Министерство внутренних дел Республики Беларусь

Управление внутренних дел Витебского областного исполнительного комитета

Криминальная милиция

УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

ПЛАН-КОНСПЕКТ
на тему: «Актуальные способы совершения киберпреступлений на территории Витебской области»

г. Витебск

Введение

В современном мире, где технологии развиваются стремительными темпами, телефонное мошенничество приобретает новые формы и масштабы. Оно стало распространенным явлением, к сожалению, затрагивающим людей всех возрастов и социальных слоёв. Несмотря на широкую осведомленность об актуальных схемах мошенничества, граждане по-прежнему становятся жертвами злоумышленников. Связь между психологией жертвы и успехом телефонного мошенника неразрывна. Телефонное мошенничество – это не просто случайность, а сложная игра на человеческих слабостях, где портрет жертвы становится ключом к успеху преступника.

Психологический портрет жертвы телефонных мошенников – это собирательный образ, объединяющий людей определенных психологических характеристик и жизненных обстоятельств, делающих их более уязвимыми. В основе лежит, доверчивость, подкрепленная наивностью.

Жертвы склонны верить людям на слово, не подвергая сомнению полученную информацию, особенно если она исходит от представителя авторитетной организации (банк, правоохранительные органы). Они легче поддаются эмоциональному давлению.

Критически важным аспектом является уровень осведомленности о распространённых схемах мошенничества. Недостаток знаний о цифровой безопасности существенно повышает риск стать жертвой обмана. Эта уязвимость часто усугубляется возрастными особенностями. В то время как пожилые люди привыкли к более традиционным формам общения.

Эмоциональное состояние, в котором пребывает человек, также играет свою роль. Стресс, тревога, страх потерять деньги или навредить близким – все эти чувства дезориентируют и ослабляют способность критически оценивать ситуацию. Мошенники умело используют эти состояния, создавая ощущение срочности и паники, вынуждая жертву действовать импульсивно, при этом её внимание рассеяно, а эмоциональная устойчивость снижена.

Немаловажным фактором является одиночество и потребность во внимании. Пожилые люди, живущие одни, особенно уязвимы проявлениям внимания, даже если они исходят от незнакомцев.

Импульсивность и склонность к азарту могут способствовать попаданию в ловушку мошенников. Обещания легкой наживы, выигрыша в лотерею могут затмить разум и заставить человека действовать необдуманно, не проверяя достоверность информации.

Важно отметить, что жертвами становятся не только люди с низким уровнем образования или интеллекта. Напротив. Успешные и образованные личности также попадаются в сети мошенников. Поскольку их уверенность в собственных знаниях приводит к переоценке своей способности распознать обман.

Любой человек, независимо от возраста, образования или социального статуса, может стать жертвой телефонного мошенничества. Психологический портрет лишь указывает на факторы, повышающие уязвимость к подобным манипуляциям. Поэтому важно постоянно повышать свою осведомленность и быть в курсе последних тенденций в сфере телефонного мошенничества.

Мошенники постоянно совершенствуют свои методы обмана, используя последние технологические достижения и психологические приемы. Чтобы обмануть своих жертв в ход идут убедительные легенды, запугивание, срочность и обещание невероятной выгоды.

В 2025 году впервые за несколько лет количество киберпреступлений по республике снизилось на 6%. При этом их доля в общей структуре преступности приблизилась к 30%. Практически каждое третье преступление в стране совершается в цифровой среде. Более 96% таких преступлений носят корыстный характер – целью злоумышленников являются деньги или персональные данные граждан. Всего за 4 месяца текущего года по Витебской области зарегистрировано 739 киберпреступлений. Общий **ущерб** от зарегистрированных в отчетном периоде преступлений составил **1 684 791,18** белорусских рублей.

По-прежнему наиболее распространенными методами обмана, используемыми злоумышленниками, являются **телефонные звонки.**

Используя телефонные звонки для выманивая личной информации, мошенники побуждают к каким-либо действиям. В большинстве случаев мошенники выдают себя за сотрудников правоохранительных органов, банковской сферы, работников государственных организаций, предприятий, операторов мобильной связи, в последнее время представляются сотрудниками кибербезопасности.

