В 2025 – 2026 годах мошенники перешли к гибридным атакам, комбинируя социальную инженерию с технологиями искусственного интеллекта.

Чтобы не потерять деньги, запомните: сотрудники банков, работники правоохранительных органов и госслужащие никогда не предлагают перевести деньги на «безопасный счет» и не просят коды из СМС

ТОП-5 УГРОЗ 2026 ГОДА

«Безопасный счет» под прикрытием ИИ

Звонок от «следователя» или «службы безопасности банка» – самая массовая схема. Теперь мошенники используют нейросети для подмены номеров (на экране высвечивается настоящий номер ведомства) и клонирования голосов.

Вам может позвонить «родственник» с просьбой о выкупе или «начальник», подтверждающий легенду.

Как действовать: *прервите разговор. Перезвоните человеку по известному Вам номеру или лично.* ***Не доверяйте голосу – это может быть дипфейк.***

Фейк от маркетплейсов и «Госуслуг»

Вам приходит СМС о невозможности доставки посылки или подозрительном входе в аккаунт со ссылкой для «подтверждения данных». Ссылка ведет на фишинговый сайт, который крадет пароли.

Внимание: *мошенники часто присылают код на английском («1111 is your login code...»), чтобы запутать пользователя.* ***Никому не диктуйте код из СМС!***

Фейковые инвестиции и «помощь» от юристов

Вам обещают сверхдоход от инвестиций в криптовалюту или предлагают «бесплатно» вернуть деньги, украденные ранее. После ввода данных на сайте лжеброкеров или юристов Вы теряете остатки средств.

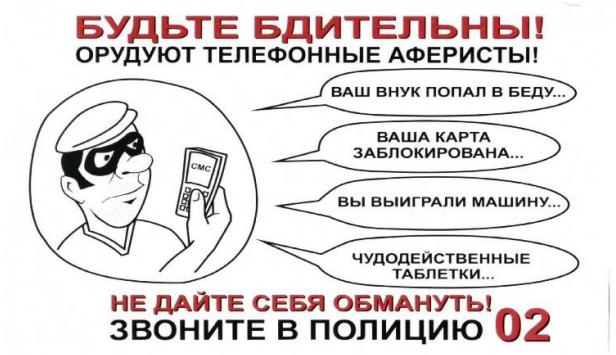
Как действовать: *прервите разговор. Если Вам действительно нужна консультация брокера либо юриста – обращайтесь лично к специалистам, которые имеют многолетнюю практику и хорошую репутацию.*

Взлом аккаунтов в Telegram и WhatsApp

Вам приходит сообщение от «друга» с просьбой проголосовать за ребенка или получить приз от адвент-календаря, или о предоставлении денег взаймы. **Переход по ссылке приводит к утрате аккаунта.** Деньги просят перевести не по номеру телефона «друга», который Вам известен, а по какому-либо стороннему номеру телефона, которым владеет мошенник.

Вредоносные приложения (троян Mamont)

Вам предлагают установить «приложение Минздрава» или «обновление безопасности». На самом деле это троян, посредством которого мошенники получают доступ к Вашим СМС-уведомлениям и банковским приложениям.



Самые частые схемы мошенников 2026 года

- **Звонок от «оператора сотовой связи»** с предложением продлить договор (якобы из-за новых законов). Цель мошенников – получить код из СМС для входа в Ваш личный кабинет на сайте оператора и перевыпуска сим-карты.

- **Сообщения в мессенджерах от имени руководителя** (дипфейк-видеозвонки или голосовые). Генеральный директор «просит» Вас срочно помочь с переводом денег на указанный им телефонный номер или банковский счет.

- **Сообщения в мессенджерах либо звонок о необходимости декларирования денежных средств, драгоценных металлов и ювелирных изделий.** Мошенники ссылаются на «приказы Центробанка», «распоряжения следователей» и новые «требования Генпрокуратуры». Для декларирования требуют передать денежные средства и драгоценности курьеру, запугивают уголовной ответственностью.

