

Будьте бдительны!

Кошелёк виртуальный, ущерб – реальный

Заявления о краже средств с банковских счетов поступают в полицию ежедневно

Несмотря на постоянное информирование граждан о мошеннических схемах, обманутых граждан меньше не становится. Среди пострадавших и пенсионеры, и студенты, и работники, и даже руководители, расска-зала специалист по взаимодействию со СМИ МВД России по Магнитогорску Мария Морщакина.

На вас оформляют кредит

С обычной зарплатой карты чаще всего много не спишешь. Но мошенники придумали новую схему, с помощью которой похищают у доверчивых граждан значительные средства – суммы ущерба идут на сотни тысяч и даже миллионы рублей.

В полицию Челябинска, Миасса и Южноуральска обратились местные жители с аналогичными заявлениями, сообщили в пресс-службе ГУ МВД России по Челябинской области 17 марта. Гражданам звонили якобы сотрудники банков и сообщали, что мошенники пытаются оформить на них кредиты, для аннулирования которых необходимо оформить свои кредиты на определённые суммы. Для полной убедительности заявителям перезванивали мнимые представители правоохранительных органов, появившиеся, что необходимо верить работникам банка и выполнять их указания. Южноуральцы доверились звонившим, оформив онлайн-кредиты в отделениях банков, а затем перечислили денежные средства на так называемые «резервные» счета для сохранности, а на самом деле – счета злоумышленников. Общий ущерб составил более 700 тысяч рублей.

По таким схемам суммы огромные, от 300 тысяч и до миллиона и выше, размер зависит от того, какой кредит готов выдать банк, – уточняет специалист по взаимодействию со СМИ МВД России по Магнитогорску Николай Жвыкин. – Если банк даёт миллион – берут всю сумму. Потом обналичивают деньги через банкомат, причём мошенники готовы даже оплатить для этого такси до ближайшего банкомата. Затем по инструкции мошенников жертва переводит деньги на счета злоумышленников. Часто преступники требуют разделить сумму на несколько отдельных счетов. А человек даже не задумывается, почему нужно на разные номера переводить одинаковые суммы. Мошенники не дают отключить телефон, чтобы у человека не было времени с кем-то посоветоваться. Только расставшись с деньгами и положив трубку, он начинает осознавать, что его обманули.

Компенсация за БАДы

Этот случай мошенничества произошёл в феврале текущего года: 68-летней жительнице Магнитогорска по телефону сообщили, что ейлагается компенсация за приобретённую биологически активную добавку. Якобы БАДы оказались опасными, а производителей отправили в тюрьму. Озвучили и сумму компенсации: 385 тысяч рублей. Правда, за содействие в получении выплаты нужно заплатить комиссию – десять процентов от суммы. Женщина не растерялась и



предложила мошенникам вычестъ комиссию из озвученной суммы, а остальное перевести. Разумеется, никакой компенсации она не получила, но и собственных средств не лишилась.

Неудачный шопинг

Покупки через Интернет – тоже распространённый способ обмана доверчивых граждан.

Мошенники выставляют товары на популярных площадках, присылают счета покупателям, но ничего, разумеется, не высылают. Так, житель города нашёл в Сети объявление о продаже шин. Списался с продавцом, указал нужные параметры. Продавец заверил, что товар в наличии, но потребовал стопроцентную предоплату. Ущерб потерпевшего – 27 тысяч рублей. Другой случай: жительница города размещала в сети «Инстаграм» объявления о продаже брендовых вещей. Писали со всей России. Не останавливали потерпевших даже негативные отзывы. Покупки оплачивали, но заказы не приходили.

Дело рассматривалось в конце января, – уточняет руководитель подразделения, занимающегося расследованием преступлений, связанных с IT-мошенничествами, подполковник юстиции Татьяна Шапкина. – Выявлено 19 эпизодов по уголовному делу, потерпевшие – жители разных городов России. Преступница К. в сети «Интернет» создавала аккаунты, размещала информацию о продаже различных товаров, в том числе бытовой техники, фенов, пылесосов, утюгов, дорогой одежды. Под предлогом поставки она требовала стопроцентную предоплату, давала реквизиты карты своего мужа. Естественно, никаких поставок не осуществляла. Общий ущерб составил более 800 тысяч рублей.

Фейковый BlaBlaCar

В полиции Магнитогорска рассказали: участились случаи хищения денежных средств через сервис поиска попутчиков. Мошенники просят оплатить поездку и присылают ссылку на оплату. После того, как человек вводит все данные банковской карты, включая CVC-код, со счёта списывают средства. Так, жительница Магнитогорска перешла по такой ссылке для бронирования поездки, но перевести деньги не получилось. «Водитель» отменил бронь, сообщив, что все места уже заняты. Спустя пару дней женщина обнаружила, что с карты исчезли все деньги – около 13 тысяч рублей.

Звонок из «органов»

В начале марта в отдел полиции «Правобережный» обратился 58-летний житель Магнитогорска. Он рассказал, что ему позвонил представитель якобы силовых структур и под предлогом того, что со счёта потерпевшего пытаются похитить деньги, убедил перевести средства «на безопасные счета». Мужчина отправился к банкомату и сделал более 25 переводов по 15 тысяч рублей на неизвестные счета. Ущерб составил более 415 тысяч рублей.

Аналогичным образом мошенники обманули 75-летнюю пенсионерку, только там ущерб оказался значительно выше – три миллиона рублей. Преступники даже обеспечили транспортом потерпевшую, а во время общения запретили ей с кем-либо общаться, пояснив, что «идёт проверка утечки информации».