Звонят через мессенджеры (Telegram, WhatsApp, Viber), а также могут использовать стационарную телефонную и мобильную связь.

Это, как правило, не один звонок, а целый многоуровневый сценарий. Мошенники работают группой: один представляется сотрудником коммунальной службы или иным другим работником организации, другой – правоохранительных органов или банка, убеждая жертву, что её данные скомпрометированы, и для «спасения» средств или разоблачения недобросовестных сотрудников банковской сферы необходимо оформить кредит или перевести деньги под предлогом их декларирования на «защищенный» или «безопасный» счет. Количество

и состав звонящих мошенников может отличаться в каждом случае. Наиболее сомневающимся жертвам даже поступают видеозвонки с человеком в форменной одежде с погонами.

Например, звонок под видом работников РУП «Белтелеком» поступает на домашний телефон. Мошенник убедительно сообщает, что заканчивается срок действия договора на оказание услуг. И для его продления необходимы паспортные данные и номер мобильного телефона. Дальше в мессенджере поступает звонок от правоохранителей. Чаще Следственного комитета, Департамента финансовых расследований, Комитета государственного контроля. Звонящий сообщает, что человек общается с мошенниками, требует прервать разговор и просит помощь в изобличении преступников. Дальше в мессенджере поступает звонок от якобы «сотрудника банка», который заявляет, что деньги поступят на счет Национального банка и будут возвращены жертве. Для убедительности жертве направляют образец заявления.

Но следует помнить, что злоумышленники часто меняют схемы обмана и на месте сотрудника РУП «Белтелекома» может быть работник РУП «Витебскэнерго», УП «Витебскводоканал», УП «Витебскоблгаз», РУП «Белпочта» и так далее. И сам сценарий истории может быть другой.

Под предлогом продления договора на оказание услуг связи, представляясь операторами сотовой связи, мошенники просят сообщить свои персональные данные и осуществить продление договора удаленно. Могут направить ссылку, перейдя по которой жертва устанавливает приложение удаленного доступа, посредством которого мошенники получают возможность совершать различные операции на мобильном устройстве. Приложение очень схоже с оригинальным. Мошенники устанавливают аналогичный значок. И общий вид приложения на первый взгляд можно принять за настоящее.

Звонки под предлогом обновления кода от домофона

Мошенники представляются сотрудником управляющей компании, службы безопасности или другой официальной организации. Сообщают, что новый код придет из смс-сообщения и его нужно сообщить для обновления в системе. А затем поступает звонок от якобы сотрудника правоохранительных органов, который продолжает обман.

Схема «фейк-босс»

В этой схеме мошенники выдают себя за руководителей и обманом заставляют жертву совершать определенные действия, как правило, связанные с переводом денег или передачей важной информации.

Мошенники тщательно собирают информацию об организации и её сотрудниках, используя открытые источники (сайты, социальные сети, СМИ). Они узнают имена руководителей, их должности, стиль общения и другие детали, которые помогут им убедительно выдавать себя за них.

Мошенники используют поддельный аккаунт одного из руководителей и связываются с жертвой, используя мессенджер. Рассылают сообщения: «Назначен куратор», «Проверка бухгалтерии». Иногда используют дипфейк-технологии, имитируя короткий видеозвонок, ссылаясь при этом на плохое качество связи, чтобы скрыть несовершенство подделки. «Фейк-босс» оказывает на жертву давление, создавая ощущение срочности и важности. Часто мошенники просят жертву не обсуждать этот вопрос с другими сотрудниками, чтобы не «помешать» важной операции.

Знакомства в социальных сетях

Мошенники создают фальшивые профили в приложениях для знакомств или в социальных сетях, используя украденные фотографии привлекательных людей. Долгое время поддерживают отношения с потенциальной жертвой, чтобы в конечном итоге попросить деньги (под предлогом болезни, проблем с визой, оплаты посылки и т.д.). Просьбы могут быть небольшими поначалу, чтобы проверить жертву, а затем возрастают.

