ОТДЕЛЕНИЕ ПО ПРОТИВЛДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

УПРАВЛЕНИЕ ВНУТРЕННИХ ДЕЛ ОРШАНСКОГО РАЙОННОГО ИСПОЛНИТЕЛЬНОГО КОМИТЕТА

ПЛАН-КОНСПЕКТ

проведения профилактического выступления

по линии противодействия киберпреступности

ТЕМА: «Актуальные способы совершения киберпреступлений»

г. Орша, 2025

На территории Оршанского района отмечается совершение значительного числа преступлений в информационной сфере, в частности – совершение хищений денежных средств путем модификации компьютерной информации или путем обмана (мошенничества). Как показывает проведенный анализ, основным условием совершения преступлений данной категории, является безответственное отношение самих потерпевших к сохранности персональных данных.

Одной из причин такого поведения, является низкий уровень цифровой грамотности населения.

Мошенники регулярно меняют свои схемы обмана, преследуя одну лишь цель — похитить деньги. По прежнему являются актуальными телефонное мошенничество (вишинг).

Наиболее распространенной в настоящее время схемой такого обмана являются звонки от имени оператора связи («МТС» или «А1»).

В большинстве случаев мошенники звонят через мессенджеры (Telegram, WhatsApp, Viber) и представляются специалистом оператора связи. Они предлагают дистанционного продлить договор на оказание услуг электросвязи или срок действия сим-карты или тарифа, которые заканчиваются буквально сейчас. Все это предлагается осуществить дистанционно, что бы не тратить время на посещение офиса оператора связи. Для это мошенники предлагают установить поддельное приложение, имеющее схожее название с оригинальным («Мой МТС» или «Мой А1»). Для этого, в том же мессенджере, жертвам направляется файл в формате *.арк. Если пользователь запустит данный файл, то на его мобильном телефоне установится «фейковое» приложение, которое дает мошенникам доступ к данным на устройстве: логинам и паролям, кодам из смс, к фото, сообщениям и другой информации. Используя полученные данные с мобильного телефона, мошенники могут оформить онлайн-кредит на доверчивого пользователя и похитить его денежные средства.

Следует помнить, что все договора, тарифы и сим-карты бессрочны, сотрудники мобильных операторов не звонят абонентам через мессенджеры и не требуют изменить пароли под диктовку. Если Вы получили звонок через любой мессенджер якобы от оператора — прервите разговор и самостоятельно обратитесь в офис Вашего оператора для проверки информации. Никогда не устанавливайте приложения по ссылкам, полученным через мессенджеры из неизвестных источников.

Если мошенники получают доступ к мобильному устройству и человек легко делиться с ними конфиденциальной информацией, то они продолжают разыгрывать свой план.

В дальнейшем, как правило, с потерпевшими связывается сотрудник правоохранительных органов или банковского учреждения. Мошенники пытаются убедить граждан в том, что на их оформляется кредит в одном из банков и с целью сохранения денежных средств, а также разоблачения недобросовестных сотрудников банковской сферы, убеждают перевести свои денежные средства на «защищенный счет», либо оформить кредиты на собственное имя, для последующего перевода денежных средств на счета злоумышленников.

Например, в текущем году одна из местных жительниц, в результате общения с сотрудником компании «МТС» в мессенджере «WhatsApp» изначально предоставила свои персональные данные и установила «фейковое» приложение, потом пообщалась с сотрудником финансовой милиции, который убедил оршанку, во избежание конфискации денежных средств во время обыска, «задекларировать» их путем пополнения личного расчетного счета. После выполнения данной просьбы, мошенники имя доступ к мобильному телефону жертвы, осуществили вывод 26 000 рублей.

Также одним из самых распространенных способов совершении мошенничеств в глобальной сети Интернет является завладение денежными средствами под предлогом получения предоплаты за продажу товаров на торговых Интернет-площадках и в группах в социальных сетях, таких как «Инстаграм», «Вконтакте», «Телеграм», «Куфар» и т.д.

