Приложение
к протоколу заседания
межведомственной комиссии по
профилактике правонарушений в
Азовском районе от 29.03.2024 № 1

О новых способах мошенничества с использованием информационных технологий

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 телефон, прикрепленного к лицевому счету, чтобы предотвратить мошеннические действия. Для этого предлагается установить на мобильный телефон приложения «RustDesk» и «Zoom».

Приложения «RustDesk» и «Zoom» позволяют 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 предлогами, 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 посредством мессенджера, поступает ссылка на поддельный (фишинговый) сайт, при переходе 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 «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 посредством мессенджера, 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 осуществляют с его счета переводы в пользу армии Украины. А также 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-площадках (Биржа, Газпроминвестиции и т.д.)

Граждане самостоятельно, через интернет, через звонок, осуществляемый злоумышленника, 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 эмулятор. Также сотрудники организаций 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 гарантировано 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 несанкционбированного 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 звонят, представляясь сотрудниками операторов сотовой связи «Билайн, Теле2, МТС, Мегафон и т.д.»

Мошенники представляются 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 звонят через мессенджер «Телеграмм»

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, жертве сообщают о том, что необходимо провести манипуляции по всем имеющимся банковским счетам и картам, находящимся в пользовании у граждан. 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» от руководителей организаций знайте, что Вас пытаются обмануть, и похитить Ваши денежные средства. Чтобы не стать жертвой данной преступной схемы, о всех поступивших такого рода сообщениях незамедлительно докладывайте своему непосредственному руководству.

Способ
жертве звонят, представляясь сотрудниками операторов сотовой связи «Билайон, Теле2, МТС, Мегафон»

Мошенники представляются сотрудниками оператора сотовой связи и сообщают, что истекает срок действия договора по оказанию услуг сотовой связи и предлагают его продлить в телефонном режиме. Для продления срока договора на абонентский номер потерпевшего приходит смс сообщение с кодом, который мошенники просят сообщить. После передачи кода, мошенники получают

доступ в личный кабинет сотового оператора и заказывают перевыпуск сим карты с материального носителя на виртуальный (Е-сим). Завладев абонентским номером, мошенник получает доступ ко всем банковским картам, страницам социальных сетей, привязанным к абонентскому номеру.

Сотрудники операторов сотовой связи не звонят клиентам с предложениями продлить срок договора использования услуг сотовой связи, он продлевается автоматически при постоянном использовании абонентского номера.

Способ
родственник попал в беду

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 «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.