Сдача жилья в аренду

Чтобы создать привлекательное объявление о сдаче жилья мошенники используют фотографии, найденные в интернете, а также используют привлекательные цены, чтобы привлечь внимание. Прежде чем показать квартиры, всегда просят предоплату. Личная встреча с арендодателем и осмотр жилья перед оплатой позволят не остаться без жилья и денег. Некоторые мошенники утверждаю, что не могут встретиться с потенциальными арендаторами по различным причинам (например, находятся в другом городе).

Шантаж

Злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства. Социальные сети – это кладезь персональной информации о человеке. Получив несанкционированный доступ к страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам и завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая, в случае отказа, распространить их в сети Интернет.

Набирают обороты вымогательства с использованием информационно-коммуникационных технологий: все преступления, предусмотренные статьей 208 УК Республики Беларусь, совершенные с использованием ИКТ, разделяются на две основные категории:

1. Вымогательства, совершенные с блокированием, модификацией или уничтожением компьютерной информации.

При этом в подавляющем большинстве случаев отмечается блокирование устройств «Apple» посредством ввода авторизационных данных (логин и пароль), предоставленных злоумышленниками под благовидными предлогами, что в последующем не позволяет потерпевшим полноценно использовать свои мобильные устройства.

Способы предлогов довольно разнообразны:

Способ №1. Онлайн-знакомство жертвы с злоумышленником, представляющимся лицом противоположного пола.

Знакомство чаще всего происходит на тематических сайтах. Затем общение переходит в мессенджер, где новый знакомый под различными предлогами (например, необходимо срочно скачать какие-либо файлы или фото из облачного хранилища iCloud) вынуждает потерпевшего зайти в чужую учетную запись «Apple iCloud» со своего устройства. Для большего убеждения, злоумышленник использует заранее заготовленные фотографии, голосовые сообщения и видеозаписи, таким образом у жертвы складывается впечатление, что он действительно общается с лицом противоположного пола. Получив согласие, мошенник высылает логин и пароль, а после входа потерпевшим в «учётку» меняет её пароль и включает режим пропажи iPhone.

Способ №2. Реклама бесплатных игр и приложений в социальных сетях.

Злоумышленники осуществляют размещение видеозаписи (рекламы), в которой указывается бесплатный способ скачать ту или иную игру либо приложение, получить на свой баланс игровую валюту. Для установки данных предложений злоумышленники предлагают зайти в предоставленный ими аккаунт «Apple iCloud». Потерпевшими в подавляющем количестве случаев становятся несовершеннолетние.

Способ №3. Трудоустройство.

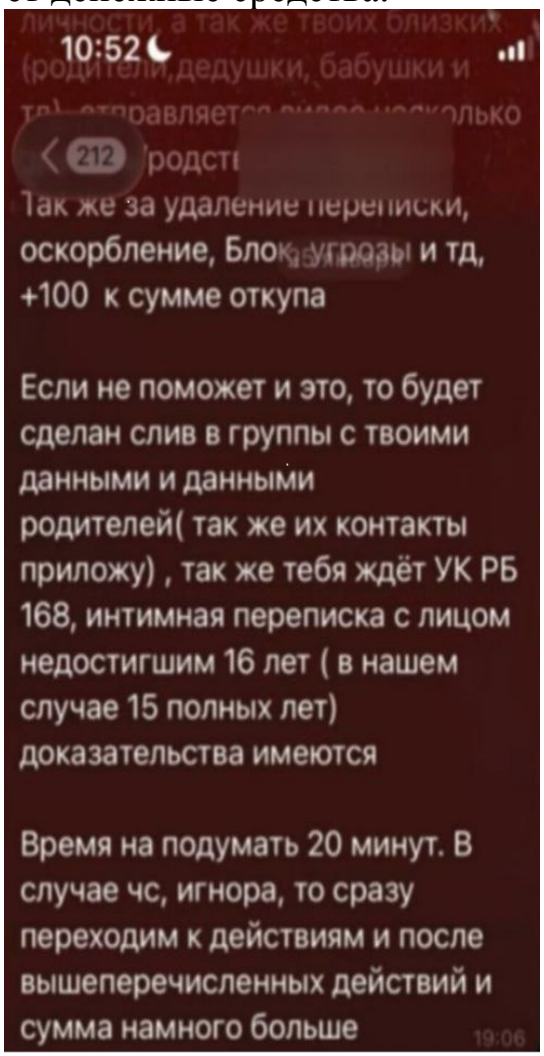
Злоумышленники осуществляют размещение рекламы в сети-Интернет, в которой осуществляется поиск сотрудника на вакансию, как правило связанную с тестированием мобильных приложений для устройства «Apple», для чего предоставляют соискателю для входа якобы корпоративный аккаунт «Apple». В момент, когда жертва осуществляет вход в «Apple iCloud», она оказывается в ловушке, т.к. не может выйти из чужого аккаунта или отключить режим пропажи, iPhone остается заблокированным и не пригодным к использованию. И тогда злоумышленники предлагают перевести деньги за разблокировку устройства.

