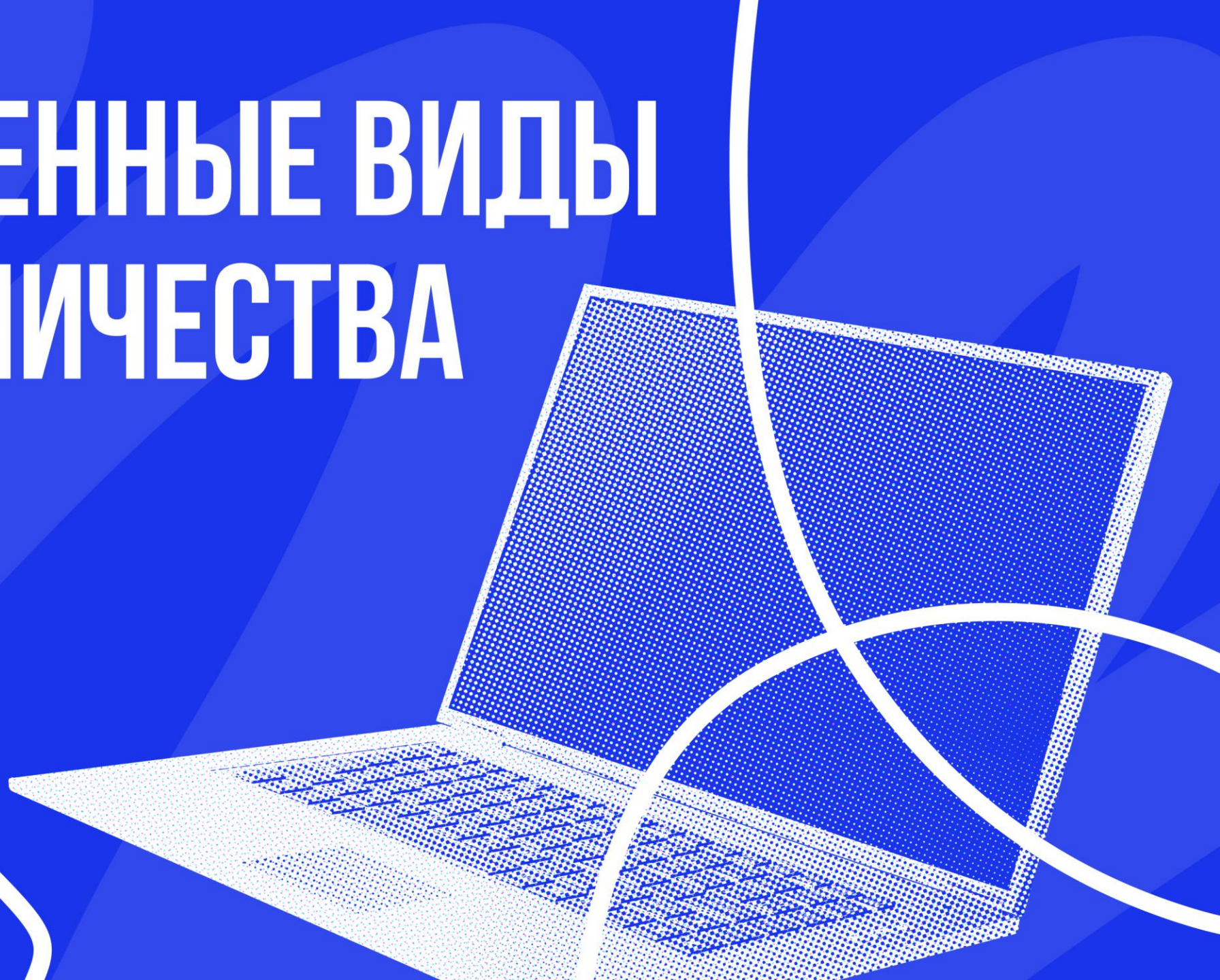
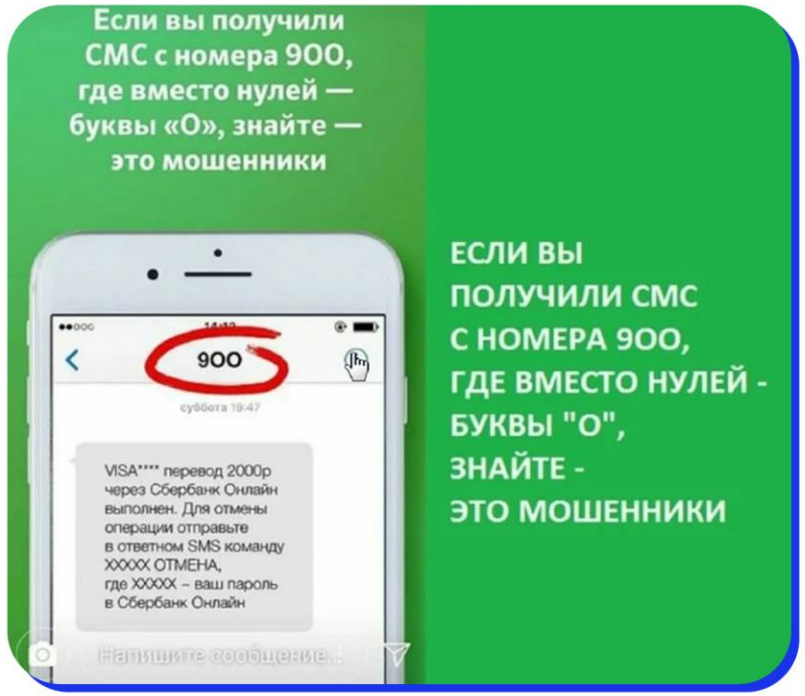


