СТАНДАРТНАЯ СХЕМА МОШЕННИЧЕСТВА

1 Захват внимания жертвы

Цель: вызвать тревогу или любопытство, спровоцировать на активное действие.

Признаки:

- СМС или push-уведомление **о взломе, списании средств, подозрительной активности.**
- Звонок или сообщение в мессенджере от имени известной организации — **банк, оператор связи, портал Госуслуг, Почта России.**
- Использование реалистичных аккаунтов и номеров с кодами регионов, эмблем, логотипов, правдоподобных имен.
- Призыв к срочным действиям**: «требуется срочное подтверждение», «иначе счет будет заблокирован», «уголовная ответственность».**

❗ ***Пример**: Жертве приходит сообщение якобы от банка о несанкционированном списании. В панике она пытается выяснить причину и ищет поддержку.*

2 Формирование доверия

Цель: убедить, что жертва общается с представителями официальной организации.

Признаки:

- Представление **«сотрудником техподдержки», «оператором банка», «сотрудником ФСБ» или ЦБ РФ.**
- Перевод от одного «специалиста» к другому: сначала техподдержка, потом "ЦБ", затем "ФСБ".
- Использование видеосвязи, фейковых договоров, инструкций с подписями и печатями.
- Активное сопровождение: **«все делается ради вашей защиты», "мы вам поможем".**

❗ ***Пример:*** *Человек получает звонок якобы от сотрудника «Госуслуг», который затем "передает его делу" ЦБ, ФСБ, и т.д.*

3 Получение критической информации

Цель: добыть коды доступа для последующих действий.

Признаки:

- ☑ Запрос персональных данных: **ФИО, дата рождения, номер телефона, СНИЛС, номер карты, код договора.**
- ☑ Запрос **одноразовых кодов из СМС** под предлогом подтверждения операций или отключения платных услуг.
- ☑ Переход по фишинговым ссылкам **(клонам Госуслуг, банков, маркетплейсов).**
- ☑ Установка **вредоносных приложений** под видом безопасных сервисов или цифровых кошельков.

❗ ***Пример:*** *Жертва сообщает код из СМС, думая, что отменяет подписку. На деле — позволяет злоумышленника авторизоваться на «Госуслугах».*

4 Манипуляция и побуждение к переводу средств

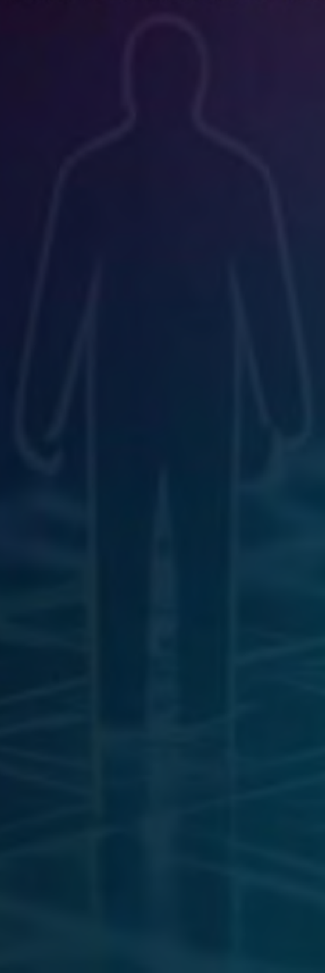
Цель: добиться от жертвы добровольного перевода всех или части денег на счёт, контролируемый мошенниками.

Признаки:

- **Внушение страха:** «ваш счет использовали террористы», «через вас отмывают деньги», «уголовное дело уже открыто».
- **Предложение решения:** «переведите деньги на безопасный счёт», «задекларируйте наличные», «внесите средства на виртуальную карту».
- **Давление:** «нельзя никому рассказывать», «мы следим за вами», «действуйте строго по инструкции».
- Финансовые манипуляции через банкоматы, личный кабинет банка или мобильное приложение.
- **Организация поездок:** вызов такси, указание конкретных адресов отделений и банкоматов.

В случае получения доступа к аккаунту на портале «Госуслуги» мошенники получают:

- **доступ к персональным данным** (ФИО, адрес, документы, привязанные номера)
- **инструмент манипуляции** — могут показать жертве "официальное уведомление" от портала (на деле — фейк)
- **авторитет** — "раз уже взломали Госуслуги, значит дело серьезное"
- **легитимация сценария:** "чтобы остановить мошенников, нужно передать деньги на безопасный счет".



5 Завершение и исчезновение

Цель: добиться от жертвы добровольного перевода всех или части денег на счёт, контролируемый мошенниками.

Пример: *Жертве сообщили, что через Госуслуги была оформлена электронная подпись, и с её помощью мошенники уже перевели средства террористам. Убедили внести наличные через банкомат на "защищённую виртуальную карту".*