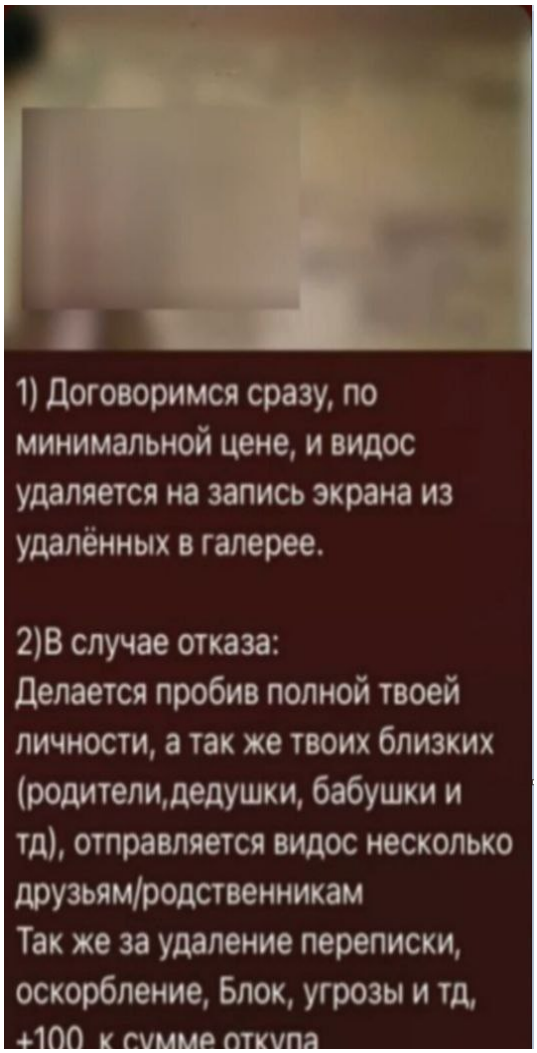
Запомните! Никогда не входите в чужие «учетки» на своих устройствах, а также не сообщайте никому свои учетные данные

от аккаунта «Apple iCloud». Не переходите по неизвестным ссылкам и не вводите данные «Apple ID» на посторонних сайтах.

2. Вымогательства с угрозой распространения личной информации потерпевших либо иных сведений, которые последние желали сохранить в тайне.

К таким сведениям преимущественно относятся фотографии и видеозаписи интимного характера, а также иные личные сведения, которые в большинстве случаев потерпевшие самостоятельно пересылали злоумышленникам, полагая, что общаются с потенциальным партнером для знакомства противоположного пола. В дальнейшем злоумышленник, под предлогом распространения данных среди круга знакомого жертвы, требует денежные средства.





Запомните! Не предоставляйте неизвестным лицам свои данные, содержащиеся в СМС-сообщениях и личные данные неизвестным лицам.

Стоит помнить, что мошенники идут в ногу со временем, а общество постоянно повышает уровень своих цифровых знаний, все больше узнает о социальной инженерии и иных методах злоумышленников, поэтому используемые сейчас последними способы и средства для хищения

денежных средств в скором времени могут стать неактуальными, поэтому любой ситуации нужно оставаться предельно внимательными и досконально разобраться в случившемся, прежде чем сообщать кому-то свои персональные данные. Ваша безопасность в первую очередь в Ваших руках.

