Будь начеку!

И до судов добрались

Южноуральцев предупреждают о мошенничестве с повестками в суд. Мошенники звонят гражданам с действующими судебными разбирательствами и представляются помощниками судей. Подробно описывают суть дела, называя его номер, фамилию судьи и участников процесса (вся эта информация в открытом доступе, поэтому узнать сведения не составляет труда). Затем злоумышленники предлагают получить уведомление о дате заседания или необходимые документы через сайт госуслуги. Для подтверждения согласия просят сообщить код из смс. Так они пытаются попасть в личный кабинет, чтобы завладеть персональной информацией. Государственные органы никогда не запрашивают подобных данных.

Заплатила за несуществующий товар

В дежурную часть полиции Озёрска обратилась местная жительница. Её обманули при покупке товара в сети интернет.

Потерпевшая нашла подходящие строительные материалы на сайте бесплатных объявлений и связалась с продавцом через чат торговой интернет-площадки. Далее общение продолжилось по телефону, а после –в одном из мессенджеров. Для большей убедительности продавец сказал, что он сотрудничает с местным магазином. Женщина заплатила полную стоимость товара, включая доставку, и ждала заказ к обговоренной заранее дате. В итоге товар так и не был доставлен, продавец перестал выходить на связь, а объявление было удалено. Женщина, осознав, что на самом деле общалась с мошенником, обратилась в полицию. Сумма ущерба составила 16 тысяч рублей. Возбуждено уголовное дело по статье «Мошенничество».

Полицейские не рекомендуют отправлять полную или частичную предоплату незнакомым людям, а также:

- передавать данные банковских карт (в том числе CVV/CVC-код банковской карты или коды из смс от банка);
- переходить по ссылкам, которые присылают другие пользователи;
- обсуждать подробности сделки по телефону или в сторонних мессенджерах.

Вам телеграмма ... с вирусом



Россиян предупредили о мошенничестве с фотографиями в телеграмм.

В МВД России рассказали о новой схеме обмана россиян, направленной на кражу денег с банковских счетов. Неизвестные рассылают в телеграмм файл, замаскированный под фото, и вынуждают пользователя скачать его. После этого на телефон устанавливается вирусная программа. В полиции предупредили, что неизвестные присылают файл с расширением apk и сообщение: «Привет, это ты на фото?». На первый взгляд файл действительно выглядит как фото, однако расширение у него – программное. Не заметив этого, пользователь скачивает файл, и на его смартфон устанавливается вирусная программа. После этого злоумышленники получают доступ ко всем приложениям, в том числе банковским. Полицейские призывают пользователей быть бдительными, ни в коем случае не скачивать файлы, тем более от незнакомцев, а также предупредить о новой мошеннической схеме близких людей.

Хищений меньше – суммы больше

Тенденция. Количество краж и мошенничеств с использованием IT-технологий постепенно уменьшается, но при этом суммы ущерба становятся всё более значительными

АНАСТАСИЯ **ЛАТЫПОВА**



Об этом нашей газете рассказал начальник уголовного розыска межмуниципального отдела МВД России «Кыштымский» Андрей ЕФАНОВ.

Спохватилась через полгода

Несмотря на постоянные предупреждения, кыштымцы продолжают верить обманщикам и переводят им свои (и кредитные) деньги.

В Кыштымском городском округе по итогам девяти месяцев 2024 года зарегистрировано 128 краж и мошенничеств, совершённых с использованием телекоммуникационных технологий. В прошлом году за аналогичный период их было 137. Немного уменьшилась и раскрываемость таких преступлений – в прошлом году было раскрыто 39, в этом – 35.

– Пострадавших стало меньше, однако суммы, которые у них похищают, увеличились, – отметил подполковник полиции. – Наглядный пример – в сентябре жительницу нашего города обманули на шесть миллионов рублей. Она увидела в телефоне рекламу дополнительного заработка, перешла по ссылке, почитала комментарии о инвестиционной площадке и поверила, что таким способом можно заработать. Пенсионерка позвонила по указанному на сайте номеру телефона, и «специалисты» пообещали ей помощь. С мая по сентябрь женщина совершила более 50 банковских операций и в общей сложности перевела мошенникам более шести миллионов! Только спустя полгода она начала сомневаться в своих действиях и обратилась полицию.

В последнее время основным видом мошенничества остаются звонки от «липовых» сотрудников банков, которые предлагают защитить средства от хищения. «Защищают» всё подчистую – и личные сбережения граждан, и кредитные средства… Мошенники ничем не брезгуют. Нередко предлагают своим жертвам «заработать» на бирже, на различных торговых площадках, на акциях и маркетплейсах.

