

Приложение № 1
к приказу ГУ МВД России
по Ростовской области
от «18» сентября 2023 года № 1595

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 личному счету, чтобы предотвратить мошеннические действия. 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».

При вводе пароля в приложении «Онлайн банка» у жертвы производится списание ВСЕХ денежных средств. **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> (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 предложениями предлагает уйти из официального сайта на общение в мессенджеры (Вотцап, Вайбер), в которых клиенту предлагается оплатить поездку, якобы на официальном сайте. После получения согласия клиента, ему по средством мессенжера, 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. 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 «Гиндер», с помощью которого, знакомятся с молодыми людьми. Далее, под различными предложениями, 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 представляют сотрудников 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 перевести 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, Газпроминвестиции и т.д.)**

Граждане самостоятельно, через интернет либо, через звонок осуществляемый злоумышленниками, становятся участниками различных инвестиционных проектов. Их убеждают участвовать 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 принесли 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, найдите 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 звонит представляясь сотрудниками операторов сотовой связи «Билайн, Теле2, МТС, Мегафон и т.д.».

Мошенники представлялись 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.