

Вся информация
об актуальных схемах
мошенничества и способах
защиты в канале УБК МВД
России



Ежедневное
опровержение
недоверенной
информации
от фактчекингового
проекта «Лапша Медиа»
(проект АНО «Диалог
Регионы»)



ТИПОВЫЕ ФРАЗЫ МОШЕННИКОВ

СЛЫШИТЕ ИХ
ИЛИ ВИДИТЕ
В СООБЩЕНИЯХ?
КЛАДИТЕ
ТРУБКУ!

- 1 «Безопасный счёт»
- 1 «Декларация средств»
- 1 «Дистанционный обыск»
- 1 «Компрометация карты»
- 1 «Секретная операция»
- 1 «Ваш аккаунт Госуслуг взломан»
- 1 «Оформлена доверенность»
- 1 «Подтвердите получение посылки»
- 1 «Мама / папа, я в беде. Срочно переведи деньги»
- 1 «С вами свяжется сотрудник ФСБ / Росфинмониторинга»
- 1 «У вас на счету подозрительная операция»
- 1 «Это ты на фото / видео?»
- 1 «Проголосуй в конкурсе»

**НЕ ДОВЕРЯЙТЕ
НЕЗНАКОМЦАМ!**

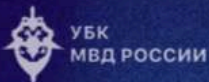


УБК
МВД РОССИИ

ДИАЛОГ
РЕГИОНЫ

ПРОСТЫЕ ПРАВИЛА

самозащиты
от
мошенников



УБК
МВД РОССИИ

ДИАЛОГ
РЕГИОНЫ

ТИПОВЫЕ СХЕМЫ МОШЕННИКОВ

ПОД УГРОЗОЙ

УСТАНОВЛЕНИЕ КОНТАКТА

Повод может быть любым: запись к врачу, замена домофонных ключей, доставка письма, проверка счётчиков или другая рядовая ситуация

ЦЕЛЬ: **ВЫМАНИТЬ КОД ИЗ SMS**

СОЗДАНИЕ И ПОДДЕРЖАНИЕ ИЛЛЮЗИИ УГРОЗЫ

Либо вам приходит сообщение от «банка», «полиции», «оператора связи», «Госуслуг» о том, что с вашего счёта пытаются украсть деньги, так как вы сообщили код из SMS, и ваш аккаунт взломан.

ЦЕЛЬ: **ЗАСТАВИТЬ ВАС ПЕРЕЗВОНИТЬ
ПО НОМЕРУ, УКАЗАННОМУ В СООБЩЕНИИ**

Либо после первого звонка вам поступает звонок от якобы сотрудника правоохранительных органов или службы поддержки, который информирует, о попытке мошенников получить доступ к вашим счетам. Для усиления доверия присылают поддельные удостоверения, протоколы и письма о блокировке, фишинговые ссылки.

ЦЕЛЬ: **ЗАПУГАТЬ И ВЫЗВАТЬ ДОВЕРИЕ
К «ОФИЦИАЛЬНЫМ» ЛИЦАМ**

УСТРАНЕНИЕ УГРОЗЫ = ХИЩЕНИЕ

- Попросят провести «дистанционный обыск» для выявления ваших средств. Говорят о необходимости задекларировать накопления, перевести деньги на «безопасный счёт», установить «официальное» приложение. Могут потребовать оформить займ для «защиты имущества».
- Вас попросят передать наличные и ценности курьеру или перевести по СБП/на карту.

ЦЕЛЬ: **ЗАСТАВИТЬ ПЕРЕДАТЬ ДЕНЬГИ
И ЦЕННОСТИ ТРЕТЬИМ ЛИЦАМ**

ПОД ПРЕДЛОГОМ ВЫГОДЫ

УСТАНОВЛЕНИЕ КОНТАКТА

- Вас находят: рекламные сообщения, «случайные» собеседники в соцсетях или мессенджерах.
- Вам обещают: скидку, выигрыш, лёгкий доход, возможность изменить жизнь.

ЦЕЛЬ: **ЗАЦЕПИТЬ ВАШЕ ВНИМАНИЕ**

ИЛЛЮЗИЯ ВЫГОДЫ

- Торопят: «последнее место», «акция дня», «гарантированный/пассивный доход».
- Демонстрируют «успех»: машины, курорты, фото/видео «клиентов».
- Сбрасывают поддельные ссылки на кабинет, графики роста, фейковые отзывы.
- Для убедительности — после простого действия возможна реальная выплата (гонорар).

ЦЕЛЬ: **СОЗДАТЬ ОЩУЩЕНИЕ ВЫИГРЫША
ИЛИ ЗАРАБОТКА**

ВЫГОДА = ХИЩЕНИЕ

Когда вы «клюнули»: просят перевести деньги на счёт мошенников для инвестиций.

ЦЕЛЬ: **ДОБРОВОЛЬНЫЙ ПЕРЕВОД
ТРЕТЬИМ ЛИЦАМ**

После основной суммы для «большой выгоды» могут потребовать:

- налог/госпошлину за приз;
- пополнить баланс в поддельном приложении для вывода;
- купить валюту/NFT для утращения;
- встречный перевод для подтверждения личности или активации.

ЦЕЛЬ: **ВЫМАНИТЬ ЕЩЕ**

ЧЕК-ЛИСТ ПРАВИЛ БЕЗОПАСНОСТИ при телефонных разговорах



- 1 **СОХРАНЯЙТЕ КРИТИЧЕСКОЕ МЫШЛЕНИЕ.** Мошенники постоянно совершенствуют свои схемы. Даже если звонок кажется правдоподобным, всегда проверяйте информацию через официальные каналы.
- 1 **ОБУЧИТЕ БЛИЗКИХ КИБЕРБЕЗОПАСНОСТИ.** Особенно важно объяснить правила безопасности детям и пожилым родственникам.
- 1 **СЛЕДИТЕ ЗА ОБНОВЛЕНИЯМИ.** Регулярно проверяйте новости о новых схемах мошенничества, чтобы быть в курсе современных методов обмана.
- 1 **ЗАПИСЫВАЙТЕ ВАЖНЫЕ НОМЕРА.** Храните в телефоне официальные контакты банков, служб безопасности и других важных организаций.
- 1 **БУДЬТЕ ОСТОРОЖНЫ С ЛИЧНОЙ ИНФОРМАЦИЕЙ.** Не публикуйте слишком много личных данных в социальных сетях — это может помочь мошенникам создать более убедительную легенду.
- 1 **ИСПОЛЬЗУЙТЕ СПЕЦИАЛЬНЫЕ СЕРВИСЫ.** Подключите услуги блокировки спам-звонков от вашего оператора связи, установите услугу «второй руки» при проведении банковских операций.
- 1 **ДОКУМЕНТИРУЙТЕ ПОДОЗРИТЕЛЬНЫЕ СЛУЧАИ.** Если вы столкнулись с попыткой мошенничества, сообщите об этом в банк, полицию и на специальные горячие линии.

**ПОМНИТЕ:
ЛУЧШАЯ ЗАЩИТА — ЭТО ПРОФИЛАКТИКА
И ПОСТОЯННАЯ БДИТЕЛЬНОСТЬ**