Бита карта. Банковская

Правопорядок. Следователи Озёрска завершили расследование уголовного дела о мошенничестве с банковскими картами

Следственным отделом Управления МВД России по ЗАТО г. Озёрск окончено расследование уголовного дела о мошенничестве и краже с банковского счёта.



Предстанет перед судом

В ходе следствия установлено, что злоумышленник в период с июня по сентябрь 2023 года занимался хищениями денежных средств, используя аккаунт в известной социальной сети. Для этого он разместил ложную информацию о возможности получения дополнительного заработка при участии в реферальной программе одного из банков, указав при этом о необходимости оформления кредитной карты.

После переговоров заинтересованные в прибыли граждане по указанию злоумышленника оформляли в мобильном приложении кредитную карту, все средства с которой переводили мошеннику.

Жертвами преступлений стали трое жителей разных городов Челябинской области. Причинённый преступными действиями ущерб составил более 54 тысяч рублей.

Оперативникам озёрской полиции удалось раскрыть преступную схему и выйти на мошенника. В настоящее время уголовное дело вместе с обвинительным заключением, утверждённым прокурором, направлено в Калининский районный суд Челябинска для рассмотрения по существу.

Зарубите на носу!

Главное следственное управление ГУ МВД России по Челябинской области призывает горожан быть бдительными и в сотый раз напоминает о наиболее распространённых способах мошенничества.

«Звонок от оператора». Мошенники представляются сотрудниками мобильного оператора и сообщают о том, что у клиента заканчивается срок действия сим карты и нужно продлить договор, либо от абонента поступила заявка на смену мобильного номера телефона или из за сбоя его перевели на тариф подороже, а также в некоторых случаях злоумышленники предлагают бесплатно подключить 5G. Далее на телефон поступает смс с кодом, который мошенники просят сообщить для подключение услуги или отмены операции.

Никому не сообщайте коды из смс, полученных от мобильного оператора, так как данной информации достаточно для того чтобы получить доступ в личный кабинет на сайте мобильного оператора, настроить переадресацию звонков и смс, а после взломать аккаунт в мобильном приложении банка и вывести сбережения или оформить кредит.

При поступлении сомнительных и тревожных звонков, положите трубку и перезвоните в службу поддержки по официальному номеру, или обратитесь в офис мобильного оператора.

«Взломали госуслуги». Мошенники представляются сотрудниками поддержки госуслуг и говорят, что профиль на портале был взломан мошенниками и для восстановления доступа нужно сменить пароль. После чего просят назвать код из смс.

Не сообщайте коды из смс, полученных от абонента госуслуги, в противном случае мошенники взломают аккаунт и получат доступ к вашим персональным данным, а после смогут оформить кредит. Если вам поступил подобный звонок, положите трубку и обратитесь в службу поддержки.

«Установите приложение». Злоумышленники выступают в качестве сотрудников банка и просят установить антивирус, новую версию банковского приложения, сервис для диагностики телефона. После установки приложения просят сообщить идентификационный код для доступа к смартфону. Установленное программное обеспечение на самом деле не находит вирусы, а даёт удалённый доступ к телефону, то есть с помощью этого приложения мошенники видят всё, что происходит на телефоне и могут им управлять. Скачивайте приложения только по ссылкам с официальных сайтов.

Новая схема мошенничества

Снимают порчу, золото и деньги

Южноуральцев предупреждают о новой мошеннической схеме со снятием порчи.



В Златоусте 69-летняя женщина стала жертвой ловкого обмана двух аферисток, которые убедили свою жертву в том, что с её семьи необходимо снять порчу, а позже украли золотые украшения и деньги. Когда пенсионерка раскрыла обман, она обратилась в полицию, и подозреваемых задержали в другом городе. Подробнее о новой мошеннической схеме рассказали в региональном полицейском главке.

К потерпевшей подошли две женщины и спросили, где находится детский сад. Пенсионерка не смогла сразу же ответить на вопрос, и пока она думала, одна из женщин внезапно сообщила ей, что видит порчу. Если её не снять, то на семью потерпевшей обрушатся беды. Затем аферистки дали разволновавшейся женщине металлическую скрепку, виртуозно заменив её на ржавую. Таким образом они «доказали», что порча действительно существует.