– Мошенники, как правило, используют два базовых сценария. Они либо предлагают что-то заманчивое – скидки, выплаты, бонусы, либо запугивают, например, потерей денег, уголовным преследованием, оформлением кредита на ваши паспортные данные и так далее, – предупреждает Андрей Викторович. – Стоит отметить, что основная часть потерпевших была осведомлена о телефонных мошенничествах, но это не остановило их при переводе денежных средств преступникам.

В пособниках даже подростки

По наблюдениям полицейских, в Кыштыме чаще всего регистрируются три вида мошенничества: звонок из банка, звонок от сотрудника портала госуслуг и вложения в инвестиции. Только с начала октября двадцать жителей города обратились в дежурную часть полиции с сообщениями о том, что они лишились доступа к госуслугам из-за действий мошенников.

Как правило, злоумышленники звонили гражданам под видом сотрудников сотового оператора. Сообщали, что срок действия сим-карты истекает, и скоро услуги связи будут ограничены, поэтому необходимо в срочном порядке продлить срок действия договора. Для этого необходимо сообщить код, который поступит в смс. Доверчивые кыштымцы диктовали код из шести цифр, и мошенники получали доступ к личному кабинету на портале госуслуг, а в некоторых случаях и вовсе ограничивали доступ в него для настоящего владельца.

– Раньше жертвами телефонных мошенников, в основном, были пожилые люди, – говорит Андрей Ефанов. – Но в последнее время на удочку проходимцев всё чаще попадается молодёжь и даже подростки. Самое страшное, что мошенники не просто обманывают подростков, но и вовлекают их в свои преступные схемы, тем самым, делая их соучастниками преступления. Мошенники используют различные предлоги, чтобы вовлечь молодёжь в противоправную деятельность. Задержанные курьеры, роль которых зачастую как раз и выполняют несовершеннолетние, поясняют, что в поисках работы оставляли резюме через сервис объявлений. Вскоре с ними связывались неизвестные и предлагали работу в качестве «выездных финансовых специалистов». Другими словами, курьеры должны забирать по конкретному адресу деньги, а затем переводить их на счета «работодателей». Также преступники озвучивают предполагаемый заработок, но не сообщают информацию о том, что, помимо запятнанной репутации, фигуранту уголовного дела предстоит в полном объёме компенсировать причинённый ущерб потерпевшим. Как правило, полученное вознаграждение составляет небольшой процент от той суммы, которую подростки переводят своим «работодателям» на неизвестные счета.

Уважаемые родители! Поговорите с детьми о том, что предложения, поступающие в сети интернет о возможном лёгком заработке, основаны на совершении противоправных деяний. Прежде, чем согласиться на такую «работу», необходимо тщательно проверить всю информацию и помнить, что отвечать придётся по всей строгости закона.

Как же всё-таки обезопасить себя, своих родных и не угодить в ловушку мошенников? Ответ очень простой: не отвечать на звонки с незнакомых номеров, а если вы ответили, всегда помните: ни один сотрудник банка, прокуратуры, полиции, следственного комитета не звонят гражданам и тем более не просят сообщать какие-либо коды или переводить денежные средства.

Если с вами пытаются провести какие-то манипуляции, не предпринимайте поспешных действий. Просто прекратите разговор. Или ответьте: хорошо, я проверю эту информацию. Положите трубку, самостоятельно перезвоните в банк или родственникам.

Если вы уже перевели деньги и поняли, что вас обманули, не тяните время. Сразу обращайтесь в банк и просите заблокировать ваш счёт и денежный перевод. Если банк успеет ограничить доступ к счёту, наложить свой запрет на перевод, то есть шанс вернуть денежные средства. Если, конечно же, мошенник не успел их снять. Обычно они делают это сразу. Но в редких случаях всё-таки удаётся их опередить.

Полицейские также советуют установить в банковском приложении ограничение по размеру суммы денежного перевода за сутки. А в госуслугах – оформить самозапрет на оформление кредитов и проведение операций с недвижимым имуществом без личного присутствия. Кстати, по статистике, среди пострадавших лишь единицы тех, кто пользуется простыми кнопочными телефонами. Практически все пострадавшие – это пользователи смартфонов, на которых установлены различные мобильные приложения.

Будьте бдительны и помните: сохранность ваших сбережений – в ваших руках!