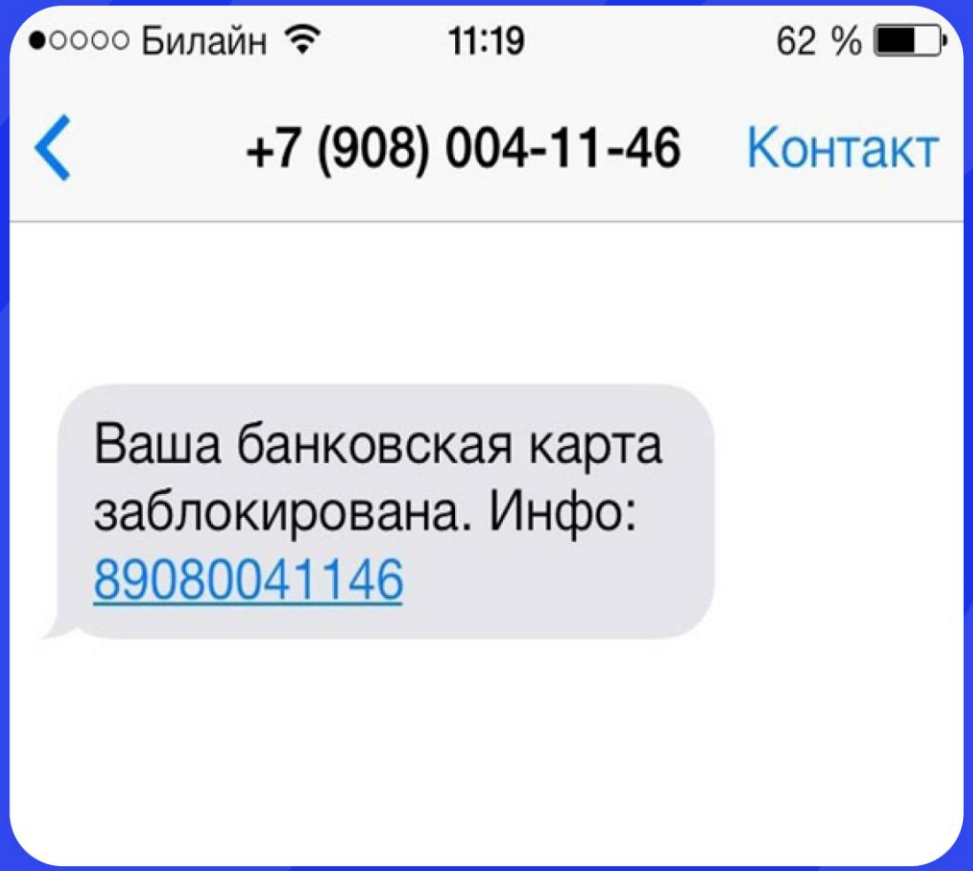
СХЕМА МОШЕННИЧЕСТВА:

