ПОЛИЦЕЙСКИЕ ОЧЕРЕДНОЙ РАЗ ИНФОРМИРУЮТ ГРАЖДАН О СПОСОБАХ МОШЕННИЧЕСТВА

Сотрудники полиции рекомендуют ознакомиться с различными мошенническими схемами, для того чтобы не стать жертвой аферистов и сохранить свои сбережения.

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 в стране в целом.

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

Жертве звонят через различные мессенджеры

Мошенники, представляясь сотрудниками службы безопасности банка звонят клиенту и сообщают, что необходимо произвести замену номера, прикрепленного к лицевому счету, чтобы предотвратить мошеннические действия. Дня этого предлагается установить на мобильный телефон приложения удаленного доступа, которые позволяют мошенникам дистанционно управлять мобильным телефоном жертвы, и открывать онлайн приложения банков. При вводе пароля в онлайн приложении банка, у жертвы производится списание всех денежных средств.

Сотрудники банков не звонят клиентам через мессенджеры и не предлагают скачивать различные приложения и программы.

Хищения денежных средств с использованием интернет-сервисов по размещению объявлений, онлайн-сервис поиска автомобильных попутчиков и прочих

При совершении преступления, злоумышленники используют официальный сайт того или иного интрнет-сервиса, в котором создают аккаунт несуществующего лица, к примеру, 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 покинуть официальный сайт и продолжить общение в мессенджере, где клиенту предлагается оплатить поездку якобы на официальном сайте. После получения согласия клиента, ему через мессенжер поступает ссылка на фишинговый сайт. При переходе по ней открывается «окно» оплаты внешне схожее 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.

Хищения денежных средств под предлогом приобретения билетов в театр (кинотеатр)

При совершении преступления, злоумышленники используют сайты знакомств, где заводят общение с потенциальными жертвами. Далее под различными предлогами, злоумышленник предлагает продолжить диалог в мессенджер, после чего приглашает гражданина(гражданку) пойти в театр, кино или на концерт. После получения согласия, потерпевшему через мессенджер, поступает ссылка на 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 поддельный аккаунт удаляется.

Жертву обвиняют в государственной измене за денежные переводы в пользу иностранной армии, либо же звонят, представляясь сотрудниками правоохранительных органов и предлагают предотвратить незаконное оформление кредита

Мошенники звонят клиенту и представляются сотрудниками силовых ведомств. Сообщают, что сотрудник банка, в котором обслуживается клиент, украл его персональные данные и осуществляет с его счета переводы в пользу иностранной армии. А также говорят, что ответственность лежит на владельце карты и 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

Граждане через сеть Интернет, либо же через звонок, осуществляемый злоумышленниками, становятся участниками различных «инвестиционных проектов». Их убеждают поучаствовать в выгодных сделках и получить прибыль, зарегистрировав аккаунт на электронной торговой площашдке (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 свои 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.

Сообщение о взломе личного кабинета на сервисе, предоставляющем государственные и муниципальные услуги

Одним из распространенных способов хищений денежных средств в последнее время является получение несанкционированного доступа к личному кабинету сервиса, предоставляющего государственные и муниципальные услуги.

Жертве поступает звонок от злоумышленника, который представляется оператором службы поддержки данного портала, 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 портала, предоставляющего государственные услуги никогда не звонят гражданам с целью несанкционированного доступа к личному кабинету. Согласно инструкции и предоставляемых услуг, пользователь сам осуществляет звонки в службу поддержки сервиса.

Жертве звонят, представляясь сотрудниками операторов сотовой связи

Мошенники звонят гражданам, 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 удаленного доступа, которые позволяют мошенникам дистанционно управлять мобильным телефоном жертвы, и открывать онлайн приложения банков, 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.

Будьте бдительны!
Проведите разъяснительную беседу о том, как не стать жертвами мошенников со своими родственниками, особенно пожилого возраста.
Обо всех подозрительных лицах и звонках незамедлительно сообщайте по тел.: 02, 102, 112, 8(8634) 632-220
Адрес Управления МВД России по г.Таганрогу: ул. Александровская, 45, г. Таганрог, Ростовская область, 347900
Адрес электронной почты: tagumvd61@mvd.ru