



Скаммы – это сайты, на которых перед вами разыгрывается целый спектакль с рисованием денежных цифр на экране. Вам кто-то должен денег, обязан выплатить некую компенсацию, либо предлагают пройти опрос, за который вам положены сотни тысяч рублей.

Откровенные мошеннические проекты рекламируют даже известные блогеры. Поэтому слепо доверять не следует. Текст сводится к тому, что некий сайт хочет отдать вам деньги просто так. На скамах показывают спектакли о том, как по кнопке «ПОЛУЧИТЬ ВЫИГРЫШ» вам начисляют деньги, а вернее – рисуют фантики на экране.

Вам предложат вывести деньги, но сперва потребуют заплатить десятки взносов: закрепительный платеж, неактивированный аккаунт, документы для транзакции и еще десятки предложений и выдуманных услуг. И так по кругу, пока вы не расстанетесь со своими деньгами. Но нарисованные фантики вывести не получится.

ЗВОНКИ ОТ ЯКОБЫ СОТРУДНИКОВ БАНКА

Современные мошенники хорошо вооружены – они обладают знаниями в области психологии, а некоторые – персональными данными о гражданах. Мошенникам известно ваше ФИО и адрес. Фальшивые сотрудники банков пытаются выудить у вас данные банковской карты, для чего по телефону разыгрывается спектакль с несколькими действующими лицами. Ниже приведён один из наиболее типичных примеров.

Вам звонит лицо, представляющее себя сотрудником банка, называет ваши фамилию, имя и отчество и сообщает, что на вас оформили кредит. Далее он просит сверить данные вашей банковской карты. Для отмены операции просит продиктовать номер карты, срок действия и код с обратной стороны.

Данные карты и код из SMS никому сообщать не следует. Об этом финансовые организации информируют в

каждой sms-рассылке. Но многие граждане сообщают, в результате чего происходит списание средств.

Иногда мошенники, войдя в полное доверие гражданина, идут ещё дальше – и заставляют человека оформить кредит в приложении банка, а после чего перевести эти деньги мошенникам.

Никому не передавайте данные карты, не оформляйте кредиты под давлением из страха блокировки карты. Настоящие сотрудники банка звонят крайне редко и не просят секретные данные.

ФИНАНСОВЫЕ ПИРАМИДЫ И ХАЙПЫ



Широко известные многим финансовые пирамиды в интернете принято называть хайп-проектами.

Что отличает пирамиду от инвестиционного проекта? Хайпы предлагают вложить деньги под очень высокие, неправдоподобные, просто фантастические проценты. Вы делаете депозит, а потом якобы выводите больше первоначальной суммы.

Какая бы легенда не была написана на сайтах подобных проектов - это выдумка. Реальной работы там не происходит, отсутствуют любые виды деятельности. Вам расскажут, что вклады идут в разработку инновационных технологий, стартапов, строительство, биржевые торги, криптовалюту и т.д. Важен ваш вклад, а профессионалы якобы сами сделают свое дело. Если друзей по реферальным ссылкам пригласите, будет еще лучше (как и делают адепты финансовых пирамид).



ПРОКУРАТУРА ЧУВАШСКОЙ РЕСПУБЛИКИ

ПРОКУРАТУРА ПОРЕЦКОГО РАЙОНА

Памятка по профилактике бесконтактных хищений



«О наиболее популярных способах хищений, совершаемых с использованием сети Интернет»

Способы хищений, совершаемых с использованием сети Интернет

Современный интернет переполнен информацией о том, как заработать как можно больше денег. Большинству пользователей интернета регулярно приходят письма с просьбой забрать деньги, пишут в социальных сетях, что вы победитель конкурса, в котором даже не участвовали. И вам уже полагается денежное вознаграждение.

Возникает чувство, будто в интернете все готовы отдать деньги просто так, просто потому что вы хороший человек, правда, доверчивый и наивный. Но в этом нет ничего плохого, ведь все успешные бизнесмены в интернете желают научить людей правильному ведению бизнеса. И вы можете создать десятки бизнесов за месяц. Они с радостью научат всему, что знают.

Кто-то просит вложить все ваши сбережения, а взамен обещают сделать финансово свободными. Сказка, не иначе. Как же обстоят дела на самом деле? Реальность же намного суровее: если вам предлагают много денег даром, значит, хотят обмануть.

