План-конспект об актуальных способах совершения киберпреступлений для использования в рамках проведения воспитательно-профилактической работы с гражданами

Мошенники постоянно совершенствуют свои схемы обмана, чтобы заполучить ваши деньги. Для связи они могут использовать не только интернет-звонки в мессенджерах, таких как Viber, Telegram или WhatsApp, но также стационарную и мобильную связь, к тому же интернет-видеозвонки. Чаще всего они представляются сотрудниками правоохранительных органов, работниками мобильных операторов, государственных учреждений или банков. Реже они могут выдавать себя за ваших родственников, начальников, брокеров или трейдеров криптобирж.

Количество мошенничеств под предлогом продления договора оказания услуг оператора сотовой связи продолжает расти.

Жертве в мессенджере поступает звонок от неизвестного, который представляется сотрудником оператора сотовой связи. Под предлогом продления договора мошенник предоставляет ссылку, перейдя по которой потерпевший устанавливает на свое устройство приложение удаленного доступа. Стоит отметить, что приложение очень схоже с оригинальным: мошенники устанавливают аналогичный значок, и общий вид приложения на первый взгляд можно принять за настоящее.

В дальнейшем потерпевшему поступает звонок якобы от «сотрудника милиции», который под различными предлогами склоняет потерпевшего оформить кредит и перевести денежные средства на банковские счета, подконтрольные мошенникам.

В то же время информируем, что мошенники осуществляют звонки гражданам и представляются сотрудниками «Водоканала» и «Электросетей».

В ходе беседы злоумышленник предлагает гражданину оставить заявку на замену счетчиков. Также мошенник пытается узнать идентификационный номер паспорта и абонентский номер мобильного телефона.

В случае предоставления потерпевшим запрашиваемых мошенником данных ему в мессенджере поступает звонок якобы от «правоохранителя», который сообщает, что гражданин в настоящий момент разговаривает по домашнему телефону с мошенниками, и требует прервать связь.

В дальнейшем мошенник убеждает, что на человека аферисты оформили кредит. Чтобы исправить ситуацию, гражданин должен сам приехать в банк и лично оформить кредит, а полученные денежные средства перевести на предоставленный безопасный банковский счет

для того, чтобы аннулировать кредит, который был оформлен мошенниками.

В то же время мошенники продолжают обзвоны граждан от имени сотрудников банка и правоохранительных органов, сообщая о возникшей проблеме, и, войдя в доверие, предлагают помощь в ее решении. Например, человеку сообщают, что его подозревают в соучастии в преступлении, в связи с чем необходимо провести обыск и изъять денежные средства. Для их сохранения предлагают перевести наличные на якобы защищенный счет или передать якобы работнику банка для декларирования. Также мошенники могут сообщить, что на жертву оформлен кредит, для аннулирования которого необходимо сообщить свои паспортные данные и реквизиты банковской платежной карты.

Внимание!

Сотрудники милиции и банков не звонят в мессенджерах и не требуют перевода денег для «декларирования» или «освобождения от ответственности», не предлагают участвовать в «спецоперациях» по поимке мошенников.

Сотрудники милиции, банков и операторов сотовой связи не звонят абонентам через мессенджеры.

Никогда не устанавливайте незнакомые приложения по просьбе неизвестных.

Никому не сообщайте свои личные данные, данные банковских карт, коды из SMS!

Не переходите по предложенным ссылкам, предоставленным вам неизвестными лицами.

Не устанавливайте на устройство приложения по рекомендации неизвестных лиц или полученные через мессенджеры.

Мошенничество в Инстаграм с требованием предоплаты — это распространенная схема, которая часто используется злоумышленниками для обмана пользователей. Вот основные аспекты этой схемы:

Мошенники создают фальшивые профили с привлекательными фотографиями, которые могут представлять товары и услуги. Часто используются фотографии из интернета, чтобы создать видимость легитимности.

Злоумышленники предлагают товары или услуги по значительно сниженной цене или проводят акции, которые выглядят слишком хорошими, чтобы быть правдой (например, специальные предложения на популярные товары).

