Кибермошенничество

В мире всегда существовали мошенники, которые умудрялись похищать средства и ценности в самых разнообразных масштабах. Постепенная информатизация мира привела к появлению нового вида злодеев – кибермошенников. Сегодня мы разберемся с 10 самыми популярными видами мошенничества, чтобы в будущем защитить себя и свои активы от потерь.

Схема с криптовалютами и ICO

Одним из самых популярных видов мошенничества в последние годы стали махинации с криптовалютами, в частности со сбором средств на запуск проектов в сфере блокчейн. Злоумышленники презентовали якобы хороший проект, на реализацию которого требовались средства. Для этого использовалось так называемое поддельное ICO (Initial Coin Offering). Это формат сбора средств на развитие проектов в сфере криптовалют. Прикрываясь этим инструментом, злодеи продавали фальшивую криптовалюту за биткоин или эфириум, которые имеют реальную стоимость. После нескольких раундов сбора средств «новаторы» пропадали без вести вместе с собранными средствами. При этом отследить их было практически невозможно т.к. всеми собранными средствами можно распоряжаться анонимно. Стоит отметить, что на рынке были и настоящие ICO, но таковых было не более 10-20%.

Совет: для начала изучите рынок криптовалют более детально, прежде чем вкладывать реальные деньги

Фейковые СМС от банка

Злоумышленники присылают на номер жертвы СМС с текстом о том, что ее карта заблокирована. В конце указывается номер телефона, по которому нужно связаться с якобы сотрудником банка. Доверчивый пользователь звонит по номеру и попадает в руки искусного мошенника, выполняя его просьбы и, сам того не замечая, передает свои конфиденциальные данные и деньги в чужие руки.

Совет: никогда и никому не сообщайте свои данные, а также любую банковскую информацию.

Дешевые товары на интернет-досках объявлений и онлайн-магазинах

Человеком часто движет желание сэкономить, чем пользуются коварные злодеи. Они регулярно размещают товары на сайте объявлений по очень выгодной цене, которая может быть на 30-40% ниже среднерыночной. Единственным условием покупки является внесение небольшого аванса на карту. После получения предоплаты исчезает не только «продавец», но и объявление с сайта.

Здесь нужно быть очень внимательным, заказывая товары в новом магазине, который продает по очень выгодным ценам. Очень часто наивные пользователи заказывают товар, внося предоплату и в итоге не получают ни посылки, ни денег. Проверяйте юридический адрес магазина, лицензии и ищите отзывы реальных покупателей.

Совет: если вы на 100% не уверены в честности продавца, то придерживайтесь покупок исключительно наложенным платежом.

Заражение вирусом-вымогателем

По всему миру активно распространяются вирусы-вымогатели, которые попадают на компьютер «жертвы» и зашифровывают все файлы, что ставит под угрозу всю хранившуюся информацию и парализует работу. Чтобы вернуть все ваши документы, вирус выдает сообщение с требованием перевести средства на криптовалютный кошелек, чтобы их невозможно было отследить. Только якобы после этого вы сможете возобновить доступ к файлам. К сожалению, в большинстве случаев вся информация так и остается зашифрованной даже после уплаты «выкупа».

Совет: регулярно обновляйте антивирус на всех своих устройствах.

Установка приложения на смартфон

Практически каждый современный человек пользуется смартфоном. Это еще одно поле деятельности для кибермошенников. Одним из вариантов хищения ваших личных данных является установка зловредных приложений под видом обычных программ.

Совет: никогда не загружайте приложения на телефон из других источников, кроме официальных магазинов приложений Google Play и App Store.

Кибермошенничество в соцсетях

Нужно быть максимально внимательным при участии в различных опросах. Очень часто мошенники проводят опросы под видом одного из популярных банков, предлагая в конце разыграть приз. Чтобы подтвердить получение выигрыша, грабители просят отправить определенную сумму на их счет для подтверждения, что вы якобы являетесь клиентом их банка. Никогда не отправляйте деньги третьим лицам под предлогом участия в розыгрыше призов. Банки никогда не требуют подобных действий.

Еще один способ выудить информацию у доверчивых пользователей - создание поддельных личных страничек с целью знакомства и получения личной информации, которая может послужить доступом к вашим реальным финансам.

Совет: в процессе общения злоумышленник постепенно переходит к более личным вопросам, поэтому будьте осторожны с онлайн-знакомствами и не раскрывайте своих персональных данных в сомнительных опросах в сети.

Обман на фриланс-услугах

Удаленная работа стала источником дохода для десятков миллионов людей по всему миру. Довольно часто можно встретить объявления и целые сайты, посвященные простому и быстрому заработку. Вам предлагается гибкий график, приличное вознаграждение и даже соцпакет. Чтобы начать работу, с вас могут потребовать небольшую плату за обучающие материалы или доступ к заказам. Когда мошенник получит деньги, то скорее всего вы не увидите ни работы, ни обучающих материалов.

Совет: остерегайтесь таких предложений, ведь на большинстве фриланс-бирж начать работу можно абсолютно бесплатно.

Фальшивые интернет-аукционы

Интернет-аукцион является хорошей возможностью купить товар по более низкой цене, но и здесь можно попасться «на удочку».

Совет: прежде чем делать ставки на лот, проверьте рейтинг и отзывы о продавце. На аукционах – это важнейшие показатели честности. Не рекомендуется делать ставки на товары продавцов с маленьким количеством отзывов и сделок или нулевым рейтингом.

Мошенничество с любителями онлайн-игр

Многие дети и даже люди старшего поколения обожают игры. Желание быть лучшим порождает зависимость, которая проявляется в растрате денег на своих игровых персонажей для покупки виртуальных улучшений и предметов. Чтобы сэкономить, многие ищут, где это можно сделать подешевле, наталкиваясь на аферистов, которые берут предоплату, но не предоставляют виртуальные ценности.

Совет: следите за собственными детьми, если они играют в сети.

Мошенничество на бесконтактных платежах

Современные банковские карточки оснащаются чипом, позволяющим совершать быструю оплату, поднося карту к терминалу, который считывает информацию и списывает соответствующую сумму со счета. Теперь подобными устройствами считывания пользуются не только магазины, но и мошенники. Они носят в сумке самодельные портативные терминалы и прислоняются к «жертвам», чтобы украсть деньги с карты.

Совет: чтобы обезопасить себя, установите в лимит на дневные платежи или поставьте необходимость вводить пин-код для подтверждения любых транзакций.