«Рекламные акции»

От имени известных в Беларуси торговых брендов мошенники распространяют рекламы поддельных сайтов. После прохождения опроса на таком сайте, пользователю для получения выигрыша предлагается скачать и установить мобильное приложение, привязав к нему банковскую карту. Если жертва выполняет это условие – мошенники получают реквизиты банковской платежной карты.

Инвестиции

На просторах интернета человек натыкается на рекламу «инвестиционного проекта». После подачи заявки с ним связывается «финансовый аналитик», трейдер, брокер, убеждают пройти обучение и вложить средства. «Финансовый специалист» инструктирует, как зарегистрироваться на бирже, пополнить кошелёк небольшой пробной суммой. После того, как потерпевший внес «первый взнос», ему начинают поступать звонки от других лиц, которые представляются личными брокерами. В дальнейшем, под предлогом 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. 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.

Интернет-юристы

Набирает популярность такая схема, как фиктивный возврат потерянных денежных средств. Мошенники выходят на связь с потерпевшими, которые ранее стали жертвами аферистов, обещают

им помочь вернуть украденные средства. Мошенники позиционируют себя «юристами», «департаментом по возврату инвестиций».

Покупка товаров Online

Мошенники активно используют группы в социальных сетях и мессенджерах, объявления на торговых площадках, таких как «Инстаграм», «ВКонтакте», «Телеграм», Чтобы обмануть покупателей и продавцов, мошенники также создают и поддельные сайты, предлагая товары по слишком низким ценам, в том числе утверждая, что товар конфискованный, используя фальшивые отзывы для повышения доверия.

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 общение с покупателем прекращается, товар никто не высылает.

Мошенники обманывают граждан на торговых площадках и под видом покупателей, Представим, что некая девушка выставила на видеокарту на «Куфар». Через некоторое время ей пишет «покупатель»: Оплачу сразу, оформлю доставку, вот ссылка. Ссылка выглядит очень похоже на сервис доставки CDEK (может быть Белпочта, Европочта) только вместо «by» было «.shop» .Девушка вводит данные карты по предложенной форме, включая CVV-код и код из смс-сообщения, после этого мошенники списывают все денежные средства с карты.

Правовое регулирование криптовалютных операций в Республике Беларусь

Операции по покупке и продаже криптовалюты за денежные средства (белорусские рубли, иностранную валюту или электронные деньги) разрешены только в криптобиржах (оператор обмена криптовалют), являющихся резидентами Парка высоких технологий. Совершение операций по купле (продаже) криптовалюты на иных криптобиржах и у физических лиц является незаконным и запрещается. Порядок осуществления сделок с криптовалютой определен Указом Президента Республики Беларусь от 17 сентября 2024 г. № 367 «Об обращении цифровых знаков (токенов)», за нарушение которого предусмотрена административная ответственность частью 3 статьи 13.3 Кодекса Республики Беларусь об административных правонарушениях, предусматривающей штраф с конфискацией всей суммы дохода.

В последнее время мошенники обещают «новый токен» или

быстрый заработок. Для участия предлагают пройти «верификацию» – пополнить депозит настоящей криптовалютой. Результат: деньги навсегда уходят аферистам.

Кто такие дропы?

Для получения за границей похищенных денег, а также для запутывания «цифровых следов» мошенникам необходимо перевести их через промежуточные счета, открытые в белорусских банках на подставных лиц, так называемых «дропов». Часто промежуточных счетов бывает более десятка.

В нашей стране открыть банковский счет может гражданин с 14 лет, с разрешения законных представителей, то есть даже несовершеннолетние могут открыть банковские счета. Этим и пользуются преступники. Находясь за границей, злоумышленники подбирают лиц, которые согласятся открыть банковский счет на свое имя и продать за небольшую сумму реквизиты доступа к нему – это логины и пароли для входа в личный кабинет интернет-банкинга, а также предоставить разовый СМС-код.

