СХЕМЫ МОШЕННИЧЕСТВА

Мошенничество с личными финансами — целая индустрия, которая благодаря технологиям может работать полностью удаленно, без личных контактов с жертвами. РБК со ссылкой на данные МВД сообщает, что в 2025 году самым массовым видом дистанционного мошенничества были попытки злоумышленников убедить доверчивых людей перевести деньги на якобы особый безопасный счет.

Разбираем 3 актуальных схемы, которые используют злоумышленники. Чем больше людей знают о методах мошенников, тем проще противостоять обману. Отправьте ссылку на эту статью близким, чтобы они понимали, как распознать махинации и что делать в подозрительных ситуациях.

Схема 1. «Сбрось мне свою геолокацию»

Сценарий начинается безобидно: переписка в боте знакомств, пара фото. Дальше собеседник предлагает перейти в мессенджер и «запланировать встречу».

После непродолжительной переписки звучит просьба: «Скинь геолокацию какого-нибудь известного места в твоем районе — так проще понять, где нам назначить встречу». Формулировки мягкие, вежливые и доброжелательные — расчет на то, что собеседник не захочет выглядеть занудой и скинет координаты. Тем более просят и так всем известную точку в городе, а не личный адрес.

Как только геометка отправлена, мошенник переходит к следующему этапу плана. На телефон приходит видеофайл. В ролике человек сообщает, что по указанным координатам могут проводиться незаконные действия. Видео снято так, чтобы создать ощущение реальности происходящего.

Затем поступает звонок якобы от сотрудника спецслужб. Он сообщает, что передача координат важного городского объекта может трактоваться как помощь в организации теракта, и начинает угрожать уголовной ответственностью за отправку геопозиции.

Дальше, чтобы «избежать проблем», человеку предлагают «доказать свою лояльность» и «помочь» правоохранительным органам:

- Показать на камеру квартиру
- Открыть банковские приложения — свои и родителей — и перевести либо снять со счета деньги
- Найти дома наличные и украшения, подготовить их для «изъятия» — и передать курьеру (им оказывается один из мошенников, который играет роль «сотрудника полиции в штатском»)

Никаких взломов банковских приложений и счетов здесь нет — жертва отдает деньги и ценности добровольно. Схема держится на психологии: человек верит, что уже совершил что-то опасное, и пытается «исправить» ситуацию через содействие «органам». Времени осмыслить происходящее

нет: преступники давят на то, что действовать нужно срочно — иначе будет поздно.

Критический момент в этой ситуации — первая угроза по телефону. Если сразу положить трубку и не продолжать диалог, схема рассыпается.

Помните, что настоящие силовики не проводят «оперативные мероприятия» через мессенджер и СМС, не требуют геолокацию и не присылают курьеров за наличными.
Не выполняйте указания неизвестных, кем бы они ни представлялись. Помните: сотрудники правоохранительных органов могут позвонить только для того, чтобы пригласить в подразделение для личной беседы. И уж точно не будут запугивать и угрожать. Блокируйте таких людей и не вступайте с ними в диалог.

Схема 2. Доверенность через Госуслуги и опасный «безопасный» счет

Вторая схема сложнее и выглядит примерно так. Жертве — обычно это человек пенсионного возраста — звонит неизвестный и представляется следователем. Сухие формулировки и юридические термины, которые он использует, заставляют поверить, что звонок официальный.

Лжеследователь говорит, что в отношении собеседника выявлена утечка персональных данных — и неизвестные уже оформили доверенность для доступа к деньгам на счетах. Эта доверенность якобы уже «висит» в разделе документов на Госуслугах и ждет подписания через приложение Госключ.

Дальше идет подробная инструкция: жертве предлагают зайти в свой аккаунт на Госуслугах, установить Госключ, найти доверенность в разделе с документами (для «достоверности» на ней размещают логотип какой-нибудь госструктуры) и подписать ее, чтобы якобы перехватить доверенность у мошенников и блокировать доступ к банковским картам и счетам.