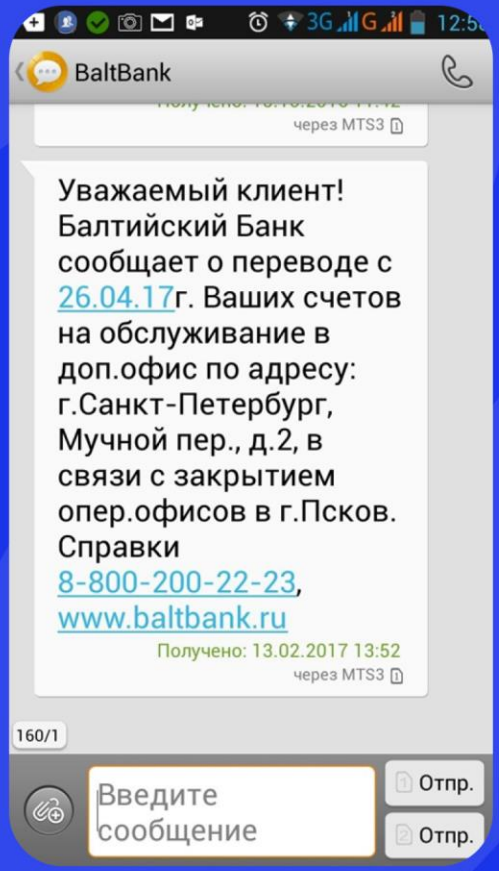
СЛУЖБА БЕЗОПАСНОСТИ «СБЕРБАНКА»

Пример обмана:
«Здравствуйте. Мы зафиксировали успешную попытку доступа злоумышленников к Вашему счету. С целью недопущения кражи Ваших денег, необходимо незамедлительно перевести все средства на специальный защищенный счет. Сейчас на Ваш телефон поступит СМС с кодом для безопасного счета. Не сообщайте оператору этот код, его нужно продиктовать нашему роботу, после специального сигнала...»