Граждане, заинтересовавшиеся объявлениями о продаже товаров по низким ценам, теряют бдительность, вступают в переписку со злоумышленниками, которые представляются продавцами Интернет-магазинов. В ходе переписки, желая получить товар по выгодной цене в кратчайшие сроки, доверчивые граждане, никак не убеждаясь в добропорядочности продавца, переводят на указанные им счета денежные средства. После этого злоумышленники завладевают этими денежными средствами, прекращают общение с покупателем, товар не высылают.

Похожий и набирающий популярность способ совершения мошеннических действий в глобальной сети «Интернет», как завладение денежными средствами под предлогом купли/продажи криптовалюты или заработка на акционной бирже. Как правило, мошенники, имея фото или логотип крупной организации, создают «фейковое» видео о несуществующих биржах.

В таком случае потерпевший самостоятельно находит рекламу о подобном заработке в социальных сетях, сайтах, мессенджерах, после чего оставляет соответствующую заявку. Далее потерпевшему начинают поступать звонки с различных иностранных номеров. В ходе

разговоров звонящие представляются менеджерами крупных брокерских компаний и под предлогом дальнейшего заработка посредством их платформы убеждают жертву зарегистрироваться на принадлежащей им трейдинг-платформе. В дальнейшем потерпевшему предлагается в качестве первого взноса для начала обучения внести небольшую сумму денежных средств. После того, как потерпевший внес так называемый первый взнос, ему начинают поступать звонки от других лиц, которые представляются личными брокерами. В дальнейшем, под предлогом более крупного заработка, потерпевшему предлагается внести более крупную сумму денежных средств. Для убедительности своих действий мошенники под видом вывода заработанных денежных средств с фальшивой трейдинг-платформы перечисляют потерпевшему незначительную сумму, тем самым убеждают потерпевшего в том, что он работает с реальной организацией. Также для того, чтобы окончательно убедить потерпевшего, мошенники посредством переписки, либо на электронную почту присылают копии несуществующих документов, фотографии с изображением удостоверений, сертификатов, лицензий, чаще всего на иностранном языке. Спустя время потерпевший не получает как перечисленные им денежные средства, так и фиктивно заработанные. В конечном итоге, когда потерпевший понимает, что был обманут, злоумышленники либо прекращают общение с ним, либо продолжают свои противоправные действия путем запугивания. Также к потерпевшему могут обращаться другие липа, которые представляются сотрудниками иностранной юридической фирмы, занимающейся возвратом денежных средств, добытых мошенническим путем, однако данные липа также являются мошенниками. При этом на балансе приложения для трейдинга, которое было установлено по указанию мошенников будут отображаться денежные средства внесенные потерпевшим, однако в действительности доступа к данным денежным средствам потерпевший не имеет.

Так, 36-летний рабочий одного из предприятий г. Орша, в социальных сетях нашел рекламное предложение о выгодном вложении денежных средств. Перейдя по ссылке, он заполнил анкету, где указал свои личные данные. Сразу после этого с ним связался специалист по трейдингу и быстро ввел в курс начинающего инвестора. Мужчина оформил на себя два кредита, занял приличную сумму и перевел на указанный мошенниками счет более 26 000 рублей. Затем под предлогом оплаты различных налогов и пошлин за вывод денежных средств, оршанца убедили перевести еще более 10 000 рублем.

На момент, когда оршанец осознал, что его обманывают, он уже успел перевести мошенникам более 40 000 рублей.

Еще одной в последнее время популярной схемой мошенничества стала схема называемая «Fake boss» (Фальшивый босс).

Данный вид мошенничества вовсю набирает обороты, и поэтому работникам организаций и учреждений нужно быть бдительнее.

Для реализации такой схемы преступники изучают чаты трудовых коллективов в мессенджерах, собирают информацию об организации и руководителях, создают учетные записи от их имени. При этом используют в качестве фото контакта - реальные фотоснимки руководителей, которые находятся на общедоступных ресурсах (порталах и социальных сетях).

Далее с помощью «фейкового» аккаунта руководителя они (мошенники) вступают в переписку с подчиненными и, используя доверие к начальнику, дают определенные указания или разъяснения.