Поиск дропов

Напрямую мошенники в интернете не могут размещать объявления о поиске таких лиц, поэтому свой интерес они прикрывают предложением различного другого заработка, не вызывающего подозрения. Например, в Telegram рассылают объявления о поиске курьеров в любом городе со стабильной оплатой труда, или людей для разгрузки товаров, или людей на вакансию «тайный покупатель», или заманивают обещанием высокой и быстрой оплаты.

Чаще всего отзываются на такие вакансии лица с нестабильным или небольшим доходом, в большинстве – молодежь. Сначала инициатор объявления разочаровывает заинтересовавшегося подработкой, сообщает, что данная вакансия уже закрыта, и тут же предлагает иной вид заработка, например, оформить банковский счет и передать за вознаграждение данные для доступа к нему.

Кроме похищенных киберпреступниками денег по промежуточным счетам также могут проводиться деньги, полученные от незаконного оборота наркотиков. Ответственность за возникновение прошедших по банковским счетам денег несут владельцы таких счетов. Ответственность

Надо знать, что статьей 222 Уголовного кодекса предусмотрена уголовная ответственность за распространение из корыстных побуждений находящихся в незаконном владении лица реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам, электронным или

виртуальным кошелькам. За предоставление своих личных данных для использования в мошеннических схемах предусмотрена административная ответственность по статье 12.35 Кодекса Республики Беларусь об административных правонарушениях.

Имеются факты, когда в преступную деятельность вовлекались несовершеннолетние.

Сдача аккаунта в мессенджере или социальных сетях.

Сегодня в сети можно встретить многочисленные предложения сдать свой аккаунт в мессенджерах за вознаграждение. Это очередной способ «легкого» заработка, который может привести к серьезным последствиям. Целевой аудиторией становятся дети и подростки, для которых выплачиваемое вознаграждение может показаться значительным. Злоумышленники вовлекают молодежь в тематических каналах, в чатах онлайн-игр, в сообществах, уверяют, что аренда аккаунта – эта легальный способ заработка. Важно понимать, что через арендованные аккаунты, мошенники обманывают граждан, шантажируют. Используют в различных целях. Наиболее распространенные сценарии включают: распространение спама и фишинговых ссылок, проведения мошеннических операций, создание фейковых профилей для выманивания денег у других пользователей. Любая передача доступа к своему аккаунту третьим лицам, является крайне небезопасной практикой. Если аккаунт был использован для преступной деятельности, значить, в первую очередь правоохранители придут к его формальному владельцу. Гражданин, сдавший аккаунт, рискует оказаться соучастником. В зависимости от тяжести совершения противоправного деяния возможно реальное лишение свободы.

Взлом аккаунтов в мессенджере Telegram

Мошенники отправляют сообщения от имени пользователя уже взломанной учетной записи имеющимся контактам с просьбой осуществить «голосование» в творческом конкурсе рисунков или благотворительной акции (с просьбой «поддержать» детей – из детских домов, малообеспеченных семей с тяжелыми заболеваниями и т.д.).

