



МИНИСТЕРСТВА
ВНУТРЕННИХ СПРАВ
РЕСПУБЛИКИ БЕЛАРУСЬ

УПРАВЛЕНИЕ
ВНУТРЕННИХ СПРАВ
ВИТЕБСКОГО ОБЛАСТНОГО
ИСПОЛНИТЕЛЬНОГО КОМИТЕТА

пр-т Фрунзе, 41-А,
210101, г. Витебск
тел./факс 60 38 36
e-mail: uvb_vitebsk@mvb.gov.by

17.08.26

На №

МИНИСТЕРСТВО
ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

УПРАВЛЕНИЕ
ВНУТРЕННИХ ДЕЛ
ВИТЕБСКОГО ОБЛАСТНОГО
ИСПОЛНИТЕЛЬНОГО КОМИТЕТА

пр-т Фрунзе, 41-А,
210101, г. Витебск
тел./факс 60 38 36
e-mail: uvb_vitebsk@mvb.gov.by

№ 22/5/38048

ад

Государственные органы
и организации
(по списку)

О доведении информации

В последнее время на территории Витебской области участились случаи мошенничества, связанных с использованием торговой площадки «Куфар» и заработком на инвестиционных биржах.

Мошенники могут притворяться покупателями, желающими приобрести ваш товар, размещенный на Куфаре. Они переводят разговор в мессенджеры и там присылают ссылку на то, чтобы «заполнить данные для получения предоплаты». После введения данных карты на **фишинговой странице**, со счета списываются все средства. Далее злоумышленники повторно могут связаться с продавцом, уже именуя себя представителями Службы поддержки Куфара и снова сбросить ссылку для ввода данных карты.

Иные мошенники могут притворяться продавцами, размещая объявление на Куфаре. Они также заманивают пользователей в сторонние мессенджеры, присылают **ссылки** для «перевода средств за товар». После введения данных карты, со счета также списываются все средства. Товар в итоге никто не высылает. Здесь особо уверенные в себе лжепродавцы могут связаться с покупателем еще раз, сообщить, что «товар продали другому покупателю» и якобы хотят вернуть уплаченные средства. Высылает новую **фишинговую ссылку**.

Мошенникам важно перевести общение в мессенджер, так как Куфар отслеживает и блокирует недобросовестных пользователей.

Для общения по сделкам, происходящим на Куфаре, безопаснее использовать только чат Куфара.

Не стоит переходить по ссылкам, присылаемым вам незнакомыми людьми.

Если все же перешли, ни в коем случае не вводите данные ваших платежных карт на страницах, ссылку на которые вам присылают незнакомцы.

Мошенники, которым удалось получить доступ к чужому аккаунту на Куфаре, размещают объявление о сдаче квартиры в аренду. Как только кто-то заинтересовался жильём, переводят общение в мессенджер (Вайбер, Telegram или WhatsApp), ведь там Куфар никак не может **защитить**. Затем мошенник предлагает перевести предоплату за квартиру. В этот момент обязательно стоит насторожиться и задать себе вопрос, а точно ли у него есть квартира или же вы сейчас переводите **деньги незнакомцу, которого даже не видели**. Запомните важное правило: никогда не переводите деньги за квартиру, которую вы лично не осматривали. Если вдруг вы деньги перевели и станете настаивать на том, чтобы вам показали квартиру, мошенник станет утверждать, что кто-то уже перевёл предоплату раньше вас, и поэтому сделка отменяется. Затем предложит вернуть вам деньги и вышлет для этого **ссылку**. Страница может выглядеть как официальный сайт банка или другой надёжной компании, однако ни в коем случае **не вводите на этой странице данные вашей карты**. Если ввести свои данные на такой странице, то возможны ещё большие финансовые потери, так как фишинговая страница предназначена для кражи денег.

Если вам предлагают перейти по ссылке и перевести предоплату за квартиру в аренду, немедленно свяжитесь с **Службой поддержки Куфара** и сообщите об этом, а также вышлите ссылку на объявление, по которому вы откликнулись.

Незнакомый вам человек выходит на связь в мессенджере или в **Инстаграм** и просит вас подать за него объявление за определенное вознаграждение.