ПРИМЕРЫ МОШЕННИЧЕСТВА





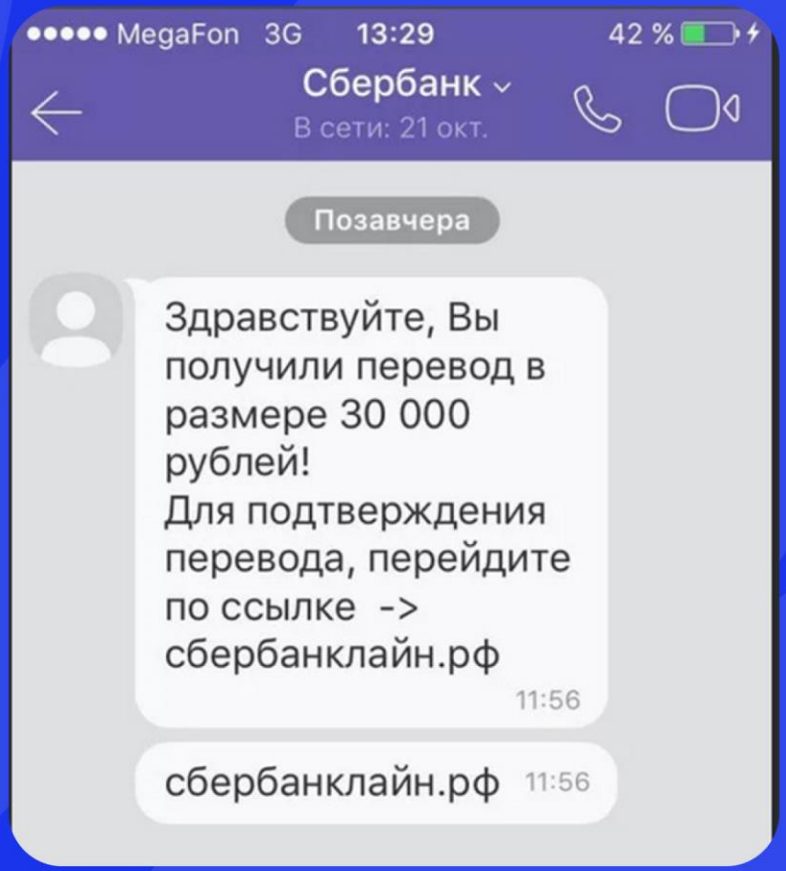


СХЕМА МОШЕННИЧЕСТВА:

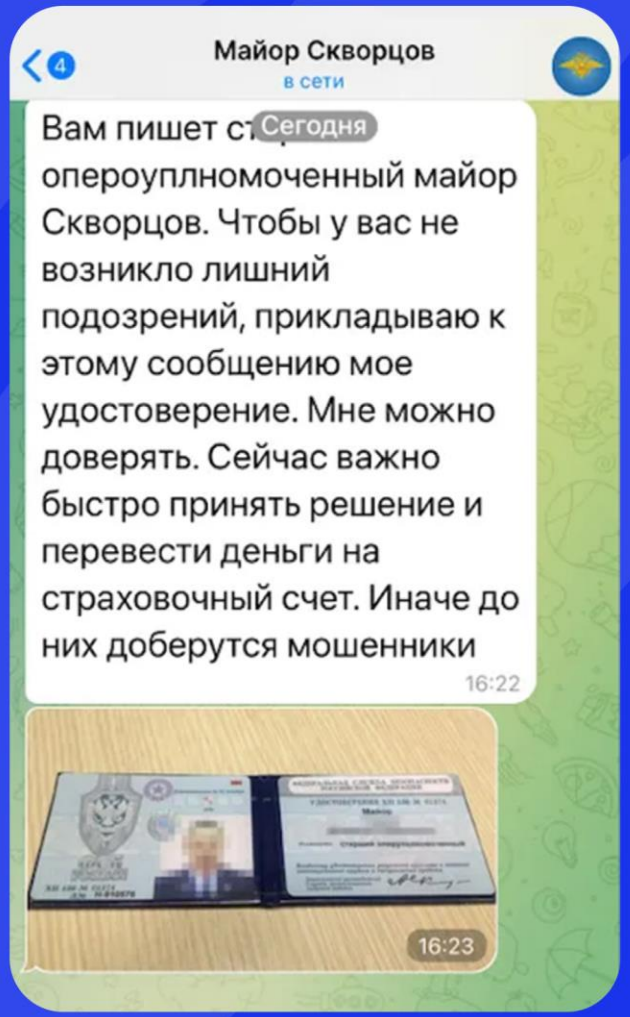
«СОТРУДНИКИ МВД»

1. Вам звонит «сотрудник» банка и спрашивает, оформляли ли вы заявку на кредит. После того как вы отвечаете «нет», он говорит, что за вас это сделали сотрудники банка, которые замешаны в мошеннической схеме.

2. С вами связывается человек из МВД и подтверждает все слова и ФИО «сотрудника» банка. Вам могут прислать выписки из банка, удостоверения и другие документы с печатями, чтобы убедить вас, что ситуация реальная.

3. Вам предлагают обратиться в отделение банка (или сразу в несколько банков) и подать новую заявку на кредит, чтобы предыдущая отменилась. При этом советуют «как можно меньше общаться» с сотрудниками банка в офисе. Как только вы получили деньги, вас просят перевести их на новый «безопасный» счет.

