О ПРОТИВОДЕЙСТВИИ ГИБРИДНОМУ МОШЕННИЧЕСТВУ И КИБЕРУГРОЗАМ

Гибридное мошенничество - совмещение в схеме обмана нескольких технологических областей (например, психология и информационные технологии) или соеденине воедино нескольких более простых мошеннических сценариев.

1. Дипфейки и чат-боты для кибермошенничества

Как работают:
Мошенники используют технологии дипфейков, чтобы подделывать видео и аудио с известными лицами или сотрудниками компаний. Чаще всего их "цель" — вызвать доверие.
Пример:
• В Индии во время предвыборной компании в парламент страны в видео созданные с помощью технологии DeepFake образы известных актеров якобы говорят, что премьер-министар Нарендру Моди не выполнил предвыборные обещания и не смог решить критические экономические проблемы в течение двух своих сроков на посту премьер-министра.
Как защититься:
•Проверяйте личность звонящего через официальный сайт или номер компании.
•Никогда не передавайте конфиденциальные данные во время звонков.

2. Поддельные сотрудники налоговых органов

Как работают:
Злоумышленники звонят жертвам, представляясь сотрудниками налоговой службы, и требуют "задекларировать доходы". Если жертва соглашается, преступники отправляют курьера за деньгами или просят перевести средства.
Пример:
В Москве пенсионерка потеряла 2,3 миллиона рублей. Курьер мошенников забрал наличные и оставил поддельный договор, который оказался обычной распечаткой.
Как защититься:
•Связывайтесь с налоговой службой напрямую, используя официальные контакты.
•Курьеры никогда не собирают деньги от имени государственных учреждений.

