Приложение № 1
к распоряжению ГУ МВД России
по Ростовской области
от «12» января 2025 года №1/4

План-конспект
«доведение в трудовых коллективах основных мошеннических схем»

Стремительное внедрение в повседневную жизнь информационно-коммуникационных технологий, в том числе различных сервисов удаленного доступа, за последние годы, привело к существенному росту зарегистрированных кибермошенничеств, как на территории региона так и по стране в целом.

Значительная часть таких преступлений совершается лицами, владеющими передовыми методами «социальной инженерии». Как правило, схемы хищений выглядят следующим образом:

Способ

Жертве звонят через мессенджер «Вотцап, Вайбер и т.д.»

Мошенники представляясь сотрудниками службы безопасности банка звонят клиенту и сообщают, что необходимо произвести замену номера прикрепленного к лицевому счету, чтобы предотвратить мошеннические действия. Для этого предлагается установить на мобильный телефон приложения «RustDesk», «AnyDesk» и «Zoom».

Приложения «RustDesk», «AnyDesk» и «Zoom» позволяют мошенникам дистанционно управлять мобильным телефоном жертвы и открывать приложения «Онлайн банка».

При вводе пароля в приложении «Онлайн банка» у жертвы производятся списания ВСЕХ денежных средств с имеющихся счетов.

Сотрудники банков не звонят клиентам через мессенджеры «Вотцап», «Вайбер» «Телеграм» и не предлагают скачивать различные приложения и программы.

Способ
хищения денежных средств с использованием приложения-сервиса «BlaBlaCar, АВИТО, ЮЛА и т.д.»

При совершении преступления, злоумышленники используют официальный сайт https://www.blablacar.ru (Авито, Юла) (приложения смартфон на Android, IOS), в котором создают аккаунт несуществующего лица (фейковый), предлагающего услуги перевозки пассажиров, где указывают маршрут передвижения. При появлении клиента на указанное направление и уточнение времени и условий поездки, злоумышленник под различными предлогами, предлагает уйти из официального сайта на общение в мессенджеры (Вотцап, Вайбер), в которых клиенту предлагается оплатить поездку, либо в случае с Автио или Юлой продать товар якобы на официальном сайте. После получения согласия клиента, ему по средством мессенджера, поступает ссылка на поддельный (фишинговый) сайт, при переходе по которой, открывается «окно» оплаты внешне схожим с официальным сайтом, где злоумышленник предлагает внести реквизиты банковской карты для оплаты поездки, либо получения денег за товар. После ввода реквизитов происходит списание денежных средств, а «фейковый» аккаунт удаляется.

Не переходите по ссылкам и не покидайте официальные сайты приложений, чтобы не стать жертвой мошенников.

Способ
хищения денежных средств под предлогом
приобретения билетов в театр (кинотеатр)

При совершении преступления, злоумышленники используют сайт знакомств «Тиндер», с помощью которого, знакомятся с молодыми людьми. Далее, под различными предлогами, злоумышленник предлагает перейти для дальнейшего общения в мессенджер «Телеграмм», где предлагает потерпевшему пойти в театр, кино или на концерт. После получения согласия, потерпевшему по средством мессенжера, поступает ссылка на поддельный (фишинговый) сайт, при переходе по которой, открывается «окно» оплаты внешне схожим с официальным сайтом билетных касс, где потерпевший вносит реквизиты банковской карты для оплаты. После ввода реквизитов происходит списание денежных средств, а «фейковый» аккаунт удаляется.

Способ

Жертву обвиняют в госизмене за денежные переводы в пользу ВСУ, либо звонки от сотрудников правоохранительных органов пытающихся предотвратить незаконное оформление кредита.

Мошенники звонят клиенту и представляются сотрудниками полиции, следственного комитета, прокуратуры или ФСБ. Сообщают, что сотрудник банка, в котором обслуживается клиент, украл его персональные данные и осуществляет с его счета переводы в пользу армии Украины. А так же ответственность лежит на владельце карты, клиент может быть обвинен в государственной измене, за что ему грозит до 20 лет лишения свободы.

Затем мошенники представляются службой безопасности банка и убеждают клиента переводить деньги на их счета и даже брать кредиты, мотивируя это тем, что так они смогут вычислить преступника внутри банка.

Сотрудники правоохранительных структур никогда не звонят гражданам с целью обезопасить их банковские счета.

Способ

Заработок на различных интернет-площадок

(Биржа, Газпроминвеститции и т. д.)

Граждане самостоятельно, через интернет либо, через звонок осуществляемый злоумышленниками, становятся участниками различных инвестиционных проектов. Их убеждают поучаствовать в выгодных инвестициях и получить огромную прибыль, зарегистрировав аккаунт на электронной торговой площадке (бирже), которая якобы имеет официальный статус, однако является эмулятором. Так же сотрудники организации убеждают гражданина, что будут консультировать его в ходе торгов и говорить, когда совершить покупку или продажу активов, чтобы сделки гарантировано приносили прибыль. В процессе торгов гражданину дают возможность немного заработать и вывести на

свой банковский счет, небольшую сумму денег. После чего, с целью получения еще более высоких дивидендов предлагают перевести на подконтрольные счета злоумышленников крупные суммы денег. Когда человек намерен вывести полученную прибыль, ему под различными предлогами отказывают и убеждают совершить еще несколько гарантированно выгодных сделок, в результате которых ничего не подозревающий гражданин, под полным контролем брокеров, совершает заведомо убыточные операции и теряет все накопления с лицевого счета.