Уловки мошенников

– Всех подкупает профессионально поставленный голос, использование финансовых терминов, – объясняет Мария Морщакина. – Мошенники используют и приёмы психологического давления, начинают торопить, мол, время уходит, вы можете лишиться крупной суммы... Человек теряет, паникует, всё это на руку преступникам. Ведь в состоянии паники сложно мыслить рационально. В числе уловок – рабочий «шум», создающий атмосферу настоящего кол-центра, перевод с одного специалиста на другого, чтобы человек поверил, что ему действительно позвонили из официальной организации.

Для обмана мошенники используют технологию подменных номеров. Но не все знают о такой возможности, чем преступники активно пользуются. У вас на телефоне может высветиться официальный номер банка, любой государственной организации. Так, жертвы обмана в полиции рассказывали, что им звонили из ГУ МВД России по Челябинской области, уверяли, что всё официально, и в доказательство предлагали зайти на сайт МВД, посмотреть контакты и убедиться, что звонок поступил с официального номера. В итоге «помощь в расследовании уголовного дела» оборачивалась кражей денежных средств.

Использование подменного номера помогает мошенникам втереться в доверие. Если жертва поверит, что с ней разговаривают официальные представители банка или государственных структур, то убедить её сообщить все необходимые сведения или выполнить перевод средств

труда не составит. Поэтому важно запомнить – даже если звонок поступил с официального номера, ни в коем случае не сообщайте данные карты, пароли и коды доступа, не совершайте никаких переводов, ни в коем случае не устанавливайте никаких приложений на телефон. Можете сослаться на занятость или просто положить трубку и перезвонить самостоятельно по номеру банка или организации.

Фишинговые сайты

Фишинговые сайты собирают информацию пользователей, которую потом используют для совершения киберпреступлений. Это могут быть логины и пароли, дающие мошенникам возможность зайти на реальный аккаунт жертвы на любом сайте, в том числе и на защищённую банковскую страницу. В случае поддельной платёжной страницы мошенники получают информацию обо всех реквизитах карты, позволяющих списать средства со счёта пострадавшего.

Фишинговые сайты выглядят как точные копии сайтов, которым мы привыкли доверять. Мошенники подделывают даже сайт госуслуг, рассылая потенциальным потерпевшим письма о якобы полагающихся выплатах. Так, с помощью фишинговой платёжной страницы была обманута женщина, попытавшаяся воспользоваться сервисом BlaBlaCar. Так как у неё не был подключён мобильный банк, о списании средств со счёта она узнала только спустя пару дней, когда отправилась в магазин и выяснила, что на карте нет средств. Чтобы заметить поддельную страницу, нужно быть очень внимательным. Иногда различие заключается в одной букве, знаке или цифре.

Вернутся ли деньги?

В ГУ МВД России по Магнитогорску создано оперативное отделение по расследованию кибермошенничеств. Сотрудники регулярно выезжают в командировки в разные города страны, ведь преступники территориально могут находиться где угодно.

– Существует определённый алгоритм действий, но граждане должны понимать, что возврат похищенных средств – длительная процедура, – объясняет Мария Морщакина. – Осложняет расследование то, что мошенники зачастую убеждают граждан подождать несколько дней, пока деньги найдутся «на безопасном счёте». Только не дождавшись обещанного возврата, человек понимает, что попался на удочку мошенников. Начинает советоваться с родственниками, снова

время уходит. К моменту, когда он решает подать заявление в полицию, иногда проходят недели.

Осложняет работу следствия и то, что человек, поняв, что его обманули, начинает удалять все смс-сообщения, вызовы и другу важную информацию, которая могла бы помочь быстрее выйти на след преступников. Приходится дополнительно запрашивать детализацию звонков через сотового оператора, что тоже требует времени.

– В МВД Магнитогорска работают опытные сотрудники уголовного розыска, которые раскрывают такие преступления по всей России, – отмечает Николай Жвыкин. – Раскрываемость таких преступлений в городе на уровне 30 процентов.

– Каждый день по городу пять-семь обращений, – добавляет Татьяна Шапкина. – Деньги часто удаётся вернуть. Так, сейчас в производстве находится дело, на счету мошенников около 300 тысяч рублей, все они были переведены с банковских карт потерпевших. Сейчас на деньги наложен арест. Когда оформляют кредиты – эти денежные средства застрахованы банком и являются собственностью банка. И не принадлежат жертвам мошенников. То есть, физическое лицо в данном случае ущерба не несёт, оно обращается с заявлением в полицию, органы внутренних дел реагируют, проводят проверку и признают потерпевшим банк. Хотя банки часто с этим не согласны и пытаются обжаловать через суды. Физлицо в данном случае ничего выплачивать не должно, так как оно было введено в состояние заблуждения.

МВД предупреждает

Чтобы обезопасить финансы, помните: не важно, с какого номера идёт звонок, пусть даже со знакомого. Как только звучит фраза: «Я сотрудник службы безопасности банка» необходимо сразу же отключить телефон и перезвонить в банк самостоятельно. Помните, номера горячих линий работают только на входящие звонки.

Также в МВД советуют – если вы активно совершаете покупки через Интернет, заведите для них отдельную систему. Важно разделить «входящие» и «исходящие» финансовые потоки. Не расплачивайтесь картой, на которую поступают денежные средства. Для совершения покупок переводите с неё ровно ту сумму, которую планируете списать. Даже если мошенники смогут завладеть данными «платёжной» карты, они не смогут воспользоваться вашими средствами.

Мария Митлина