Типовая лекция
по профилактике преступлений в сфере
информационно-телекоммуникационных технологий.

На территории Оренбургской области в преобладающем большинстве хищения с использованием информационно-телекоммуникационных технологий совершаются следующими способами:

1) Звонки от псевдо операторов сотовой связи, пенсионного фонда России, почтового отделения, которые под предлогом продления договора услуг связи, улучшения качества связи, получения дополнительных пенсионных выплат, перерасчета пенсии, получения заказного письма, доставки, посылки просят сообщить смс-коды, поступившие на телефон. После сообщения данных кодов поступает звонки с других номеров, где мошенники представляются сотрудниками банков, полиции, Следственного комитета, ФСБ России, Росфинмониторинга и сообщают, что ранее поступал звонок от мошенников, которые получили код из смс-сообщения, пытаются похитить денежные средства. С целью предотвращения хищения денежных средств убеждают граждан пойти в банки, где снять все сбережения со счетов, через банкомат перевести их на «резервный», «безопасный» счет или передать их через курьеров для последующего декларирования. При этом поясняя, что курьер денежные средства поместит в специальную ячейку Центрального банка, а после чего купюры будут проверены на подлинность и после проверки возвращены потерпевшему.

2) Заработок на инвестициях. Данные преступления совершаются в результате поиска потерпевшими дополнительного источника дохода. Как правило, потерпевшие оставляют в сети интернет заявку на регистрацию и спустя некоторое время им перезванивает злоумышленник, который представляется брокером и предлагает создать личный кабинет на платформе одной из бирж либо перечислить денежные средства для инвестирования. После чего жертва под влиянием злоумышленника систематически перечисляет денежные средства различными сумма на лицевой счет, который отображается в личном кабинете биржи либо на банковские карты мошенников, думая, что инвестирует денежные средства. Злоумышленник, в свою очередь, закрывает доступ к личному кабинету и потерпевший не может вывести данные денежные средства. Для этого его убеждают в необходимости внесения дополнительной суммы денег;

Если Вы все - таки решили заработать данным видом, то следует играть на проверенных биржах, а также пользоваться услугами проверенных лиц (брокеров), занимающихся данной деятельностью. Также следует осознавать риск потери своих денежных средств при игре на бирже, инвестировании, в том числе очень крупных сумм.

3) В настоящее время увеличилось количество киберпреступлений, связанных с оформлением займов в микрофинансовых организациях на граждан третьими лицами, используя их персональные данные через портал Госуслуг, доступ к которому преступники получают при использовании кодов из смс-

сообщений, которые граждане сообщают псевдо сотрудникам сотовых компаний, пенсионного фонда, почтового отделения и других структур, оказывающих услуги. Кроме того доступ к порталу услуг мошенники могут получить используя старый абонентский номер, который был привязан ранее.

В указанных случаях необходимо немедленно прекратить разговор, позвонить по номеру «горячей линии» банковского учреждения, организации в сфере оказания социальных услуг, либо лично посетить офисы и поинтересоваться по поводу сомнительных манипуляций.

Запомните! Сотрудники банка, работники салонов операторов связи никогда не спрашивают по телефону коды из СМС и персональные данные банковских карт. Не существует такого вида сохранения средств, как внесение наличности через терминал на «резервный» счёт либо перевод на абонентский номер. Ни в коем случае не устанавливайте в своем смартфоне либо компьютере какие-либо программы по просьбе неизвестного лица. Также при прекращении пользования абонентским номеров необходимо отвязать его от всех банковских приложений и личного кабинета портала Госуслуг.

4) Установка приложений удалённого доступа под видом программного обеспечения, повышающего банковскую безопасность. Данные приложения открывают доступ к удалённому использованию смартфона и позволяют переводить денежные средства на подконтрольные злоумышленникам счета, оформлять кредиты, использовать персональные данные.

Преступники при помощи ссылок широко начали распространять вирусное программное обеспечение т.н. (APK.файл), которое самостоятельно устанавливается на смартфон и предоставляет возможности удалённого доступа к устройству, в том числе полный контроль над приложениями в смартфоне, беспрепятственный вход в мобильные приложения банков и т.д. При этом для отправки ссылок на указанные программы преступники используют различные предлоги, в том числе плановое обслуживание населения сотрудниками «Энергосбыта» (бесплатная замена и поверка счетчиков), пенсионного фонда (перерасчет пенсии), часто внимание потерпевших привлекают, играя на их любопытности, путём отправки ссылки в мессенджере с названием «Посмотри, это ты на фото (видео)».

Если же Вы по каким-то причинам установили на смартфон неизвестное приложение и заметили нестабильное его функционирование, то немедленно отключите Интернет соединение, что позволит прервет сеанс удалённого управления Вашим устройством. После чего предпримите меры по удалению установленного приложения.