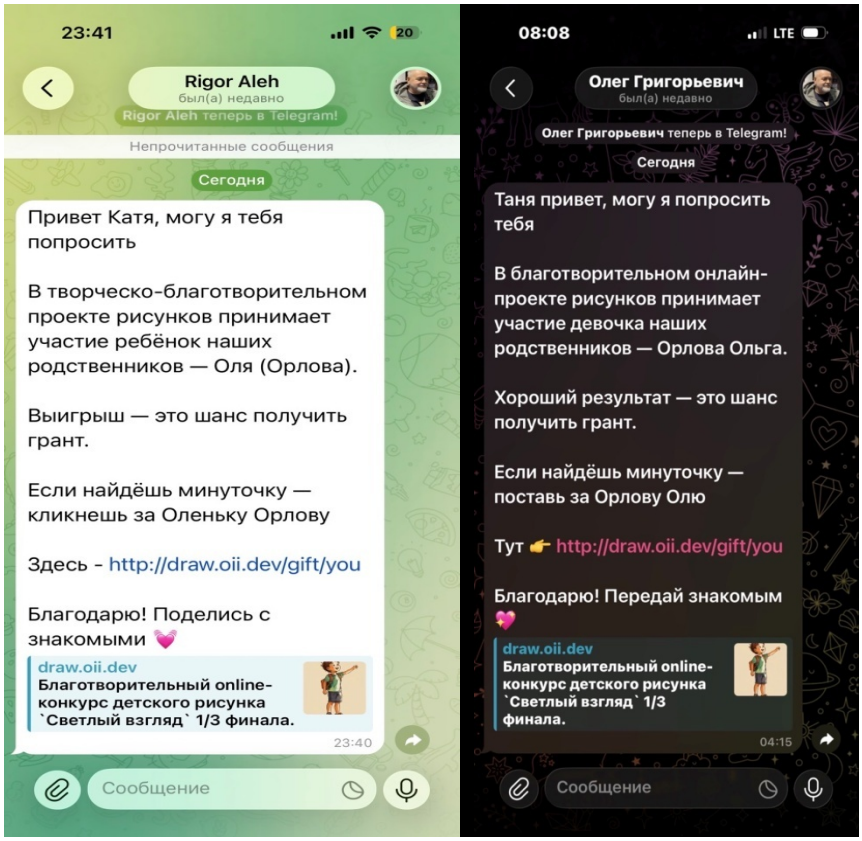
Получив подобное сообщение, граждане переходят по ссылке. Для подтверждения «голоса» требуется ввести свой номер телефона и поступивший код из сообщения. После получения необходимой информации злоумышленники на стороннем устройстве осуществляют вход в учетную запись гражданина, который осуществил «голосование». При этом владельцу учетной записи приходит Push-уведомление, а также в служебном диалоге с Telegram высвечивается уведомление об авторизации нового устройства. Чтобы удалить устройство владельца учетной записи, мошенники некоторое время не совершают каких-либо

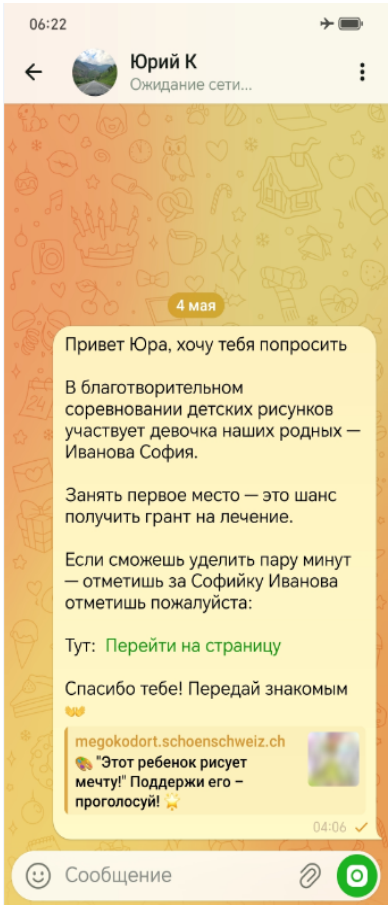
действий на аккаунте, чтобы не привлечь внимание владельца.

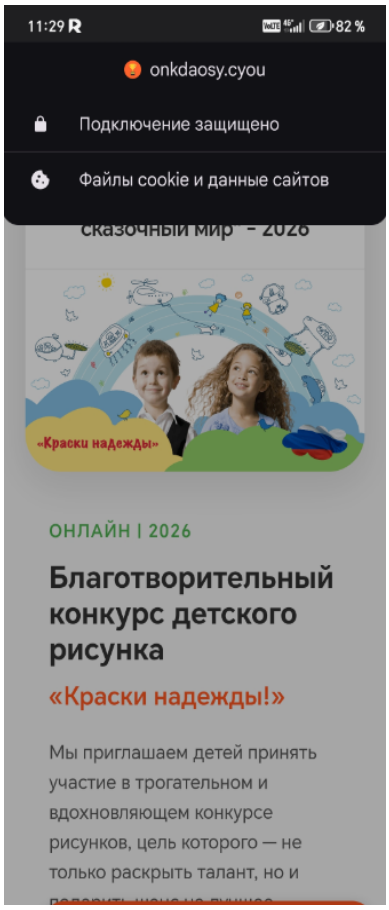
Полученный новый аккаунт используется для продолжения рассылки сообщений с просьбой осуществить «голосование» либо одолжить денежные средства, при этом владельцы теряют доступ к своей учетной записи.