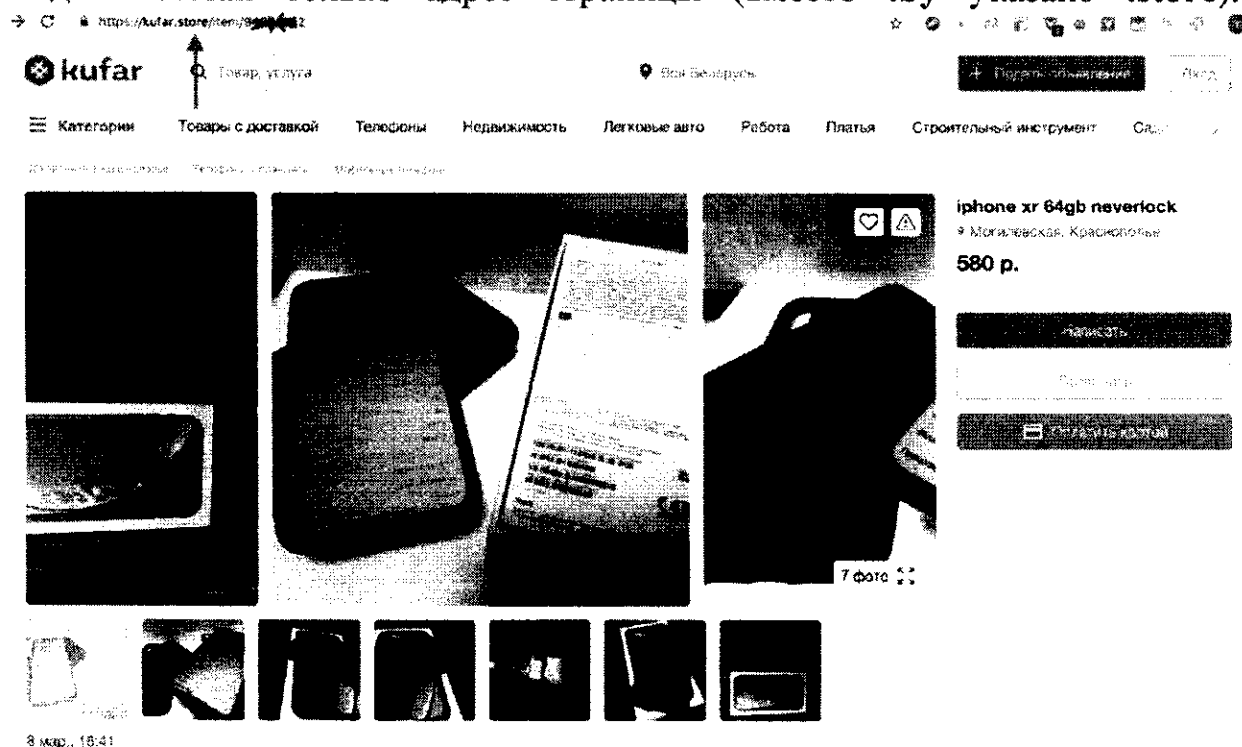
Он передаёт информацию об объекте продажи с описанием, фотографиями, ценой (обычно это дорогие товары с привлекательной ценой), чтобы вы разместили за него объявление на ресурсе Куфар. После публикации объявления мошенник просит передавать контактную информацию покупателей ему. Мошенник связывается с покупателем в **мессенджере**, так как на Куфаре его могут обнаружить и заблокировать. Просит предоплату, скрывается после ее получения.

Размещая чужое объявление у себя в профиле, **владелец профиля несет ответственность** за достоверность информации, указанной в нем. Помогая незнакомому человеку за скромную плату, можно стать соучастником серьезного обмана наивного покупателя.

Мошенники создают страницу, которая визуально очень похожа на страницу реально существующей компании или вовсе идентична ей. Размещают её на сайте, название которого визуально тоже очень

похоже на название реальной компании и имеет лишь незначительные различия. Отправив такую ссылку пользователю, они ждут, когда он введёт на такой странице свои данные. Как только он это сделает, данные окажутся в руках мошенников, и они смогут их использовать по своему усмотрению.

