

Он подчеркивает – вся информация об официальных трейдерах есть на сайте Центробанка. Те, кто имеет разрешение и работает на рынке годами, всегда отмечают, что инвестиции – это долгосрочная история, а не быстрый способ обогатиться за месяц.

Поддельные сайты по продаже автомобилей и схемы на «Авито»

– Мошенники активно используют любую информационную волну. В этом году, после новостей о повышении утильсбора и росте цен на автомобили, люди бросились искать машины по выгодной цене.

Злоумышленники стали делать копии реально существующих сайтов по продаже автомобилей.

Всё то же самое, только другие контакты, – продолжает Олег Русин.

Человек видит знакомый сайт, оставляет заявку, его переводят в мессенджер. Там «менеджер» объясняет условия, требует предоплату, скидывает договор. Человек подписывает документы, переводит деньги – и остается ни с чем.

– Схема работает безотказно, жертвами становятся даже опытные пользователи. Человек ориентируется на сайт и отзывы, но не проверяет, с кем именно ведет переписку. В таких схемах задействованы группы, находящиеся за пределами России, а внутри страны действуют посредники, которые обеспечивают отдельные этапы – связь, прием денег, их дальнейшее движение.

Похожая схема используется и на агрегаторах – крупных сайтах объявлений. Схемы мошенничества на сайтах объявлений также пока остаются массовыми. Человек размещает объявление или откликается на чужое, например, на «Авито», дальше его уводят в мессенджер и там продолжают общение. В одном случае ему предлагают оформить «безопасную сделку» и присылают ссылку, которая полностью копирует интерфейс площадки: те же поля, оформление, логика действий. Он вводит данные карты и код подтверждения – и деньги списываются.

– Предлагают «безопасную сделку», переводят в мессенджер и присылают ссылку. Он вводит данные карты и код, думая, что оформляет сделку, но на самом деле просто теряет деньги. Не надо проводить никаких сделок вне агрегаторов, на сторонних сайтах, – говорит Русин.

Во втором варианте никакой подмены интерфейса нет. Договорились о цене, человек переводит деньги напрямую, после чего продавец перестает выходить на связь. Всё происхо-

РИСУНОК
МАКСИМА СМАГИНА



дит быстро: короткая переписка, реквизиты, перевод. Решение принимается без проверки – не смотрят на дату объявления, историю аккаунта, отзывы, хотя именно эти признаки чаще всего указывают на риск.

– Если объявление появилось недавно, нет отзывов и человек раньше ничего не продавал, нужно быть очень бдительным. На любом ресурсе есть безопасная сделка, и деньги списываются только после получения товара, – отмечает он.

По словам Олега Русина, такие преступления чаще совершаются внутри страны. Суммы в отдельных случаях могут быть небольшими, но за счет количества это остается одной из самых распространенных категорий мошенничества в Интернете.

Курьеры, дропы и сим-боксы

Организаторы мошеннических схем, как правило, находят за рубежом, преимущественно на Украине. Но внутри России действует разветвленная сеть пособников. Это дропы – подставные лица, которые участвуют в мошеннических схемах, принимая на свои банковские карты украденные деньги, обналчивая их или переводя дальше. Управляют ими так называемые дроповоды – вербовщики, которые организуют цепочки передачи денег.

В схемах обмана активно используют поддельные сим-карты – при помощи сим-боксов.

Они позволяют использовать сотни сим-карт одновременно, и звонок выглядит так, будто идет из любого российского города.

Раньше привлечь к ответственности дропов или владельцев сим-боксов было сложно. С 2025 года в Уголовный кодекс внесены изменения. Статья 187 позволяет наказывать за оформление и передачу карт за вознаграждение. Появились статьи за использование сим-боксов.

Теперь пособников мошенников стали задерживать и давать им реальные сроки.

Важно, чтобы человек понимал: риск привлечения к уголовной ответственности превышает возможный заработок, – подчеркивает Олег Русин.

Информация о подозрительных счетах и номерах вносится в электронные базы в режиме реального времени. Если дроп попал в блок, он не сможет открыть карту ни в одном банке страны, отмечает он.

Статистика показывает, что меры работают: за три месяца этого года количество преступлений с использованием IT-технологий на Среднем Урале снизилось почти на 30%. Но окончательная победа над мошенниками зависит от каждого. Бдительность, холодный ум и привычка перепроверять информацию – вот что реально защищает кошелёк и нервы.

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ



Всегда перепроверяйте информацию.

Пришло сообщение от знакомого – позвоните ему по обычному телефону. Не переходите по ссылкам, не сообщайте коды из SMS, не вводите данные карты на сторонних сайтах.



Запомните: сотрудники банков, ФСБ, МВД, Центробанка никогда не звонят с требованиями снять деньги и перевести их на «безопасные счета».

Если вам предлагают быстрый заработок – скорее всего это обман.



На сайтах объявлений не уходите в сторонние мессенджеры, пользуйтесь только встроенной безопасной сделкой.

Проверяйте отзывы и историю продавца. Не переводите предоплату, если не уверены в человеке.



Установите самозапрет на кредиты.

Это бесплатная услуга, которая поможет, даже если мошенники оформят заявку.



Не храните все деньги на одной карте.

Подключите уведомления о всех операциях.



Не поддавайтесь панике.

Мошенники давят на страх и срочность. Любое требование «срочно и тайно» – повод положить трубку и перезвонить в банк или полицию по официальному номеру.



Если вы поняли, что общаетесь с мошенниками, сразу же обращайтесь в полицию.

Номера, с которых вам звонили, заблокируют – это также поможет уберечь и других людей.



Немедленно лично уведомьте банк.

Он имеет право заблокировать подозрительную операцию и начать проверку. Чем быстрее вы это сделаете, тем больше шансов, что мошенники не успеют завладеть вашими деньгами.