«Колдуньи» сообщили, что снять порчу можно с помощью золота. Они поручили пенсионерке пойти домой, сложить все золотые изделия в носок и принести им для проведения «магического ритуала по очищению». Женщина так и сделала, а также передала им полторы тысячи рублей за оказанную услугу. Подозреваемые якобы провели ритуал, вернули женщине носок и велели вернуться на следующий день в это же место, чтобы заклинание сработало.

Только на следующий день пенсионерка решила проверить содержимое носка. Но вместо золота она обнаружила камни. Поняв, что её обманули, она обратилась в полицию.

Подозреваемых задержали в Челябинске. Они раскаялись в содеянном и пообещали возместить ущерб в размере 80 тысяч рублей. Однако в их отношении всё равно возбудили уголовное дело о мошенничестве. Также правоохранители выясняют, причастны ли проходимки к другим подобным преступлениям.

– Злоумышленники, промышляющие «снятием порчи», применяют различные уловки. Вот некоторые из них: просят человека принести яйцо, затем накрывают яйцо тряпкой, в это время заменяют хорошее яйцо на другое, принесённое заранее, и когда открывают тряпку, жертва видит вместо обычного яйца чёрное. Существует такой же обман со стаканом воды, – предупреждают в полиции.

Южноуральцев просят быть бдительными, не доверять незнакомцам и их сомнительным сообщениям о порче, а также не передавать им деньги и драгоценности.

По материалам ИА «Первое областное»

Попался в сети

Вот так «услужили»!

Житель Кыштыма перевёл мошенникам более одного миллиона рублей из-за подозрительной активности на госуслугах.

К кыштымским полицейским обратился местный житель 1965 года рождения. Он рассказал, что ему позвонил незнакомец и уведомил об истечении срока действия сим-карты, после чего настоятельно просил сообщить код, который был отправлен в смс. Это якобы было необходимо для того, чтобы продолжить пользоваться услугами сотовой связи. Местный житель принял всё за чистую монету и тут же выполнил данное условие.

Вскоре ему позвонила незнакомка, она представилась сотрудником банка. Собеседница сообщила, что в личном кабинете мужчины на портале госуслуг ею была замечена подозрительная активность, для решения которой необходимо внести денежные средства.

Доверчивый кыштымец обналичил со своей кредитной карты 265 тысяч рублей и перевёл денежные средства на указанный девушкой счёт. Затем оформил кредит на 800 тысяч рублей и четырьмя платежами перевёл деньги на тот же счёт.

Но на этом мошенница не остановилась. Она убедила мужчину в необходимости оформления ещё одного кредита. Однако настоящие представители банковской организации заподозрили, что мужчина имеет дело с мошенником, и, уведомив его об этом, посоветовали обратиться в полицию.

Общая сумма ущерба составила один миллион 65 тысяч рублей. В полиции Кыштыма по данному факту возбуждено уголовное дело.

Полицейские вновь призывают южноуральцев не совершать никаких денежных переводов по инструкциям незнакомцев. Не вступайте с ними в диалог и инициативно прерывайте телефонный разговор с собеседником, который вынуждает вас оформить кредит и отправить деньги на «безопасный» счёт, которого, как известно, не существует. Проконсультируйтесь с близкими родственниками или друзьями. Безопасность ваших денег зависит от совершённых вами действий.

Открытки от мошенников

В России распространился новый тип мошенничества в мессенджерах. Под видом поздравительных открыток от родственников людям приходят фишинговые ссылки. Когда пользователь переходит по ним, мошенники получают доступ к данным банковских карт или аккаунта на госуслугах. Эксперты предупреждают: если вам приходит ссылка с «поздравлением» непонятно от кого, то лучше сразу удалять это сообщение и заблокировать адресата. Если ссылка отправлена родственником или другом со своего аккаунта, нужно попросить его прислать открытку картинкой. Потому что аккаунт вашего близкого человека может быть взломан мошенниками.

