

Осторожно: Мошенники!

Телефонное мошенничество, фейковые магазины, инвестиционные ловушки и блокировка iPhone — злоумышленники становятся всё изобретательнее. Знайте их схемы, чтобы не стать жертвой.

КИБЕРБЕЗОПАСНОСТЬ

ПРЕДУПРЕЖДЕНИЕ



Звонки от имени должностных лиц



Аферисты представляются работниками домофона, нацбанка, коммунальных служб, поликлиники или **правоохранительных органов**. Они действуют в паре и выманивают коды из СМС под разными предложениями.

Первый мошенник

Под видом замены ключей или обновления данных выманивает код из СМС

Второй мошенник

Представляется правоохранителем, пугает обыском и предлагает «временный счёт»

Как распознать телефонного мошенника



Искусственная срочность

«У вас есть только несколько минут!» — давление и спешка лишают возможности подумать



Угрозы и запугивание

Обыск, арест счетов, уголовная ответственность — если не выполнить требования немедленно



«Временный счёт»

Таких счетов не существует. Переведённые деньги вернуть невозможно



Звонки через мессенджеры

Государственные органы не звонят через WhatsApp, Telegram и не требуют переводов



Помните: Никаких временных счетов не бывает. Сотрудники правоохранительных органов не требуют переводов для декларирования денег.

Схема №2

Мошенничество в I n s t a g r a

Мошенники создают красивые профили с привлекательными фото и предлагают товары по ценам значительно ниже рыночных. После получения предоплаты — исчезают и блокируют покупателя.

→ Привлекательная цена

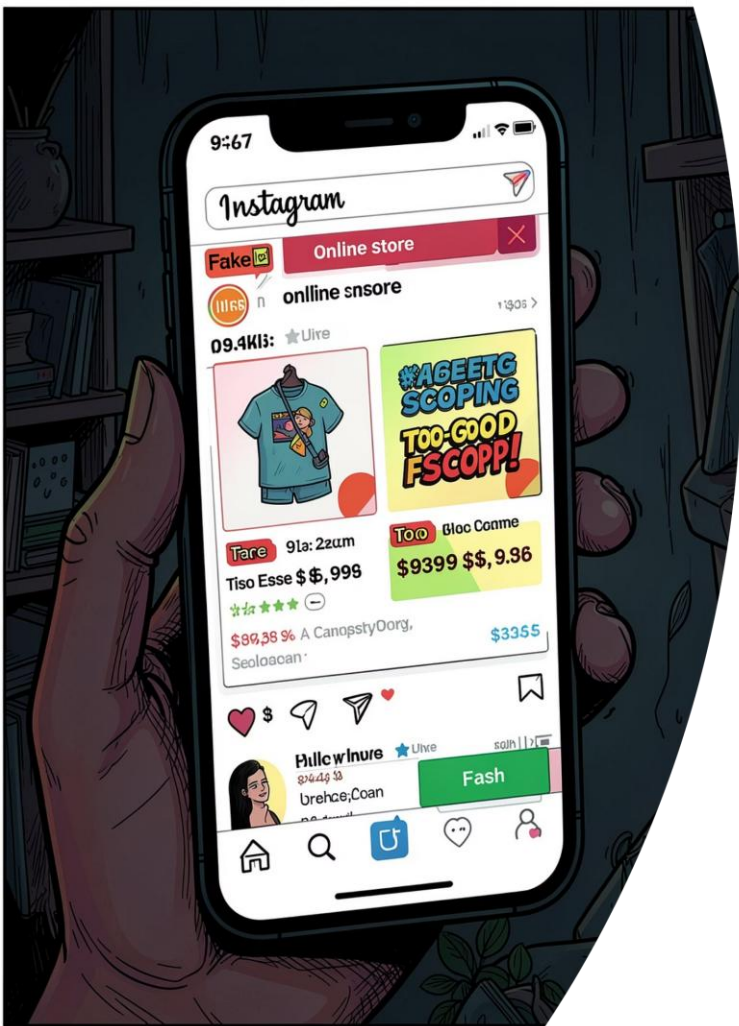
Товары стоят в 2–3 раза дешевле рынка — это первый сигнал опасности

→ Требование предоплаты

Продавец настаивает на полном или частичном переводе до отправки товара

→ Блокировка и тишина

После оплаты покупатель оказывается заблокированным, товар не приходит



«Заработок» на бирже и криптовалюте



Реклама «гарантированного дохода», «прибыльных стратегий» и «обучения у успешных трейдеров» — это заведомо мошеннические предложения.

- ✗ Личный брокер создаёт иллюзию активной работы и высокой доходности. При попытке вывода денег всплывают «комиссии» и «технические проблемы» — в итоге деньги получить невозможно.



Схема №4

Блокировка iPhone через чужой iCloud

Мошенники добиваются того, чтобы жертва **добровольно вошла в чужой iCloud** на своём устройстве. После этого iPhone мгновенно блокируется, и требуется выкуп.

1

Приманка

Призы в TikTok, бонусы в играх, модифицированный Telegram или знакомства в соцсетях

2

Вход в чужой iCloud

Для получения «услуги» просят временно войти в аккаунт, который предоставляют мошенники

3

Блокировка устройства

Злоумышленник дистанционно активирует «Режим пропажи» и требует выкуп за разблокировку

Главные правила безопасности ⚡



Не верьте срочности

Любое давление и угрозы — признак обмана. Возьмите паузу и проверьте информацию



Не платите заранее

Предоплата незнакомым продавцам в соцсетях — прямой путь к потере денег



Нет гарантированного дохода

Обещания быстрой прибыли на бирже — это всегда мошенничество



Не входите в чужой iCloud

Ни при каких условиях не вводите чужие учётные данные на своём устройстве



Будьте бдительны!

Сотрудники правоохранительных и государственных органов не звонят через мессенджеры и не требуют переводов денежных средств для декларирования.

Звонки

Не сообщайте коды из СМС и не переводите деньги незнакомцам

Покупки

Избегайте предоплаты в соцсетях и подозрительно низких цен

iPhone

Никогда не входите в чужой iCloud — это мгновенная блокировка

Подпишитесь на телеграм-канал КИБЕРКРЕПОСТЬ



Для получения информации о новых схемах киберпреступлений и способах защиты подпишитесь на телеграм-канал «КИБЕРКРЕПОСТЬ» с использованием QR-кода, а также путем введения в поисковую строку мессенджера названия телеграм-канала «КИБЕРКРЕПОСТЬ».