Обратите внимание, как выглядит фишинговая страница, которая маскируется под Куфар, внешний вид абсолютно идентичен Куфару, выдаёт обман только адрес страницы (вместо **.by** указано **.store**):



**Под каким предлогом мне могут выслать ссылку на
фишинговую страницу?**

Фишинговая страница, которая выглядит как интернет-банк. Мошенник под видом покупателя пишет продавцу о желании приобрести товар, а также сообщает, что прямо сейчас забрать его не может. Чтобы продавец гарантированно его оставил, предлагает перевести деньги продавцу немедленно, а для этого спрашивает, какой у него банк и номер карты. После чего сообщает, что нужно подтвердить перевод, высылает ссылку на поддельную страницу, выглядящую как интернет-банк, где пользователю предлагается ввести свои данные для входа в интернет-банк, а затем ввести код из смс. Если пользователь введёт свои данные, то мошенник сможет от его имени зайти в интернет-банк и перевести деньги куда угодно.

Фишинговая страница, которая выглядит как Куфар. Мошенник размещает объявление о дорогостоящем товаре по привлекательной цене. Пишет в объявлении, что связь только через мессенджер

(Viber, WhatsApp, Telegram), после чего получает телефоны заинтересованных пользователей в личные сообщения. Пишет им в мессенджере, что готов продать товар, но так как находится в другом городе, то вышлет вещь через Куфар Доставку. После чего высылает ссылку на страницу, которая выглядит совершенно так же, как Куфар, и на которой предлагается ввести свои данные карты для оплаты за товар. Если доверчивый пользователь вводит свои данные, то мошенник с их помощью переводит деньги с карты пользователя на свой счёт.

Также обязательно нужно убедиться в том, что у вас есть реальный номер телефона продавца. Для этого нужно спросить его у продавца, если он не указан в объявлении, а потом позвонить на этот номер, чтобы убедиться, что он реален и принадлежит именно пользователю, с которым вы совершаете сделку.

Бывают случаи, когда по просьбе покупателя продавцом предоставляется несуществующий номер телефона под предлогом того, что номер пока недоступен (в ремонте, нет денег и т.д.).

Ни в коем случае не отправляйте деньги до тех пор, пока не пообщаетесь с продавцом по телефону.

Схемы с инвестиционным мошенничеством часто выглядят убедительно. Человеку предлагают заработать на бирже, криптовалюте, акциях, валюте, нефти, золоте, международных рынках или инвестиционной платформе. Реклама обещает высокий доход, быстрый результат, помощь личного аналитика, обучение с нуля, гарантированную прибыль. Сначала человеку предлагают внести небольшую сумму денег. Затем показывают в личном кабинете красивый график и якобы рост прибыли. Потерпевший видит, что баланс увеличивается, и начинает доверять. Ему звонит «аналитик», объясняет, какие сделки выгодные, советует внести больше денег. Потом человек пытается вывести прибыль, но ему говорят: «Нужно оплатить комиссию», «Нужно заплатить налог», «Нужно пройти верификацию», «Нужно заплатить налог», «Нужно внести страховой депозит», «Нужно разблокировать счет».

Это один из главных признаков инвестиционного мошенничества: чтобы вывести якобы заработанные деньги, от вас требуют внести еще деньги.

Нормальная инвестиционная деятельность не строится на переводах на карты физических лиц, личных сообщениях в мессенджере и обещании гарантированной прибыли. На финансовых рынках не бывает высокой доходности без риска.

Особенно осторожно нужно относиться к ситуациям, когда вам предлагают установить приложение, включить демонстрацию экрана, передать доступ к телефону, зарегистрироваться по ссылке, купить

криптовалюту под руководством неизвестного человека или перенести деньги на иностранные реквизиты.

В целях своевременного информирования об актуальных киберугрозах УПК КМ УВД в мессенджере Telegram ведется профилактический Telegram-канал «Цифровая грамотность».

Подключиться к Telegram-каналу «Цифровая грамотность» можно воспользовавшись ссылкой: <https://t.me/cifgram> или используя QR-код:



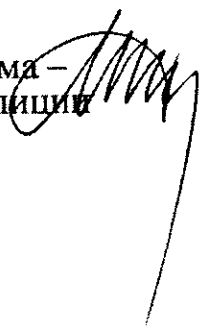
Прошу оказать содействие в доведении тематической информации работникам, что позволит не стать очередной жертвой мошенников.

О проделанной работе просим сообщить в наш адрес.

Приложение: электронный файл профилактической листовки.

С уважением,

Заместитель начальника
УВД Витебского облисполкома –
начальник криминальной милиции



А.Н.Краско