Прокуратура Тарасовского района информирует о способах мошенничества в сфере инвестиций и дополнительного заработка

Предлагают вложить деньги и получить прибыль до 250% годовых? Не спешите переводить сбережения: скорее всего, под маской сотрудников инвестиционной или брокерской компании скрываются финансовые аферисты. Рассказываем, как их распознать и не потерять свои деньги.

Схемы аферистов с инвестициями

Инвестиционные мошенники — хорошие психологи, которые знают, как вызвать интерес, расположить собеседника к себе и убедить человека расстаться с собственными сбережениями.

Часто для обмана злоумышленники создают сайты, которые сложно отличить от настоящих сайтов банков и брокерских компаний. А еще выкладывают посты в соцсетях от имени вымышленных людей или выступают под видом компетентных экономистов, рекламируя подозрительные инструменты с высоким доходом.

Прежде всего в таких предложениях должна насторожить высокая доходность: от 30% до 250% годовых и выше.

Первый шаг этой схемы — заставить человека зарегистрироваться на сайте. Второй — пополнить виртуальный счет, то есть перевести деньги.

Но первое время все выглядит по-настоящему. К начинающему инвестору подключают «опытного» экономиста, который дает советы: как выгоднее распорядиться деньгами и во что инвестировать. Цель у наставника одна — вытащить у клиента как можно большую сумму. Поэтому вначале «доход» на виртуальном счете растет, якобы от удачных инвестиций. Но все это — фейковая информация, а деньги на самом деле находятся у злоумышленников.

Иногда, чтобы вызвать доверие, жертве действительно поступает на карту небольшая сумма — якобы дивиденды с акций. Но это всего лишь еще одна наживка.

Если человек пытается вывести вложения или откажется инвестировать больше, мошенники стараются давить сильнее: рисуют перспективы обогащения, предлагают взять кредит и продать имущество ради быстрого заработка.

Но даже если человек продолжит настаивать на своем и потребует вернуть деньги, сделать это вряд ли получится. Мошенники могут объяснить это высокими комиссиями, которые «съели» всю сумму, или просто перестанут выходить на связь.

Как распознать аферистов:

Схемы у инвестиционных мошенников примерно одинаковые. Распознать их помогут эти 8 базовых факторов:

Обещают высокий доход за короткий срок, например, 50% за два месяца.

Настаивают на немедленном перечислении денег.

Общаются непрофессионально, порой несдержанно и грубо.

Требуют доступ к личному счету, электронному кошельку или карте.

Действуют от имени известных банков и инвесткомпаний, но отношения к ним не имеют.

Рекомендуют установить сторонние приложения.

Настаивают на получении займов, чтобы продолжить инвестировать.

Сайт выполнен непрофессионально, но на первым взгляд его сложно отличить от сайта настоящей компании.

Как понять, что с вами действительно общается сотрудник банка

Сотрудник банка предложит открыть счет у брокера, работающего по лицензии Центробанка. Список таких брокеров есть на сайте ЦБ

В деталях проинформирует об активах, комиссиях и налоговом вычете

Развернуто ответит на вопросы, не станет давить или настаивать на вложениях в конкретный проект, а тем более — на немедленном переводе денег

Не обещает сверхприбыль и гарантированный доход. Предупреждает о рисках

Не просит перевести деньги на карту или на криптокошелек

Не предлагает общаться в сторонних сервисах видеосвязи и мессенджерах: Zoom, Skype, WhatsApp. Разговор происходит в чате на сайте или в приложении банка, либо по телефону

Никогда не запрашивает данные карты и код из СМС для подтверждения операции

5 правил на случай, когда предлагают инвестировать:

Держите в секрете данные карты, не сообщайте коды из СМС и пуш-уведомлений.

Не переводите деньги незнакомцам.

Не торопитесь. В банке не будут настаивать на быстром пополнении счета.

Проверяйте и перепроверяйте информацию о банке и брокере. Она есть на официальных сайтах банковских учреждений.

При малейшем подозрении на попытку мошенничества прекращайте разговор.

Что делать, если данные попали к мошеннику:

Если все же мошенникам удалось завладеть данными карты, обратитесь в службу поддержки банка или заблокируйте карту самостоятельно в банковском приложении.

Блокировка карты поможет сохранить оставшиеся деньги.

Помощник прокурора
Граур В.В.

Прокуратура Тарасовского района информирует о способах мошенничества в мессенджере «МАХ»

Мошенническая схема с мессенджером Max и кража аккаунтов на Госуслугах

В СМИ появились сообщения о новой схеме мошенничества, в которой злоумышленники используют российский мессенджер Max (был назначен национальный мессенджер в июле) для получения доступа к аккаунтам пользователей портала «Госуслуги». Мошенники звонят жертве, представляются сотрудниками Max и под предлогом «дополнительной защиты» просят продиктовать СМС-код, якобы для активации аккаунта. На самом деле это код подтверждения входа на Госуслуги. Получив его, злоумышленники получают доступ к учётной записи и могут похищать персональные данные или оформлять кредиты на имя пользователя.

Как это работает:

Звонок с неизвестного номера с предложением зарегистрироваться в «национальном мессенджере» Max.

Убеждение пройти «активацию аккаунта безопасности» для защиты личных данных.

Запрос СМС-кода, якобы присланного Max, который на самом деле приходит от Госуслуг.

Пострадавшим внушают, что код из СМС связан с регистрацией в Max, хотя на самом деле это одноразовый код от Госуслуг. Несмотря на заявления об интеграции сервисов, официально она пока не реализована.

Социальная инженерия и фишинг в схеме

Мошенники применяют методы фишинга (voice-phishing) и социальной инженерии, опираясь на:

Имитацию государственной принадлежности. Преступники подчеркивают, что Max – это национальный «государственный» мессенджер, якобы тесно интегрированный с другими госуслугами, включая портал «Госуслуги». Это используется для повышения доверия жертвы и снятия подозрений: «раз мессенджер государственный, значит всё официально».

Создание ощущения срочности. Пользователя убеждают, что нужно срочно защитить аккаунт.

Притворство службой поддержки. Звонящий представляется сотрудником Max или Госуслуг.

Использование техноязыка. Жертве говорят о «проверке безопасности» или «двойной защите».

Сценарий построен на реальных новостях и предполагаемой связи Max с госструктурами, что делает обман особенно правдоподобным для неподготовленных пользователей.

Помощник прокурора
Граур В.В.