После подписи начинается вторая часть спектакля. Звонит другой псевдосотрудник полиции и заявляет, что первый звонивший был мошенником — и теперь счета действительно в опасности.

Решение, которое предлагают жертве:

- Срочно идти в банк
- Снять все деньги со счетов и передать их «сотруднику в штатском»
- Якобы он временно разместит сумму на «специальном безопасном счете»

Другой вариант — собеседника убеждают самостоятельно перевести деньги на «безопасный счет». Злоумышленник просит никому не рассказывать о его указаниях, чтобы «не помешать оперативным действиям». Благодаря этому у аферистов появляется запас времени, чтобы успеть вывести деньги до того, как подоспеет помощь.

На самом деле доверенность, которая дает доступ к банковским счетам и позволяет распоряжаться деньгами, составляют только очно — в банке или у нотариуса. Через Госключ и любое другое приложение для электронной подписи такая доверенность не оформляется.

Многие об этом не знают — и поэтому верят мошенникам.

Помните: ни один документ в Госуслугах не может открыть кому-либо доступ к вашим счетам и деньгам. Мошенники используют электронную «доверенность» как психологический крючок. Деньги жертва передает злоумышленникам самостоятельно: переводом или наличными.

Схема опасна тем, что очень похожа на реалистичный сценарий:

- Мошенники ссылаются на реальный сервис — Госуслуги. Он вызывает доверие. Также они называют реальные факты о человеке: полное имя, дату рождения, адрес прописки.
- «Документ» на Госуслугах действительно есть — злоумышленники подгружают фальшивую доверенность в личный кабинет жертвы. Отправить «доверенность» можно от имени организации или ИП, либо через аккаунт жертвы, украв или подобрав пароль. Чтобы этого не случилось, стоит придумывать сложные пароли, не хранить их в открытом доступе и менять каждые несколько месяцев.
- **Если вы увидели доверенность в своем кабинете на Госуслугах, проверьте раздел «Действия в системе» на предмет несанкционированных доступов и смените пароль.**

Схема 3. Поддельные службы доставки

В этом сценарии мошенники притворяются специалистами известных служб доставки: СДЭК, Яндекс Доставка, Сбермаркет, Delivery Club. Они пишут людям в мессенджерах с поддельных аккаунтов этих сервисов, которые похожи на реальные: мошенники используют такие же логотипы, описания и названия, стилистику общения.

Люди получают сообщения примерно такого содержания: «Ваш заказ готов к доставке, подтвердите адрес» или «Для выдачи посылки оплатите хранение/доплату за вес». Дальше злоумышленники присылают ссылку «для отслеживания».

Но ссылка ведет не на официальный сайт компании, а на фишинговую копию. На странице предлагают ввести:

- Реквизиты карты
- Логин и пароль от интернет-банка
- Одноразовый код «для подтверждения» операции или входа

- В итоге с карты списывают деньги

Более изощренный вариант схемы — к человеку приезжает реальный курьер с коробкой и QR-кодом для оплаты или подтверждения заказа. Получатель сканирует код, попадает на такой же фальшивый сайт и вводит реквизиты карты, включая секретные данные. Дальше — то же самое: деньги уходят на счет мошенников.

Критичный момент — клик по ссылке. Не стоит открывать ссылки из сообщений или переходить на сайты по отсканированному QR-коду. Вводите адрес сайта нужного сервиса вручную или используйте приложение из официального магазина (например, RuStore, Google Play, Galaxy Store, AppStore). Если человек сам вводит адрес сервисов доставки в браузере или пользуется официальным приложением, шансы наткнуться на клон резко падают.

Если Вы стали жертвой преступления, в обязательном порядке необходимо обращаться в полицию по телефону 112 или 02.

Берегите себя и своих близких!

Автор: Михалькова А.Р.