Мошенники покупают рекламу и используют популярные хэштеги, чтобы достичь широкой аудитории и привлечь внимание потенциальных жертв.

Создают привлекательные посты и сториз с яркими изображениями и заманчивыми предложениями.

Мошенники могут создавать фальшивые отзывы и комментарии от фейковых аккаунтов, чтобы создать иллюзию положительного опыта других клиентов.

В ходе общения с жертвой мошенники могут использовать различные тактики, чтобы создать доверие, включая дружелюбное общение и обещания быстрой доставки.

После того как жертва изъявляет желание приобрести товар или услугу, мошенники объясняют, что необходима предоплата для подтверждения заказа, которая осуществляется посредством банковской платежной карты путем перевода денежных средств.

Иногда мошенники могут направлять жертву на поддельные сайты, которые выглядят как настоящие с целью возврата денежных средств из-за проблем с доставкой, где жертве предлагается ввести реквизиты своей банковской платежной карты, однако у жертвы списываются все оставшиеся денежные средства.

После получения денег мошенники прекращают общение, блокируют жертву или могут удалить свой аккаунт.

Как избежать мошенничества в Инстаграм:

Ищите отзывы о продавце в открытых источниках сети Интернет. Обратите внимание на наличие негативных отзывов или предупреждений о мошенничестве!

Ни при каких обстоятельствах не перечисляйте денежные средства до получения товара!

Если цена кажется слишком низкой или предложение слишком хорошим, чтобы быть правдой, это может быть признаком мошенничества.

Мошенники продолжают вымогать деньги за «разблокировку» iPhone.

Знакомство злоумышленника с жертвой чаще всего происходит на тематических сайтах. Затем общение переходит в мессенджер, где новый знакомый под различными предлогами (например, необходимо очень срочно скачать информацию или фото) вынуждает потерпевшего зайти в чужой iCloud со своего устройства. Получив согласие, мошенник высылает логин и пароль, а после входа потерпевшим в «учетку» меняет пароль на iPhone и включает режим пропажи.

В этот момент жертва оказывается в ловушке, так как не может выйти из чужого аккаунта или отключить режим пропажи, iPhone

остается заблокированным и не пригодным к использованию. И тогда аферисты предлагают перевести деньги за разблокировку устройства.

Запомните!

Никогда не авторизуйтесь в чужих «учетках» на своих устройствах, не вводите свои личные данные и пароли на сомнительных сайтах. Используйте двухфакторную аутентификацию и никогда никому не сообщайте свой пароль или коды подтверждения.

Мошенничества под предлогом заработка на бирже не теряют своей актуальности.

Мошенники предлагают поторговать на бирже и инвестировать деньги в ценные бумаги, обещая при этом получение хорошей прибыли в кратчайшие сроки.

Потерпевшему попадается реклама о выгодном инвестиционном проекте в одной из социальных сетей, после чего он оставляет заявку с абонентским номером.

В дальнейшем потерпевшему поступает звонок от личного брокера, который будет вести его по ходу всего проекта.

Жертва переводит средства личному брокеру, который якобы регистрирует личный кабинет, создает иллюзию активной работы и высокой доходности. Но при попытке жертвы вывода денег всплывает множество причин, по которым вывод невозможен. Также потерпевшему по различным причинам (таким как оплата комиссии) предлагается перевести еще большую сумму денежных средств — «комиссия», после оплаты которой выясняется, что деньги получить нельзя, так как клиента якобы подозревают в мошенничестве.

На что стоит обратить внимание, чтобы избежать обмана?

Остерегайтесь слишком выгодных предложений: если что-то кажется слишком хорошим, чтобы быть правдой, скорее всего, это мошенники.

Не передавайте личные данные: никогда не делитесь своими финансовыми данными или паролями с незнакомыми людьми.

Действуйте осторожно: не спешите с инвестициями, особенно в том случае, если вас подталкивают к быстрому принятию решений.