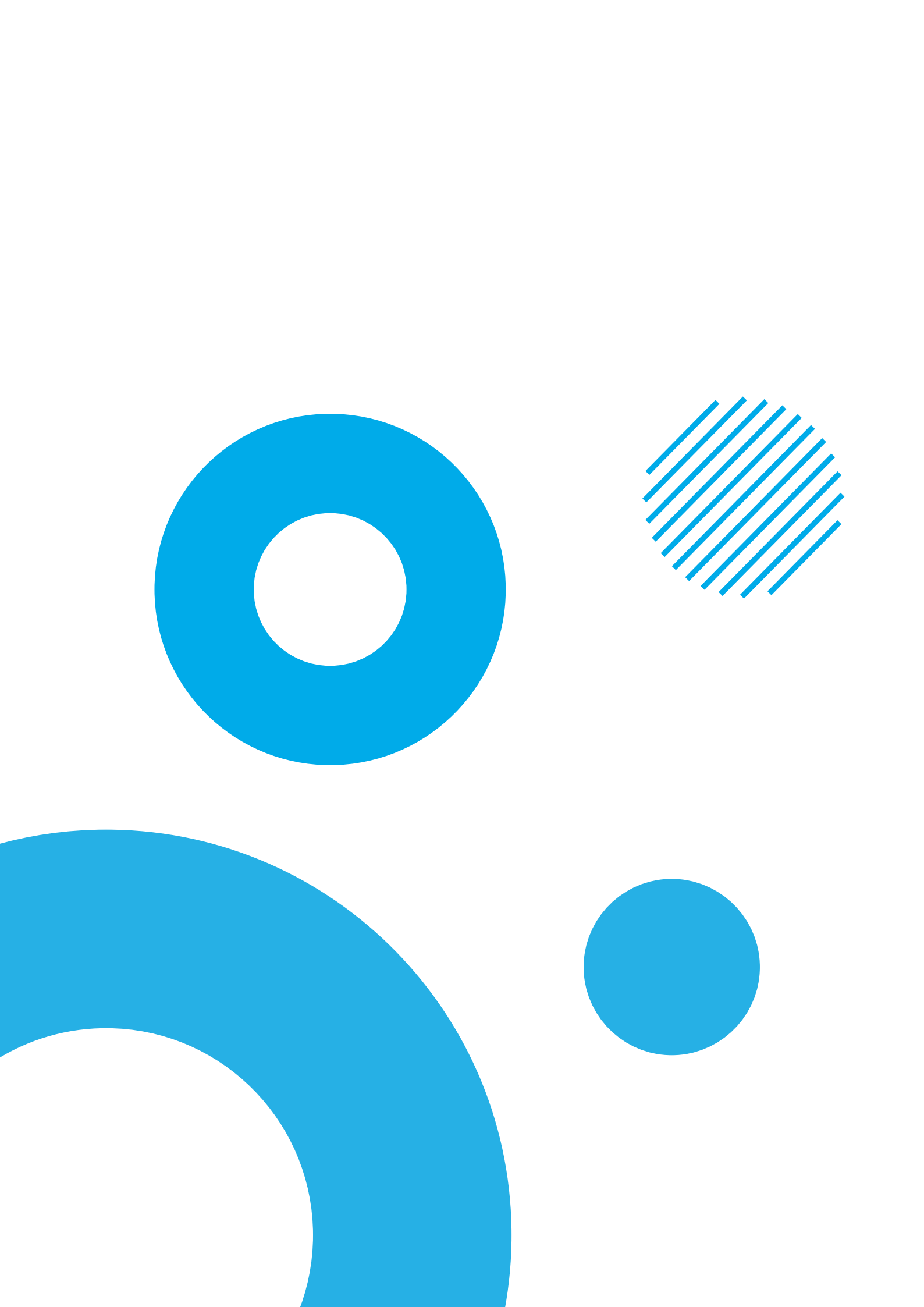
ЦИФРОВОЕ МОШЕННИЧЕСТВО С КРИПТОВАЛЮТОЙ

Криптовалюта – это специальная цифровая валюта, которая существует только в виртуальном виде. У многих пользователей криптовалюта ассоциируется с прибылью, заработком и инвестицией. Любая криптовалюта имеет определенную ценность, чем пользуются мошенники.

Фальшивые биржи

- **Фальшивые биржи – это мошеннические копии реальных криптовалютных бирж,** где пользователи продают и покупают криптовалюту. Как правило, мошенники подделывают мобильные приложения, но вы также можете встретить целые программы или сайты-подделки. Будьте осторожны, потому что некоторые фальшивые биржи очень похожи на оригинальные. Их цель – украсть ваши деньги.
- **Фальшивые биржи привлекают криптотрейдеров** (людей, которые торгуют криптовалютой) и инвесторов, предлагая бесплатные криптовалюты, низкие цены, низкие комиссии на торговлю и даже подарки.
- **Чтобы избежать мошенничества** на поддельной бирже, **тщательно проверяйте** адрес сайта, обращайте внимание на детали и соблюдайте правила защиты от фишинга.