ПРИМЕРЫ МОШЕННИЧЕСТВА



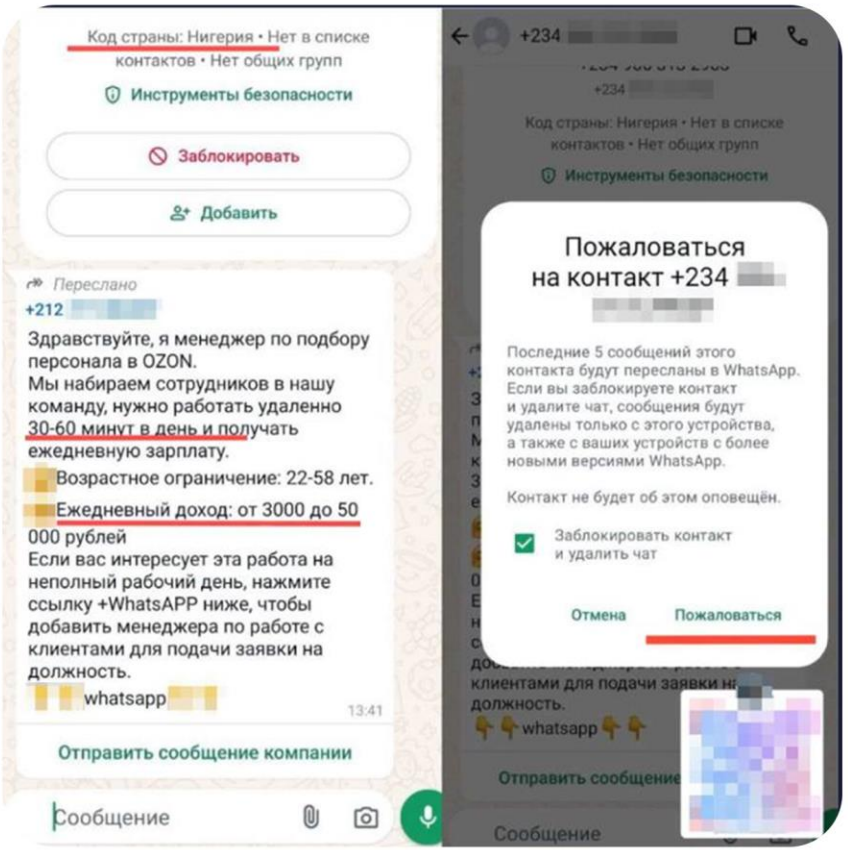
Даже если вам прислали удостоверение сотрудника полиции – это еще ничего не значит. Часто мошенники делают это для убедительности.

СХЕМА МОШЕННИЧЕСТВА:

СООБЩЕНИЯ С ПРЕДЛОЖЕНИЕМ РАБОТЫ

Суть схемы:
человек получает в мессенджере сообщение о «наборе» сотрудников.

Злоумышленники-«работодатели» предлагают удобные условия и стабильный заработок. На самом деле их цель — получить данные к аккаунтам или банковским счетам жертвы.



