

ИНФОРМАЦИЯ О СПОСОБАХ МОШЕННИЧЕСТВА, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, И ПРАВИЛАХ ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ.

1. Обман потерпевшего при продаже им вещей на интернет- площадке (потерпевший продает имущество).

На торговых интернет-площадках правонарушитель находит объявление, размещенное пользователем о продаже какого-либо имущества, после чего в различных мессенджерах пишет продавцу о том, что хочет его приобрести, однако по различным причинам не имеет возможности приехать лично. Злоумышленник предлагает произвести оплату путем перевода денежных средств на банковскую платежную карту продавца и оформить доставку покупаемого имущества, в связи с чем высылает ссылку на фишинговую (поддельную) страницу сайта, которая чаще всего визуально схожа со страницами служб доставки (Европочта, СДЭК, Куфар Доставка, Автолайтэкспресс и Белпочта), а также интернет-банкинга. В открывшемся окне продавцу предлагается ввести реквизиты своей банковской карты, логин и пароль от интернет-банкинга либо паспортные данные, а также код из смс-сообщения. В это время всю введенную информацию видит злоумышленник и вводит ее на действительном сайте банка или ином ресурсе, получая тем самым доступ к денежным средствам жертвы и совершая их хищение.

2. Обман потерпевшего при покупке им вещей на интернет- площадке (потерпевший покупает имущество).

На торговых интернет-площадках злоумышленник размещает объявление о продаже какого-либо имущества, пользующегося спросом, и преднамеренно устанавливает цену ниже рыночной. Граждане, которых заинтересовало указанное объявление, пишут мошеннику и в ходе переписки последний сообщает, что не имеет возможности *лично встретиться для передачи имущества и предлагает* воспользоваться услугами доставки. Это может быть на условиях:

- полной предоплаты (в таком случае после перевода потерпевшим денег на указанные злоумышленником реквизиты, последний перестает выходить на связь, а товар не высылается);
- оплаты за товар через службу доставки (в данном случае злоумышленник высылает покупателю фишинговую ссылку для заполнения им якобы необходимых реквизитов для оплаты и последующего получения товара по нужному адресу, а в действительности для получения доступа к его денежным средствам).

3. Обман потерпевшего под предлогом оказания помощи от имени банковских работников, операторов сотовой связи, энергетического предприятия, сотрудников правоохранительных органов, учреждений здравоохранения.

На мобильный телефон потерпевшего поступает входящий звонок от злоумышленника. Как правило, при этом последний пользуется сервисом по подмену номера телефона либо использует для осуществления звонка интернет-мессенджер. Далее под различными предложениями (блокировка несанкционированных переводов, оформление посторонними лицами кредитов от имени жертвы, необходимость оказания помощи правоохранительным органам в изобличении преступника, необходимость удаленного подписания договора либо дополнительного соглашения к нему, запись на бесплатную диспансеризацию, участие в рекламной акции и т.д.) мошенник просит жертву назвать отдельные реквизиты банковской карточки либо паспортные данные и сообщает, что высылает в адрес пользователя смс- сообщение с кодом, который необходимо назвать после звукового сигнала. В это время все полученные сведения злоумышленник вводит на

сайте банка, получая доступ к денежным средствам жертвы и совершая их хищение.

Следует помнить, что запрашиваемая преступником информация вышеуказанным реальным сотрудникам не требуется ни при каких обстоятельствах и они не будут узнавать о ней у клиента.

4. Обман потерпевшего под предлогом покупки билетов в кино, театр, саун и пр.

Киберпреступники с фейковых аккаунтов на различных сайтах, представляясь девушками, знакомятся с мужчинами и предлагают продолжить общение в мессенджерах. Для убедительности они направляют собеседникам фотографии и голосовые сообщения, ведут беседы по телефону. Затем мошенники присылают фишинговую (поддельную) ссылку на сайт, например, несуществующего кинотеатра, в котором предлагают провести время. Мужчинам необходимо забронировать места и все оплатить. Потерпевшие вводят реквизиты своих банковских карт, тем самым предоставляя мошенникам полный контроль над своими денежными средствами.

5. Обман потерпевшего под предлогом получения посылки на «Белпочте».