Что делать, если Вас взломали или обманули

Если Вы перевели деньги мошенникам:

- Немедленно **заблокируйте карту** через приложение банка или по телефону горячей линии банка.
- **Позвоните в банк** и сообщите о мошеннической операции (постарайтесь сделать это в течение суток – выше шанс возврата средств по системе «Чарджбэк»).
- **Напишите заявление в полицию** (лично или через сайт МВД России). Возьмите талон-уведомление.

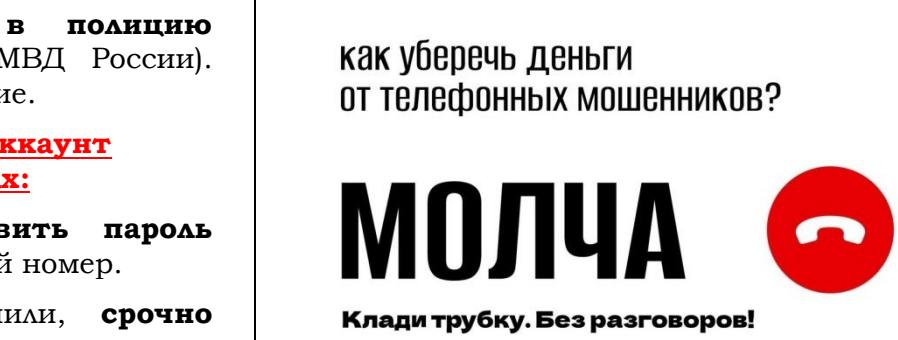
Если взломали Ваш аккаунт на Госуслугах:

- **Попытайтесь восстановить пароль** через СМС на привязанный номер.
- Если номер тоже сменили, **срочно идите в МФЦ с паспортом** для восстановления доступа.
- **Проверьте**, не пытались ли оформить на вас **кредиты** (закажите кредитную историю через Госуслуги или банк).

Если Вы установили вредоносное приложение:

- **Переведите телефон в «режим полета»** (отключите Интернет), чтобы вирус не передавал данные.
- Удалите все подозрительные приложения.
- **Смените** с другого устройства **пароли от всех важных сервисов**.
- Проверьте смартфон **антивирусом**.

Любые сообщения в мессенджерах и звонки от незнакомцев с требованиями совершить финансовые действия (перевести деньги, оформить кредит, списать долги, задекларировать имущество) **или назвать персональные данные – это признаки мошенничества.**

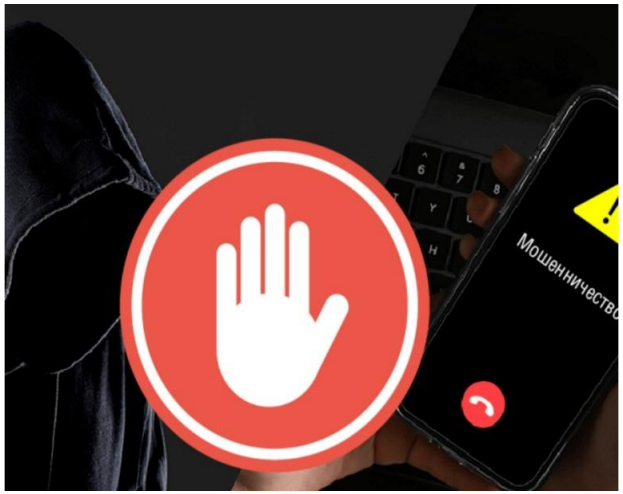


Если вы все-таки стали жертвой мошенников, немедленно сообщите об этом в полицию, позвонив по телефону 02 либо по телефону дежурной части УМВД России по Тюменской области 8 (3452) 291-600.

Совет при Тюменской областной Думе по повышению правовой культуры и юридической грамотности населения Тюменской области

Управление МВД России по Тюменской области

ПАМЯТКА



ПО ПРОТИВОДЕЙСТВИЮ МОШЕННИЧЕСТВУ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

г. Тюмень, 2026