ПРИМЕР МОШЕННИЧЕСКОЙ СХЕМЫ

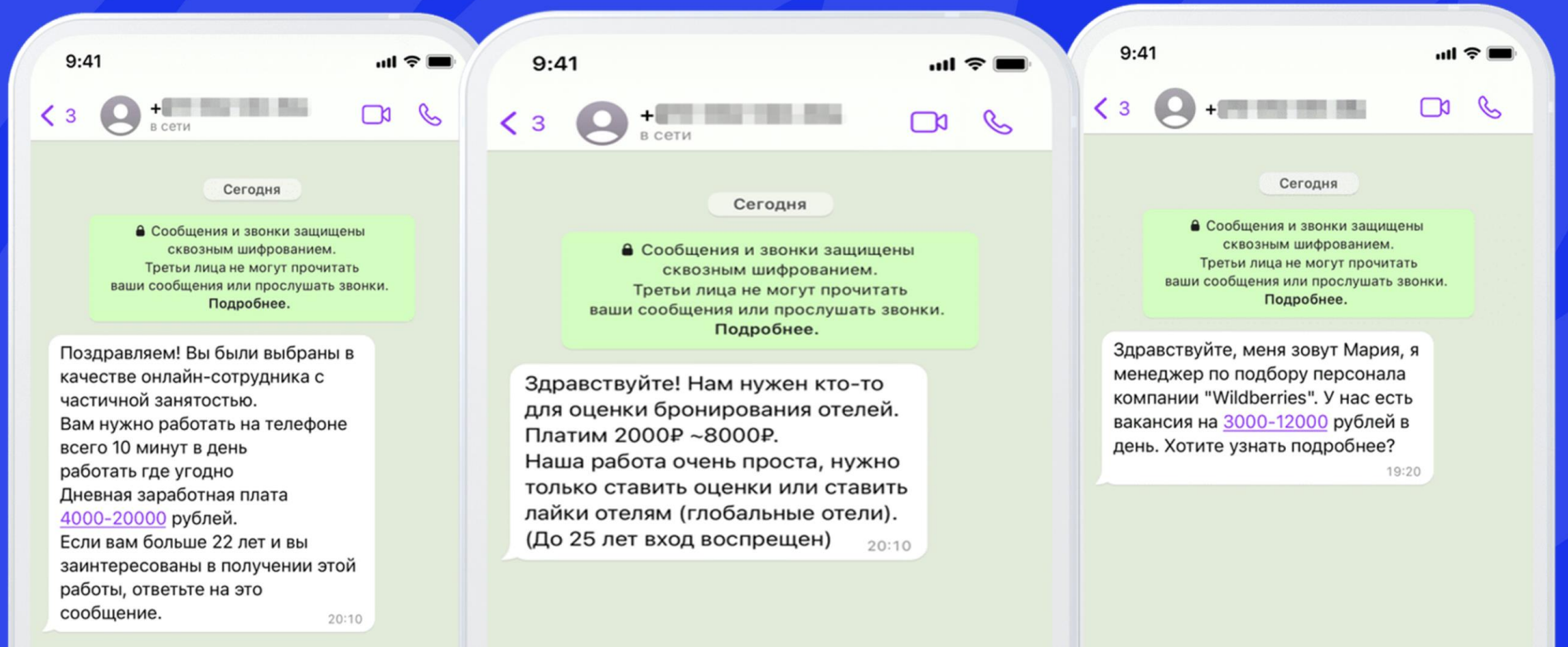


СХЕМА МОШЕННИЧЕСТВА:

ВЫПУСК ВИРТУАЛЬНЫХ КАРТ

Суть схемы:
злоумышленники убеждают завести
и добавить в электронный кошелек
«специальную» виртуальную карту — человек
уверен, что сохранит деньги, перечислив
их в «надежное место».

Жертва пополняет фальшивую карту через
банкомат наличными по присланному
мошенниками пин-коду и лишается средств.

СХЕМА МОШЕННИЧЕСТВА:

МОШЕННИЧЕСТВО ПОД ВИДОМ ТРУДОУСТРОЙСТВА В ПВЗ

Мошенники под видом владельца ПВЗ с подставных аккаунтов в мессенджере публикуют объявления о поиске сотрудников.

