Цифровой тенге как «приманка»: новая схема мошенников

Каждый день мы все меньше пользуемся наличными – и все чаще доверяем экрану смартфона. Переводы по номеру телефона, маркетплейсы, инвестиционные приложения, «выгодные предложения» в мессенджерах. Цифровая среда стала удобной. Но вместе с удобством выросли и риски.

Сегодня финансовое мошенничество все чаще происходит не на улице, а в чате, по видеосвязи или через якобы инвестиционный фишинговый сайт. Разберем ключевые цифровые схемы и отдельно остановимся на спекуляциях вокруг цифрового тенге.

«Инвестиции» в цифровой тенге: как мошенники используют государственный проект

В последние месяцы участились случаи, когда гражданам предлагают вложиться в «новый государственный инвестиционный проект», «платформу цифрового тенге» или «официальную программу от Нацбанка» с гарантированной доходностью 50-100% в месяц или даже в неделю.

Здесь важно четко понимать, что Цифровой тенге – это государственный проект, реализуемый Национальной платежной корпорацией и Национальным Банком Казахстана. Это форма национальной валюты в цифровом виде (ЦВЦБ), равная обычному тенге. Он не является инвестиционным инструментом и не предназначен для получения прибыли.

Цифровой тенге создается как инструмент расчетов: оплаты товаров и услуг, переводов, социальных выплат. Это еще одна форма денег, а не актив для спекуляций. Его не «продают» через сторонние сайты и не предлагают «купить на старте».

И самое главное – государственные организации в целом не реализуют инвестиционные проекты и не привлекают для них средства от населения.

Сценарий мошенников построен на сочетании трех факторов: доверие к государству, страх упустить выгодную возможность и обещание высокой прибыли (до 100% в неделю) без риска. В результате потенциальному инвестору показывают личный кабинет с «ростом дохода» и даже могут в первый раз сделать минимальную выплату. После чего злоумышленники предлагают внести еще больше средств, демонстрируют якобы высокую доходность, а затем связь обрывается – обычно в момент попытки вывода средств. Стоит помнить, что гарантированная высокая доходность – главный маркер мошенничеств. В финансовой сфере высокая прибыль всегда связана с высоким риском. Без исключений.

Если вам предлагают заработать на «росте цифрового тенге» – это не инвестиция, а попытка мошенничества!

Реклама лже-инвестиционных проектов довольно часто появляется в социальных сетях, а в комментариях можно обнаружить множество однотипных хвалебных отзывов. Кстати, большинство ссылок на якобы инвестиционные сайты ведут на сомнительные порталы, которые не находятся в казахстанской интернет-зоне и имеют домены: .com, .net, .xyz, .top, .info, .vip, .online. Кроме того, мошенники зачастую пытаются подделать реально существующие сайты и площадки. И это еще один фактор, на который стоит обратить внимание.

Фишинговые сайты: копия, которая может стоить вам денег

Представьте: приходит сообщение о подозрительной операции. Внутри — ссылка «для срочной отмены». Пользователь переходит на сайт, который выглядит как страница банка: логотип, дизайн,

привычные кнопки. Разница — в одной букве в адресе. Либо наоборот, очень длинный адрес, например, login.имябанка.invest.com.

Дальше все происходит быстро. Пользователь вводит номера карты, срок действия, CVV-код, SMS-подтверждения – и деньги списываются уже по-настоящему. Фишинг работает потому, что создаёт ощущение срочности и угрозы. В состоянии тревоги люди меньше проверяют детали. А именно детали — главный ориентир безопасности. Кстати, если перед вводом логина, пароля или реквизитов сайт не имеет защищённого соединения (начинается не с https://), закрывайте его.

Аналогичные схемы могут быть связаны и с торговыми площадками. Мошенники рекламируют товары по сильно заниженной цене, предлагают различные акции, подарки и программы лояльности. А всё для того, чтобы усыпить бдительность и получить перевод от не разобравшегося в деталях покупателя.

Кстати! Здесь мошенники также могут использовать лже-информацию о цифровой валюте!

Это может быть сообщение на портале о том, что все сделки якобы защищены цифровым тенге, а их легитимность контролирует государство. Такие сообщения не несут юридической силы и направлены лишь на одну цель – усыпить бдительность жертвы и добиться от нее перевода средств.

Кроме того, фишинг может не иметь цели заполучить деньги здесь и сейчас, а рассчитан на получение личных данных и другой информации о пользователе. И уже в последующем мошенники будут применять эту информацию в иных схемах.

Помните, что фишеры не ограничиваются одним конкретным доменом – они могут маскировать сайт под любое популярное имя в любой доменной зоне, главное, чтобы он выглядел правдоподобно. Хорошая привычка — проверять домен дважды, прежде чем вводить важные данные. Мошенники активно используют как национальные зоны, так и международные домены для подделок, поэтому важно обращать внимание не только на название сайта, но и на его адрес в целом.

Базовые правила цифровой финансовой безопасности

- Не инвестируйте в проекты с гарантированной высокой доходностью.
- Прежде, чем инвестировать в проект, проверьте его, в том числе и по списку сомнительных организаций: https://www.gov.kz/memleket/entities/ardfm/documents/details/318075?lang=ru
- Не передавайте банковские карты и доступ к счетам третьим лицам.
- Никогда не сообщайте коды из SMS и push-уведомлений.
- Не переводите деньги на «безопасные» или «резервные» счета по звонку.
- Проверяйте адрес сайта перед вводом данных.
- Подключите двухфакторную аутентификацию и установите лимиты на операции.
- При сомнении завершите разговор и самостоятельно перезвоните в банк по официальному номеру.

Цифровая экономика делает финансы быстрее и удобнее. Но скорость — союзник не только пользователя, но и мошенника.

Цифровой тенге — это форма национальной валюты, а не билет в мир сверхдоходов. И чем раньше это станет очевидным, тем меньше шансов у тех, кто пытается заработать на доверии.

Материал подготовлен при помощи www.fingramota.kz