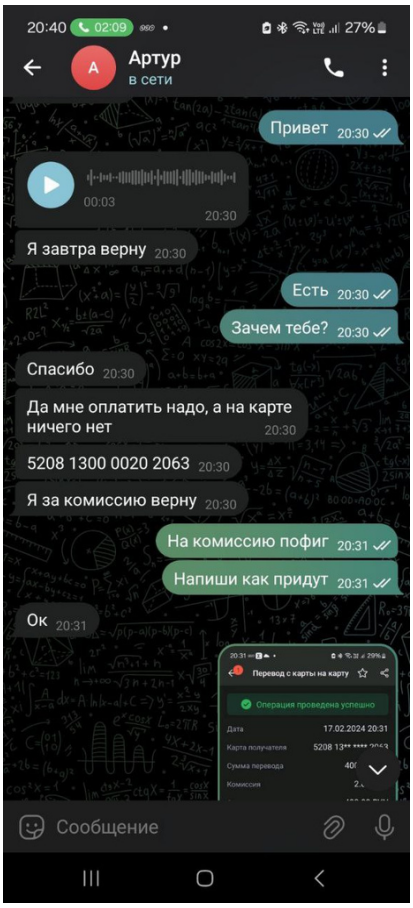
Взлом аккаунта вызывает серьезные проблемы для пользователей. Это может привести к потере конфиденциальной информации, финансовым потерям и ущербу репутации.

Настоятельно рекомендуем ни при каких обстоятельствах не переходить по подозрительным ссылкам из сообщений, особенно если в них содержится эмоциональный призыв о помощи. Проверять любую информацию о сборах средств или голосованиях.









В ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКОВ

Запомните следующие правила:

– если незнакомый заводит беседу про ваши деньги, прекратите разговор;

– не доверяйте незнакомым и не выполняйте то, о чем они просят, даже если обещают помощь в сохранении денежных средств;

– не устанавливайте непроверенные программы на свои электронные устройства по указанию незнакомых;

– при совершении покупок в сети Интернет производите оплату только после получения товара и проверки его состояния;

– не забывайте, что мошенники могут представляться вымышленными данными, использовать для подтверждения личности фотографии чужих паспортов, чужие аккаунты в соцсетях, чужие абонентские номера.

– не доверяйте красивому оформлению сайта или страницы Интернет-магазина, комментариям пользователей. На сегодняшний день создать сайт с любой информацией не составляет труда. Отличить добросовестных продавцов от мошенников стало невозможно, наилучший способ общения – личная встреча с продавцом, осмотр товара на месте;

– покупайте товары в проверенных магазинах, либо перед покупкой проверяйте их посредством мониторинга в сети Интернет;

– не попадайтесь на уловки мошенников, обещающих Вам продать товар по низкой цене, какими бы выгодными не были условия сделки;

– сотрудники правоохранительных органов и работники банков не звонят в мессенджерах и не просят оформить кредит или оказать содействие в поимке злоумышленников, а также не предлагают застраховать и обезопасить денежные средства;

– обращайте внимание на абонентские номера, с которых вам звонят в мессенджерах, чаще всего абонентские номера, с которых звонят злоумышленники, принадлежат иностранным государствам;

– не переводите деньги на «защищенный счет»;

– не сообщайте неизвестным лицам свои персональные данные, реквизиты банковских карт, SMS-коды;

– не переходите по ссылкам от неизвестных пользователей;

– при поступлении подобных звонков немедленно прекратите разговор и сообщите о произошедшем в милицию.

«Цифровая грамотность»

Рекомендуем подписаться на Телеграм-канал «**Цифровая грамотность**» (ссылка-приглашение «**t.me/cifgram**»), где на регулярной основе публикуется актуальная информация о способах совершения киберпреступлений и методах противодействия им.

Управление по противодействию киберпреступности
КМ УВД Витебского облисполкома