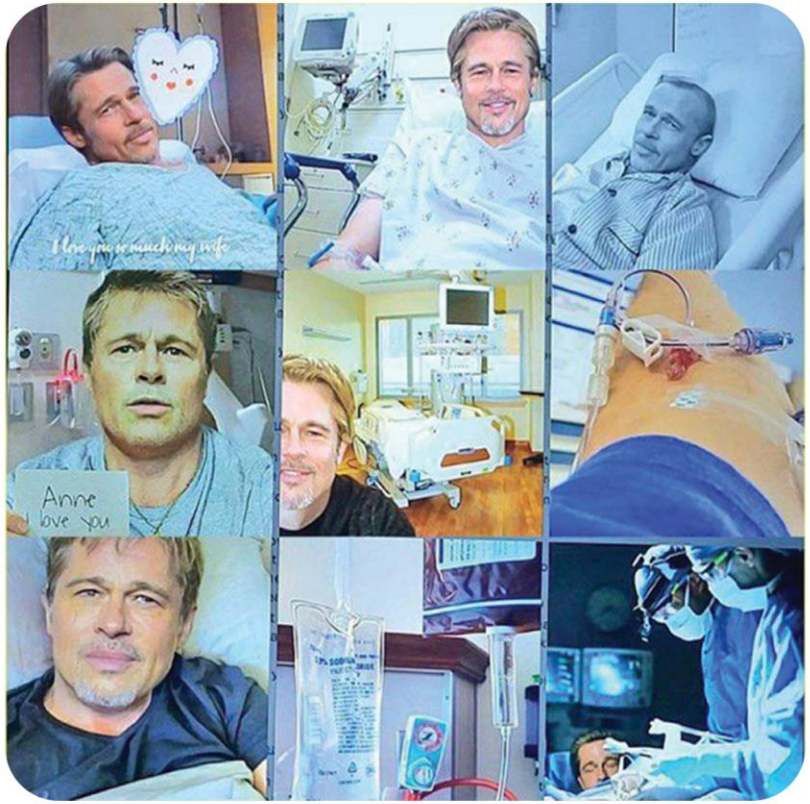
Человеку предлагают пройти собеседование в WhatsApp или через звонок. Ключевой вопрос — каким смартфоном пользуется жертва (преступников интересуют пользователи Android).

Жертву обмана просят заполнить анкету и направляют ссылку для загрузки приложения якобы для работы. На самом деле с помощью программы вносят троян удаленного доступа (RAT). Таким образом, мошенники взламывают телефоны и снимают деньги со счетов пользователя.

ДИПФЕЙК-АТАКИ

Мошенники совершают тысячи дипфейк-атак на сайтах знакомств, создавая фальшивые профили с использованием голоса и изображения реального человека. С помощью технологий искусственного интеллекта злоумышленники имитируют переписку, создают убедительные изображения, голосовые сообщения и видео.

Злоумышленники могут манипулировать эмоциями и убеждать переводить деньги, шантажировать угрозой распространения личных фото и видео.



«Аферист под видом Брэда Питта обманул 53-летнюю француженку на 830 тысяч евро. Женина ушла от мужа-миллионера, сделав выбор в пользу «голливудского актера».

КОЛЛЕГИЯ ПРИСЯЖНЫХ ЗАСЕДАТЕЛЕЙ

Мошенники через мессенджеры или электронную почту приглашают в коллегию присяжных заседателей.

В мессенджер или на почту могут приходить сообщения о том, что гражданин выбран для участия в коллегии присяжных заседателей. При этом за неявку обещают наступление административной и уголовной ответственности.

Для того, чтобы отказаться от этой обязанности, также предлагают нажать на ссылку в вызове для указания причин невозможности участия в коллегии присяжных.

Переход по ссылке дает злоумышленникам доступ к личным данным.

ОБМАН ПО ФЕЙКОВОМУ QR-КОДУ

- Мошенники публикуют в интернете фейковые объявления о гарантированной социальной выплате. В них есть ссылка на портал, похожий на «Госуслуги».

- На сайте пользователь сканирует QR-код и переходит в чат-бот в одном из мессенджеров. В нем человеку сообщают о положенной ему выплате: например, пособии для пенсионеров или семей с детьми, студенческой стипендии. Затем под предлогом оформления выплаты злоумышленники узнают личные данные и сведения о банковских счетах жертв.

- Мошенники начали наклеивать поддельные бумажные QR-коды поверх настоящих — сначала на товары и счета в кафе, а с недавних пор и на арендные самокаты.