Потерпевшему направляется сообщение о пришедшей посылке, которую можно получить после заполнения недостающей информации, перейдя по ссылке. В реальности же данная ссылка является фишинговой (поддельной), а ввод данных позволяет мошенникам получить доступ к карт-счету и похитить деньги.

6. Обман потерпевшего под предлогом оказания помощи его родственнику или близкому человеку.

На телефон потерпевшего поступает входящий звонок от злоумышленника, который сообщает, что родственник жертвы попал в неприятную ситуацию (например, он участник ДТП). После чего трубку берет якобы врач (следователь, милиционер) и говорит, что срочно нужны деньги на оплату дорогостоящего лечения. Используя эффект неожиданности, мошенники выведывают необходимую информацию, вынуждают оформить кредит и перевести деньги на указанный ими счет либо сообщают, что придет курьер, которому следует передать наличные деньги.

7. Схема «фейк босс».

Внедрившись в рабочие чаты в различных мессенджерах и социальных сетях, используемых гражданами для коммуникации по служебным вопросам, злоумышленники изучают данные участников переписки, содержание сообщений и определяют учетные записи руководителей, после чего создают их копии (фейковые учётные записи) и вступают в личную переписку с иными участниками таких чатов. В ходе переписки, выдавая себя за руководителя, злоумышленник сообщает вымышленные сведения о том, что работником интересовались сотрудники правоохранительных органов и настаивает на сохранении конфиденциальности факта общения. Далее гражданину поступают звонки посредством мессенджеров или телефонной связи от якобы сотрудников правоохранительных органов, а также банковских учреждений. В ходе беседы псевдосотрудники убеждают в необходимости совершения определенных действий, в том числе по перечислению денежных средств под различными мошенническими предложениями.

8. Неожиданные поступления на банковскую карту или номер мобильного телефона.

Мошенники якобы от имени банка (сотового оператора) рассылают SMS-уведомления о пополнении счета, а затем связываются с жертвой и просят вернуть ошибочно зачисленные деньги.

9. Вирусные файлы, картинки, фотографии.

Хакеры применяют технику, позволяющую скрывать вирусы в изображениях. После

скачивания файла (картинки, фотографии) вредоносная программа запускается на компьютере или телефоне жертвы, и злоумышленники получают доступ к устройству и всей хранящейся на нем информации.

10. Операции с криптовалютой.

Мошенники размещают рекламу об оказании помощи при осуществлении различных операций с криптовалютой с высоким процентом доходности. Создают поддельные платформы для торговли криптовалютой, фейковые версии официальных криптокошельков или ботов, которые работают одним из следующих способов:

- как фишинговые (поддельные) страницы, т.е. все указываемые на них данные, такие как пароль от кошелька и фраза для восстановления средств, а также другая финансовая информация попадают в руки к мошенникам;
- как простое воровство, а именно изначально сайт позволяет вывести небольшую сумму денег, что создает впечатление надежности и доходности вложений и направлено на побуждение увеличения жертвой суммы вложений. Однако при последующих попытках вывести средства, сайт либо закрывается, либо отклоняет запрос.

Все вышеприведенные примеры показывают, что мошенники используют фактор неожиданности и создают для жертвы максимально неудобные, ограниченные по времени условия для анализа происходящего.

Рекомендуем соблюдать следующие важные правила:

- не спешить верить всему, о чем говорит позвонивший незнакомый человек;
- не разглашать паспортные данные, логины, номера телефонов, пароли, ПИН-коды, реквизиты банковских карточек, расчетных счетов и прочей информации третьим лицам;
- проверять информацию, позвонив по официальному номеру организации, представителем которой назвался позвонивший человек;
- убедиться, с реальным ли человеком ведется общение, перезвонив ему по Номеру из своей записной книги;
- оплачивать товары, приобретенные на интернет-площадке только после их получения и визуального осмотра;
- не переводить накопления на расчетные счета физических лиц или криптокошельки;
- при появлении подозрений или в случае, если оказались жертвой мошенников, немедленно обратиться в правоохранительные органы.

Осуществите подписку на региональный телеграм-канал Следственного комитета - «КиберПул» (@cyberpoolofsharks, ID2076885523) и телеграм-канал УВД Брестского облисполкома - «КИБЕРКРЕПОСТЬ» (@CYBER_FORTRES S BREST, ID2460172178):



@CYBERPGOLOFSHARK5



@CYBER_FORT