Ниже поведаем вам о наиболее часто встречающихся схемах хищения денежных средств бесконтактным способом.

МОШЕННИКИ НА АВИТО

Авито – удобная площадка для объявлений, но и там ежедневно встречается обман. Причем, мошенники постоянно придумывают новые способы хищений. Обманывают как покупателей, так и продавцов. Недавно появился обновленный обман на доставке товара из объявления. Это классический фишинг, но им до сих пор удается обманывать людей.

Злоумышленник в данном случае подробно и детально оформляет объявление, указывая причину продажи, например, смартфона: к примеру, хочет купить новый аппарат, а старый

продает. При этом цена занижена в пределах 20-30 %. На такой лакомый кусочек сразу находят покупатели, и начинается процесс сделки. После убедительного разговора с продавцом, подозрений у потенциальной жертвы обычно не остается. Есть важный момент: многие площадки объявлений внутри своего сайта блокируют чужие ссылки, чтобы продавец не увел покупателя в другой мессенджер, и не начал его там благополучно разводиться. Это делается в целях вашей безопасности.

Представим, что план мошенника сработал, и ваша переписка перешла в социальную сеть (WhatsApp, Viber, Telegram и др.), где никакие ссылки уже не блокируются. Там вам покажут липовые фотографии смартфона (фото обычно взяты с других досок объявлений, обрезаны или отредактированы). Ну а дальше вас попросят оплатить доставку телефона.

Тут и начинается все самое интересное, но не для вас. Мошенник присылает ссылку на фишинговый сайт, внешне выполненный как Авито. Адрес «фейкового» сайта будет отличаться, но покупатель, конечно же, не заметит эту неброскую деталь. Для оплаты вы укажете все данные своей банковской карты, нажмете ввод – и все. Ваша карта скомпрометирована, и мошенник быстро спишет с нее деньги.

БИНАРНЫЕ ОПЦИОНЫ



Занимаются этим видом мошенничества так называемые трейдеры. Они создают себе в социальных сетях визуальный образ успешности: вам может показаться, что в жизни этого человека сплошной праздник. Он живёт на берегу океана, ни в чем себе не отказывает, купается в успехе и очень хочет, чтобы вы заработали в интернете и стали таким же. Он уверяет, что научит этому.

Обычно трейдеры завлекают в некие закрытые группы в социальных сетях и говорят, что готовы поделиться с вами

информацией и торговыми сигналами. Доступ в группу платный или свободный, но трейдеру важно, чтобы вы перешли туда по ссылке, которую он даст.

Далее «гуру» подтолкнет вас зарегистрироваться на бинарных опционах с внесением депозита, после чего начнется торговля по его сигналам. Схема обмана с трейдерами проста: он зарабатывает проценты от вашего депозита, но чаще всего наживает именно на проигрышах. Итог всегда один: вы полностью сливаете свой депозит, играя на бинарных опционах.

КАК ОБМАНЫВАЮТ «ЧЕРНЫЕ» БРОКЕРЫ



Стоит однажды оставить на просторах интернета свой номер телефона и с высокой долей вероятности он попадет в базу «чёрных» брокеров. Начнутся регулярные, надоедливые звонки, с предложением поторговать на бирже, похожей на «Форекс». Иногда можно наткнуться на людей, которые якобы будут делать прогнозы на спортивные события и точно указывать выгодные ставки – так называемые «капперы».

Если согласиться так зарабатывать, брокер сначала попросит вложить немало денег. Не беда, если у вас их нет. Вежливые брокеры предложат взять кредит, и даже с плохой кредитной историей помогут это сделать. За вами закрепят некий софт и установят в свой телефон или компьютер. Он объяснит, как завести там аккаунт, вложить свои деньги и начать торги на, к примеру, бинарных опционах. Вы, в свою очередь, видя высокие цифры, подделанные в этой программе, начнете мечтать о покупке квартиры и машины, но фактически все намного печальнее.

В скором времени начнутся просадки с нарастающими процентами потерь. Главная задача персонального менеджера – заставить человека вложить как можно больше денег. Для этого он будет регулярно давить, и уговаривать вложить еще денег, ведь скоро все будет хорошо, и вы якобы выйдете в плюс. Но выгоды вы так и не дождетесь, наблюдая очередной слив своих денег. Вернуть деньги от мошенников будет уже невозможно.