ПРИМЕР МОШЕННИЧЕСТВА:

ПИСЬМО С QR-КОДОМ

Важная информация для **юристов** и специалистов по оформлению договоров!

Эта программа поможет Вам правильно вести дела, эффективно **выступать в судах** и снизить правовые риски Вашего предприятия!

Подробная информация в **QR коде**:

СХЕМА МОШЕННИЧЕСТВА:

ОБМАН ОТ «YOUTUBE»

СХЕМА МОШЕННИЧЕСТВА:

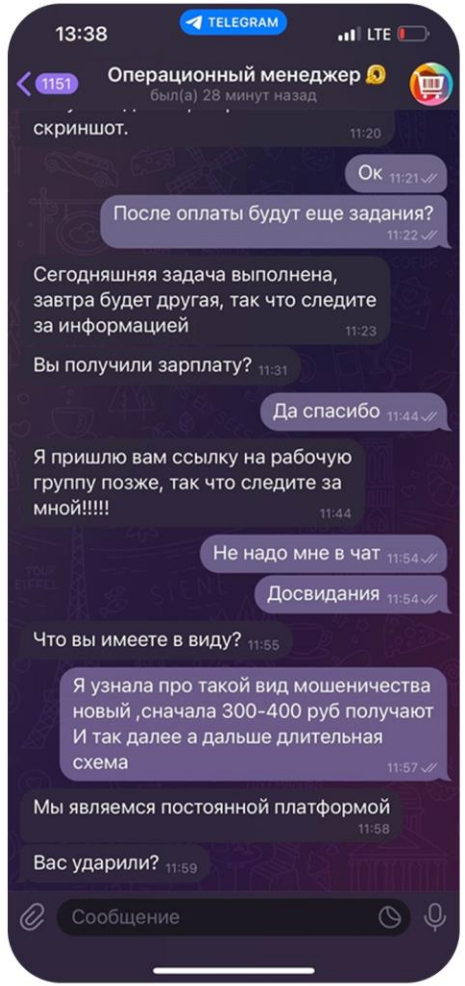
РАБОТА ЗА «ЛАЙКИ»

Мошенники под видом продавцов с маркетплейсов предлагают заработать денег за лайки товаров. Тут у аферистов несколько видов обмана:

После выполнения задания просят сообщить платежные данные карты для начисления вознаграждения. После отправки злоумышленники получают доступ к финансам жертвы.

После начисления денег мошенники могут попросить сообщить им номер телефона и код из SMS для подтверждения личности.

ПРИМЕРЫ МОШЕННИЧЕСКОЙ СХЕМЫ



КАК ЗАЩИТИТЬСЯ ОТ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА?

- Блокируйте номера, с которых поступают подозрительные звонки.
- Не сообщайте логины и пароли от аккаунтов, платёжные данные, одноразовые коды из смс.
- Не переводите деньги на счета, номера которых вам называют по телефону.
- Если вам поступило подозрительное сообщение от «руководителя организации», позвоните руководителю напрямую и уточните, присылал ли он подобное сообщение.

КАК ЗАЩИТИТЬ СЕБЯ ОТ ИНТЕРНЕТ-МОШЕННИКОВ?

- Внимательно проверяйте ссылки на сайты, требующие ввода учетных данных, не переходите по ссылкам из писем, смс и т. п.

- Для входа в интернет-банк используйте приложение банка, а не сторонние серверы.

- Если к вам обращаются с выгодным предложением работы, то перепроверьте другие вакансии у данного работодателя.

- Будьте бдительны. Всегда находите первоисточник и анализируйте материал, прежде чем совершать какие-либо действия.

- Если же вдруг вы поняли, что стали жертвой преступления, незамедлительно сообщайте об этом в правоохранительные органы. При этом не забудьте приложить скриншоты всех переписок, подтверждающих обоснованность вашего обращения.

Материал подготовлен НЦПТИ

На наших ресурсах больше полезных материалов для работы с молодежью!

Сканируйте QR-код
или ищите по никнейму

@NCPTI