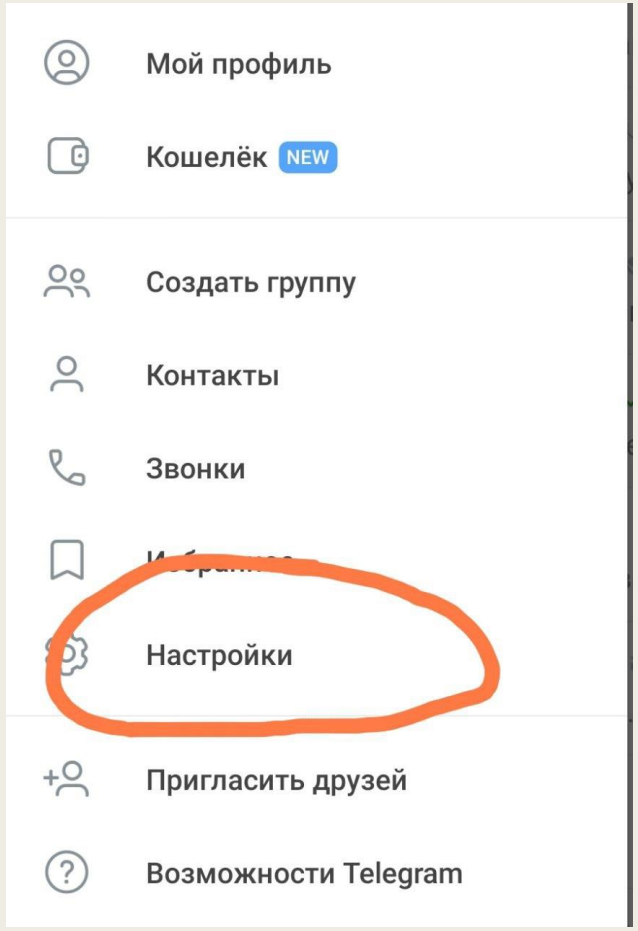
3. Фишинг через маркетплейсы

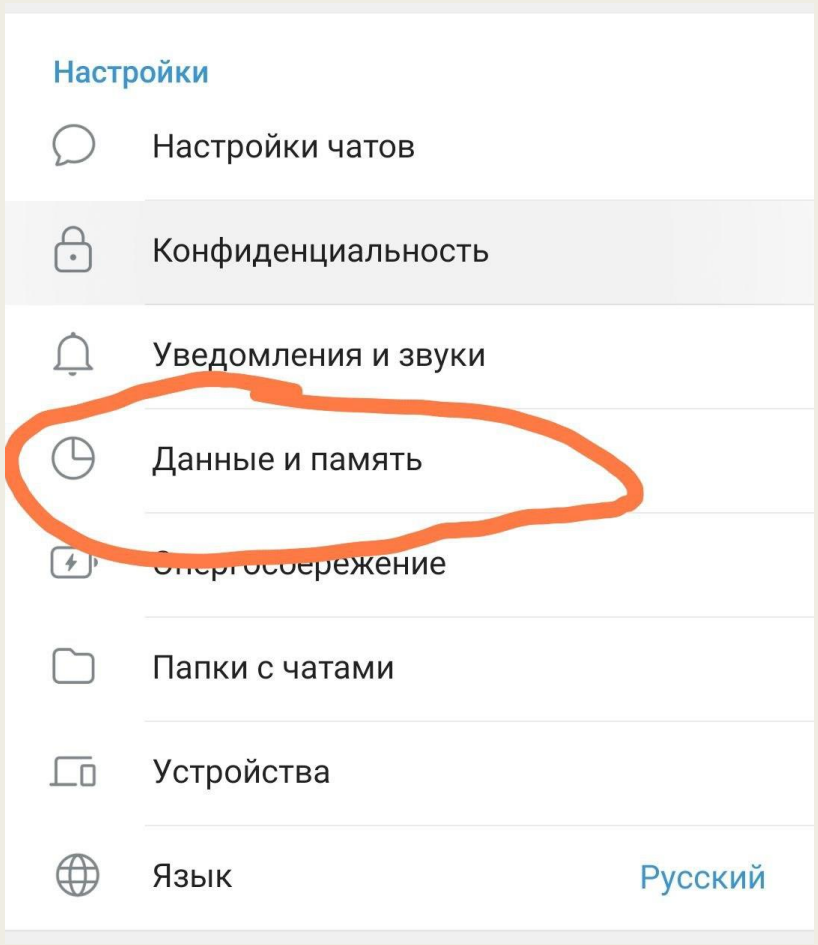
Как работают:
Мошенники создают сайты, внешне похожие на популярные маркетплейсы. Они предлагают "эксклюзивные скидки", заманивая пользователей вводить данные банковских карт.
Пример:
В период распродаж "чёрной пятницы" в России зафиксировано более 17 тысяч фишинговых сайтов. Один из них копировал дизайн известного маркетплейса, похищая данные карт пользователей.
Как защититься:
•Проверяйте адрес сайта: он должен соответствовать официальному домену.
•Используйте только проверенные приложения для покупок.

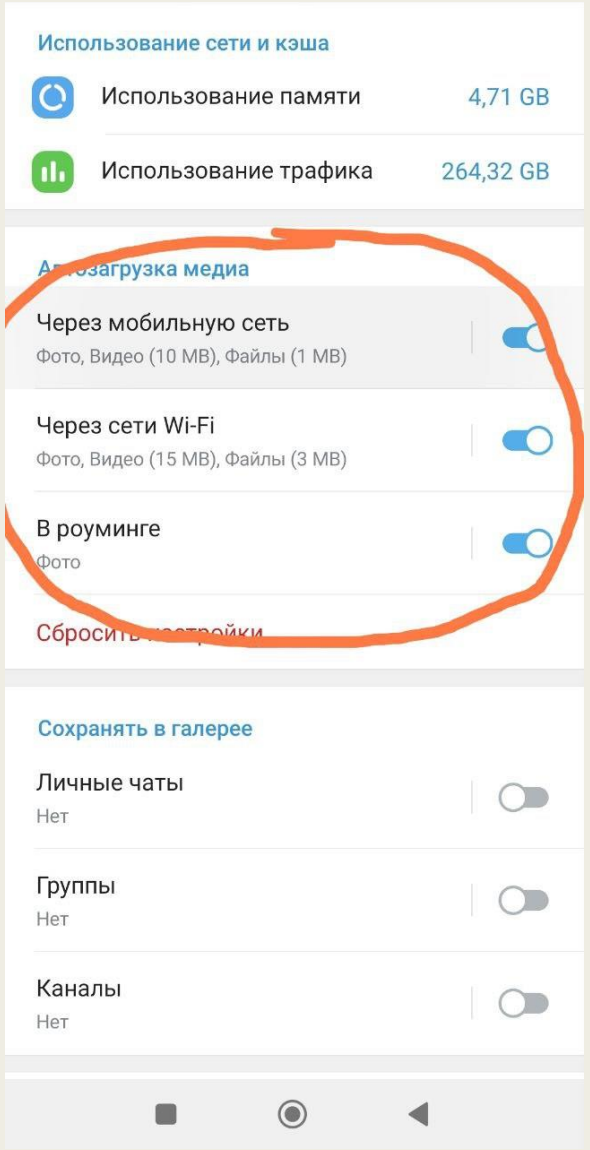
4. Вредоносные изображения, документы и приложения

