



УФСБ  
МВД РОССИИ

ЛАПША  
ПРОФИ

# ТОП МОШЕННИЧЕСКИХ СХЕМ В МЕССЕНДЖЕРАХ





УБК  
МВД РОССИИ

ЛАПША  
медиа

## УГОН АККАУНТА

**Злоумышленники охотятся за аккаунтами, чтобы использовать доверие к знакомому имени, аватарке и истории переписки.**

Привет Юра, хочу попросить тебя

В творческо-благотворительном соревновании рисунков участвует ребёнок нашей родни – Маша (Янкова).

Участие – это возможность получения гранта.

Если найдёшь немного времени – за Янкову Машеньку отметишь пожалуйста

Здесь: [\[ссылка\]](#)

Благодарю! Передай друзьям ❤️

**Получив контроль над профилем, они атакуют не одного человека, а все его контакты: рассылают вредоносные ссылки, выманивают коды из СМС и ищут в переписках финансовые данные или документы.**



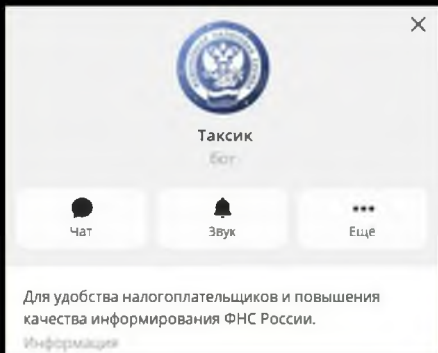


УБК  
МВД РОССИИ

**ЛАПША**  
медиа

# ПОДДЕЛЬНЫЕ БОТЫ ГОСОРГАНОВ

Мошенники создают ботов с логотипами ФНС или Социального фонда и предлагают «проверить долги» или «оформить выплату». Для получения услуги просят ввести номер телефона и код из СМС.



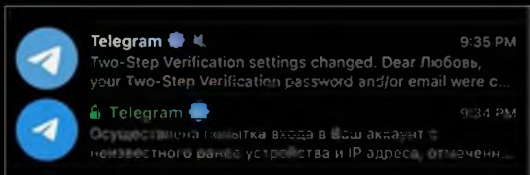


УБК  
МВД РОССИИ

ЛАПША  
МОДНА

## ФИШИНГ ОТ ЛИЦА СЛУЖБЫ БЕЗОПАСНОСТИ И АДМИНИСТРАТОРОВ КАНАЛОВ

Злоумышленники используют «секретный чат», чтобы маскироваться под службу безопасности Telegram, и отправляют предупреждение о «входе с нового устройства» вместе с ссылкой для подтверждения. Опасная ссылка также может прийти от «администратора» известного тг-канала под видом голосования или приза.



В обоих случаях аккаунты выглядят правдоподобно: с «галочкой» отдела безопасности или известным логотипом, но ссылка в сообщении — фишинговая. Ввод кода из СМС или сканирование QR приведут к угону аккаунта.



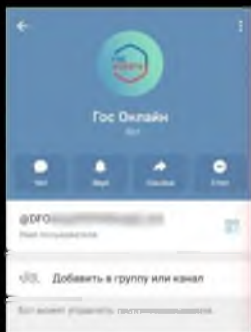


УБК  
МВД РОССИИ

**ЛАПША**  
медиа

## ФЕЙКОВЫЕ «ГОСУСЛУГИ»

Вас добавляют в фейковый домовый или районный чат и под видом «проверки счетчиков воды» просят перейти по ссылке. Помимо чата жильцов можно встретить срочные петиции и голосования по социально значимым вопросам.



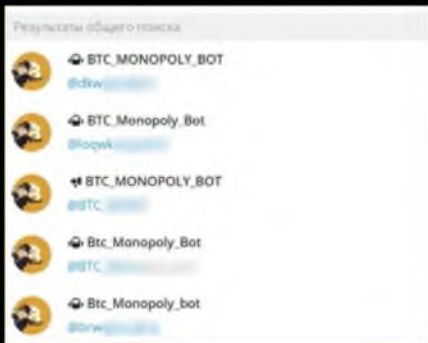
И там, и там ссылки ведут на страницу, имитирующую вход в «Госуслуги». Однако при вводе логина, пароля и СМС-кода ваш аккаунт переходит в чужие руки.





## КРИПТО-БОТЫ

Злоумышленники регистрируют домены, визуально неотличимые от адресов известных криптобирж или обменников: заменяют букву «О» на ноль или «q» на «р».



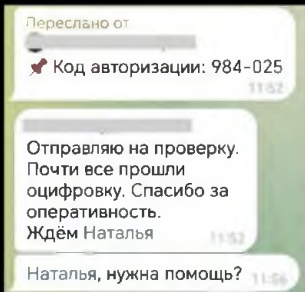
Через ботов жертв торопят совершить перевод, ведь «курс действует 5 минут». Но если не заметить подмену, деньги будут потеряны.





## РАБОЧИЙ ЧАТ-ЛОВУШКА

С помощью открытых источников мошенники собирают имена, должности и фото сотрудников компании. Они создают липовый рабочий чат и добавляют туда жертву и ботов, изображающих коллег и начальника.



От имени руководства ставится «срочная задача» — передать код для «оцифровки архива» или «подтвердить доступ». Боты-коллеги в свою очередь создают эффект группового давления и подтверждают, что всему происходящему якобы можно доверять.





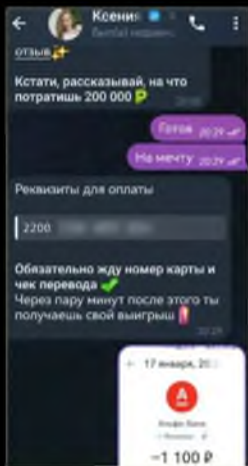
УБК  
МВД РОССИИ

**ЛАПША**  
медиа

## ОБРАТНЫЙ ВЫИГРЫШ

Жертве сообщают о крупном выигрыше или высоком доходе от инвестиций. Для убедительности присылают поддельные скриншоты банковских уведомлений.

Чтобы «разблокировать средства» или «увеличить процент конвертации», просят сделать встречный перевод на указанную карту. На самом деле никакого выигрыша нет, а «денежное подтверждение» просто украдут.





УБК  
МВД РОССИИ

**ЛАПША**  
медиа

## КАК ЗАЩИТИТЬСЯ?

- **Никогда и никому не передавайте коды из СМС, даже если просит ваш знакомый.**
- **Включите двухфакторную аутентификацию.**
- **Не переходите по подозрительным ссылкам.**



**ПОДЕЛИТЕСЬ ЭТОЙ  
ИНФОРМАЦИЕЙ  
С БЛИЗКИМИ**