При обнаружении в сети интернет рекламы по дополнительному заработку на различных биржевых платформах, знайте это мошенники. Не переходите на данные сайты, чтобы не стать жертвой мошенников.

Способ

Сообщение о взломе Единого портала государственных и муниципальных услуг

Одним из распространенных способов хищений денежных средств в последнее время является получение несанкционированного доступа к личному кабинету пользователя сервиса «Госуслуги». Жертве поступает звонок от злоумышленника, который представляется оператором службы поддержки Единого портала государственных и муниципальных услуг, где сообщается о том, что произошел неправомерный доступ к личному кабинету, и для предотвращения необходимо сообщить поступающие на телефон гражданина соответствующие коды. При сообщении кодов злоумышленники получают доступ ко всем сервисам портала с аккаунта жертвы и имеют возможность подать заявку на оформление и получения кредита с последующим переводом денежных средств на подконтрольные счета. **Сотрудники Единого портала государственных и муниципальных услуг(Госуслуги) никогда не звонят гражданам с целью несанкционированного доступа к личному кабинету. Согласно инструкции и предоставляемых услуг, пользователь сам осуществляет звонки в службу поддержки портала.**

Способ

Жертве пишут через мессенджер « Телеграмм » от имени руководителя

Схема хищения выглядит следующим образом: на стационарный телефон пожилых граждан поступает звонок от злоумышленников, которые представляются сотрудниками правоохранительных органов, и сообщают о том, что их родственник совершил ДТП (либо попал в ДТП). Чтобы урегулировать («решить») проблему необходимо передать денежные средства, при этом просят потерпевшего не прерывать разговор. В случае согласия потерпевшего, к нему по месту жительства за денежными средствами выезжает курьер.

Необходимо провести беседу с пенсионерами, которые могут являться потенциальными потерпевшими разъяснив, что не нужно не кому передавать свои сбережения.

Способ

Мошенники обманывают детей в онлайн играх, выманивая сведения о банковских счетах родителей

Мошенники выманивают у детей денежные средства в онлайн играх, к примеру в таких как «Роблокс» или «Стендофф 2». Злоумышленники притворяются блогерами, либо такими же игроками имеющими много игровой валюты или располагающие какой-то секретной версией игры, тем самым в процессе онлайн общения (общение зачастую переходит в мессенджеры или соц. сети) втираются в доверие и предлагают детям получить бесплатно игровую валюту или подписку в игре. Детям надо только совершить некоторые действия, при этом не сообщать об этом родителям. Мошенники просят сделать перевод через банковское приложение родителей (в том числе бабушек и дедушек, либо других родственников к чьим телефонам имеется доступ) или сфотографировать банковскую карту со всех сторон, а потом отправить мошенникам смс-код поступивший на телефон родителя. Мошенники получают таким способом доступ к приложению «Онлайн банка» и похищают имеющиеся личные денежные средства, а также оформляют онлайн кредиты.

Ограничивать доступ к сотовому телефону от детей, разговаривать с детьми об информационной безопасности, разъясняя о подобных случаях.

5

Способ

жертве звонят представляясь сотрудниками операторов сотовой связи «Билайн, Теле2, МТС, Мегафон и т.д.».

Мошенники представляясь сотрудниками оператора сотовой связи и сообщают, что необходимо обновить приложение оператора связи или улучшить тарифный план, для этого необходимо скачать программу которая позволит внести вышеуказанные изменения. Для этого предлагается установить на мобильный телефон приложения «RustDesk» и «Zoom». Приложения «RustDesk» и «Zoom» позволяют мошенникам дистанционно управлять мобильным телефоном жертвы, и открывать приложения «Онлайн банка», с целью хищения денежных средств.

Сотрудники операторов сотовой связи не звонят клиентам с предложениями установить программное обеспечение на телефон. При поступлении таких звонков необходимо отклонить вызов, чтобы не стать жертвой мошенников.

Способ

Жертве пишут через мессенджер « Телеграмм » от имени руководителя

Мошенники представляются руководителями государственных и коммерческих организаций, где осуществляют трудовую деятельность граждане и сообщают, что им поступит звонок от представителей различных служб «ФСБ, МВД, Министерства Юстиции, Прокуратуры, Центрального банка и т.д.», указания которых необходимо выполнить незамедлительно. При поступлении звонка от вышеуказанных служб, жертве сообщают о том, что необходимо провести манипуляции по всем имеющимся банковским счетам и картам находящимся в пользовании у граждан и при этом ни о чем не кому не рассказывать. В процессе обмана на потерпевшего оформляются многомиллионные кредиты. Данные действия приведут к хищению денежных средств как личных так и кредитных.

При поступлении сообщений через мессенджеры «Вотцап», «Вайбер» «Телеграм» от руководителей организаций знайте, что Вас пытаются обмануть, и похитить Ваши денежные средства. Что бы не стать жертвой данной преступной схемы, о всех поступивших такого рода сообщениях незамедлительно докладывать своему непосредственному руководству.