Как работают:
Атаки через стеганографию: вирусы скрываются в обычных изображениях или текстовых файлах. При их открытии вредоносное ПО устанавливается на устройство.
Пример:
В связи с блокировкой Viber гражданам предлагается скачать новый VPN сервис, который по сути является шпионской програмой
Как защититься:
•Не скачивайте вложения из писем от незнакомых отправителей.
•Установите защитное ПО на устройства и обновляйте его регулярно.

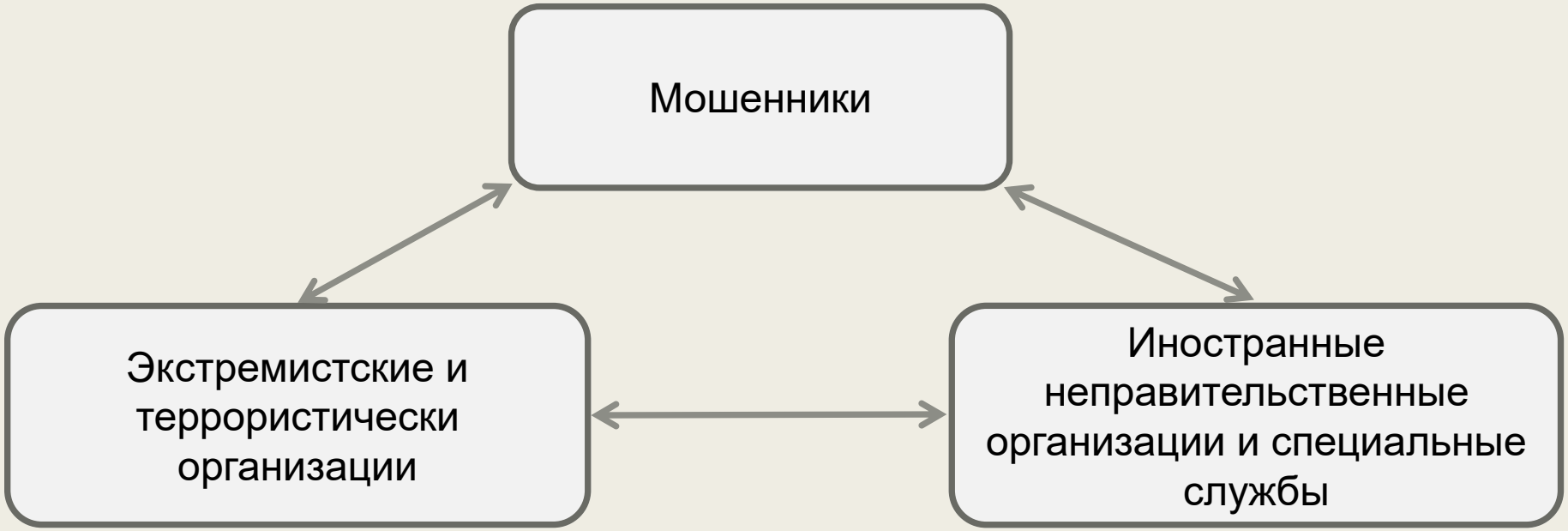
4. Настройки Telegram







Виды киберугроз



Статья 205 УК РФ. Террористический акт

Совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями -

Мошенники продолжают использовать новые технологии и адаптироваться к защитным мерам.

Способы защититься:

- Осведомлённость
- Внимательность
- Использование современных инструментов кибербезопасности.

Берегите свои финансы

обучайте своих близких

делитесь полезной информацией!