Обязательно проверяйте информацию о разработчике, количестве загрузок, читайте обзоры и комментарии!



Осторожно, шантаж!

- **Шантаж – это метод, часто используемый мошенниками,** при котором жертвам угрожают раскрытием конфиденциальной информации, если они не выполнят требования преступников. Очень часто мошенники требуют заплатить им именно криптовалютой.
- **Шантаж заключается в том, что мошенники либо находят, либо подделывают конфиденциальную информацию** о вас и используют ее, чтобы принудить вас отправить им криптовалюту или деньги в другой форме.
- **Лучший способ избежать вымогательства – тщательно выбирать учетные данные для входа,** следить за сайтами, которые вы посещаете в Интернете, и за тем, кому вы передаете свою информацию. Также разумно использовать двухфакторную аутентификацию, если это возможно. Если информация, которой мошенники вас шантажируют, поддельная, и вы это знаете, проблем получится избежать.

Мошеннические раздачи

- **Мошеннические раздачи используются для того, чтобы выманить у вас криптовалюту,** предложив что-то бесплатно в обмен на небольшой взнос. Обычно мошенники просят вас отправить средства на некий кошелек, чтобы вы могли получить обратно бóльшую сумму (например, «отправьте 0.1 BTC и получите 0.5 BTC»). Но если вы переведете криптовалюту, то ничего не получите и больше никогда не увидите свои средства.
- **Существует множество вариантов мошенничества с фейковыми раздачами.** Вместо биткоина мошенники могут просить другие криптовалюты. В некоторых случаях они могут запросить и другую конфиденциальную информацию. Мошеннические раздачи все чаще появляются в социальных сетях.
- **Лучший способ избежать мошенничества в виде фейковых раздач – никогда не участвовать в розыгрышах,** где вам нужно сначала отправить деньги. По условиям честных акций с вас не будут требовать средства.

Фишинг в социальных сетях

- **Мошенники создают учетную запись будто бы от лица человека,** обладающего большим авторитетом в мире криптовалют (такой метод также известен как «присвоение личности»). Затем они объявляют о фейковых раздачах через рассылки или личные чаты.
- **Лучший способ избежать мошенничества с помощью фишинга в социальных сетях – проверять, на самом ли деле человек тот, за кого себя выдает.** На некоторых платформах социальных сетей есть индикаторы подлинности, например, синие галочки и т.д. Однако на некоторых ресурсах эти индикаторы могут стоять и на фальшивых страницах.

Вредоносные программы. Вирусы

- **Вредоносные программы перехватывает данные** из вашего устройства, и, если вы не будете осторожны, то отправите деньги напрямую злоумышленникам.
- **Вредоносные программы используют фактор перевода криптовалюты друзьям.** Как обычно, мошенник отправляет вам адрес своего кошелька, чтобы вы могли скопировать его и вставить в специальное приложение. Однако, если на вашем устройстве установлен вирус, то вместо адреса кошелька своего приятеля, вы отправите деньги на адрес кошелька злоумышленника.

Финансовые пирамиды

- **Финансовые пирамиды – это инвестиционная стратегия, при которой прибыль предыдущим вкладчикам выплачивается за счет денег новых вкладчиков.** Когда мошенник больше не может привлекать новых вкладчиков, деньги перестают поступать. Финансовые пирамиды бывают и в мире криптовалюты.
- **Лучший способ избежать финансовой пирамиды – тщательно изучить криптовалюту, которую вы планируете купить.** Если стоимость криптовалюты зависит от появления новых инвесторов, участников или вкладчиков, то, скорее всего, перед вами финансовая пирамида. Избегайте участвовать в таких покупках!

Вирусы-вымогатели

- **Вирусы-вымогатели – это такие вирусы, которые блокируют какие-нибудь функции устройства пользователя или блокируют само устройство.** После этого пользователь может получить сообщение о том, что для разблокировки устройства ему нужно перевести мошенникам деньги или криптовалюту. Нет гарантии, что злоумышленники выполнят свое обещание, если пользователь согласится и отправит им выкуп.
- **Чтобы защититься от вирусов-вымогателей, будет полезным настроить на устройстве резервное копирование данных.** Это позволит вам восстановить устройство в случае, если оно будет заблокировано или если вирус удалит какие-либо ценные данные.

Полезные советы

- **Тщательно следите за безопасностью всех ваших устройств.**
- **Остерегайтесь подозрительных сообщений** и электронных писем, которые могут содержать зараженные файлы или опасные ссылки.
- **Обратите внимание на сайты, которые посещаете,** и на программы, которые устанавливаете на свои устройства. Не пренебрегайте антивирусом и своевременными обновлениями операционной системы.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт ligainternet.ru

СЛЕДСТВЕННЫЙ ДЕПАРТАМЕНТ МВД РОССИИ

СЛУЖИМ РОССИИ, СЛУЖИМ ЗАКОНУ!