Чаще всего такой «руководитель» сообщает о предстоящем разговоре с якобы сотрудниками правоохранительных, контролирующих и иных государственных органов, при этом просит сохранить конфиденциальность общения. Для убедительности мошенники отправляют голосовые сообщения с голосом руководителя, созданные с помощью ИИ (искусственного интеллекта) или вовсе осуществляют звонки. Потенциальным жертвам для подтверждения полномочий могут прислать фотографию удостоверения или копии каких-либо служебных документов, не соответствующих действительности. В результате такого общения злоумышленники склоняют потерпевшего к передаче реквизитов доступа к банковским счетам, перечислению денежных средств или передаче денег курьерам.

Наиболее часто указанная мошенническая схема используется среди работников сфер образования и здравоохранения, среди пострадавших есть, в том числе работники предприятий агропромышленного комплекса и продовольствия, промышленности и торговли, исполнительных органов власти.

Как пример, в текущем году, от имени председателя одного местного сельского Совета депутатов, с «фейкового» аккаунта, осуществлялась рассылка сообщений о якобы грядущей внеплановой проверки, которую будет проводить «куратор» от городского исполкома. Со слов «руководителя», имеется список лиц, с которыми желает побеседовать «куратор». Также «руководитель» настаивал, что необходимо полностью довериться «куратору» и следовать его инструкциям.

Все дальнейшие инструкции сводились к совершению каких-либо финансовых операций: декларирования денежных средств на «специальном счете», оформление кредита, чтобы аннулировать взятые на ранее кредиты и т.п.

При поступлении сообщения или звонка, от имени руководителя с подобным содержанием, вначале необходимо убедиться в правильности названия аккаунта и номера телефона. Затем, связаться с начальником по городскому или мобильному телефону и убедиться подлинности содержания полученного сообщения, а не действовать бездумно, по указке неизвестного лица.

Краткие рекомендации «Как не стать жертвой мошенников?»

- Ни под каким предлогом НИКОМУ НЕ СООБЩАЙТЕ SMS-коды, направленные от банка.
- Никому не сообщайте конфиденциальные данные, использующиеся для доступа к личному кабинету Интернет-банкинга.
- Если ссылок на официальные сообщества банка в социальных сетях нет на официальном сайте, не используйте эти сообщества.
- При возникновении проблем с оказываемыми банковскими услугами ЗВОНИТЬ НАПРЯМУЮ в банк по указанному номеру на официальном сайте банка или на вашей банковской карте.
- Общаясь с клиентами в социальных сетях, сотрудники банка НИКОГДА не переводят общение «в личку» и не пишут персональных сообщений. Они консультируют только в официальном сообществе, в открытых обсуждениях.
- Сотрудники банка оказывают консультацию ТОЛЬКО ПО ОБЩИМ ВОПРОСАМ, что снимает необходимость персонализации клиента.
- Стоит учесть, что сотрудники банка НИКОГДА НЕ ТОРОПЯТ клиента с решением, задача же мошенников – не дать времени проанализировать ситуацию.
- Соблюдайте правила кибербезопасности. Не кликайте подозрительные ссылки, даже если их вам прислали знакомые — их тоже могли заразить вирусом.
- Не УСТАНАВЛИВАЙТЕ на телефон приложения из сомнительных источников. А также ПО для удаленного управления устройством (RustDesk, AnyDesk и др.)
- Заходите ТОЛЬКО НА ОФИЦИАЛЬНЫЕ САЙТЫ компаний и банков. Не оставляйте свои персональные данные и данные банковской карты на сомнительных ресурсах. Обращайте внимание на доменное имя и интерфейс ресурса.
- НЕ ДОВЕРЯЙТЕ НИЗКИМ ЦЕНАМ, не производите предоплату и не переводите деньги на карту или электронный кошелек продавцов.
- НЕ ПРОВОДИТЕ оплату банковской картой на сайтах с небезопасным соединением, без сертификата https. Наличие сертификата в адресной строке существенно снижает риск мошенничества, но в некоторых случаях его тоже подделывают.
- Ставьте последние обновления операционной системы, антивируса и используемых программ.

Оршанский регион (криминал)

Социальная сеть "Вконтакте" https://vk.com/orshacriminal

Цифровая грамотность

"Telegram" https://t.me/cifgram