5) Использование аккаунтов в мессенджерах, созданных от имени руководителей, для осуществления переписки, в ходе которой преступники просят перечислить деньги в долг на банковскую карту, либо оказать содействие правоохранительным органам в поимке преступников в банковской сфере. Далее, как правило, гражданину звонят неизвестные, представляющиеся сотрудниками силовых структур (ФСБ, МВД) и под предлогом его

задействования в «спецоперации» по установлению преступников, убеждают оформить кредиты, снять личные сбережения и переводить деньги на подконтрольные им счета;

Если в мессенджере Вам написал руководитель и попросил деньги в долг, либо сказал, что с Вами должны связаться сотрудники правоохранительных органов и им необходимо помочь, а также неукоснительно выполнять их указания, не рискуйте, а просто перезвоните ему, либо свяжитесь другим удобным способом, который позволит понять, что с Вами на связи именно руководитель, а не преступник.

6) Взлом социальных сетей или аккаунтов в мессенджерах, и осуществление рассылки сообщений с просьбой одолжить денежные средства, либо перейти по ссылке и проголосовать за кого-либо;

Если Ваш знакомый в социальной сети просит деньги в долг, необходимо связаться с ним по телефону, либо убедиться в ходе переписки, что с Вами общается именно он, а не мошенник, у которого в пользовании находится взломанная страница знакомого.

7) Мошенничество на торговых интернет-площадках. Для этого, как правило, мошенники предлагают перейти для общения в мессенджеры, договариваются о получении (отправке) товара с помощью служб доставки, скидывают интернет – ссылку на поддельные сайты, где жертва вносит реквизиты банковской карты и лишается денежных средств.

Запомните! Торговые площадки оснащены системой защиты от сомнительных операций по переводу средств, позволяющей блокировать различные ссылки, поэтому если Вас покупатель/продавец просит перейти к общению в мессенджере и кидает ссылку, то это первый тревожный сигнал к тому, что Вас хотят обмануть. Зачастую ссылки, отправляемые преступниками, по названию могут быть схожи с названиями различных компаний по доставкам товара, даже с названиями самих торговых площадок. Не переходите по ссылкам, отправленным неизвестными лицами.

8) Популярность в преступной среде набирает способ использования удалённого приобретения товаров в сети Интернет посредством приложений крупных торговых площадок (маркетплейсов). Преступники, выступая в качестве продавцов, размещают объявление о продаже различного товара по выгодней цене. После оформления покупателем доставка выбранного товара в указанный срок в пункт выдачи умышленно не осуществляется, в связи с чем покупатель вынужден обратиться в адрес технической поддержки маркетплейса с претензией о возврате товара, о чем сообщается недобросовестному продавцу. В ходе разбирательства по неисполнению денежно-товарных обязательств псевдо продавцы инициативно выходят на связь с покупателем и предлагают отменить ранее сделанный заказ (так как возникли технические проблемы на сайте «OZON») и осуществить новый. Покупатели в мессенджере («WhatsApp» или «Telegram») проходят по предоставленной им ссылке и попадают на

«фишинговый» сайт «OZON», где осуществляют оплату товара, тем самым лишаются денежных средств.

Кроме того, не теряет актуальности способ совершения хищений денежных средств в сети Интернет под предлогом дополнительного заработка. Лицам за определённую сумму предлагают оценивать товары в приложении «OZON» с целью повышения их рейтинга популярности. Наряду с оценкой потерпевшему даётся задание на приобретение за свой счет дорогого товара под предлогом того, что в дальнейшем стоимость вернётся на счёт покупателя вместе с денежной выплатой за оценку товара. Хищение денежных средств происходит на стадии покупки товара большой стоимости, после внесения суммы на подконтрольные преступникам счета.

Если Вы столкнулись с тем, что покупатель в маркетплейсе не вовремя доставил товар, после чего просит отказаться от заказа, а также предлагает продолжить дальнейшие товарно-денежные отношения напрямую без участия маркетплейса, перейдя по ссылке в мессенджере, будьте осторожнее, это могут быть мошенники.

9) Среди потерпевших от действий мошенников нередко становятся и дети. Играя в онлайн-приложении на телефоне, подростки в чате получают различные сообщения, связанные с улучшением качества игры. Затем в переписке дети рассказывают о том, с кем они сейчас находятся и есть ли у них доступ к телефонам взрослых. Далее их убеждают продиктовать конфиденциальные данные, которые поступили на телефонные номера родственников. После чего происходит списание денежных средств.

Необходимо довести до детей информацию о различных уловках мошенников, в том числе о схемах, где под разным предлогами злоумышленники побуждают их сообщать конфиденциальную информацию взрослых, например, реквизиты банковских карт.

10) Мошенническая схема «родственник попал в беду». Осуществляется звонок, где представитель якобы правоохранительных органов сообщает пожилому человеку, что по вине его близкого родственника совершено ДТП и для урегулирования ситуации необходима крупная денежная сумма наличными, после чего приезжает курьер мошенников, забирает деньги и переводит на счета кураторов преступной схемы;

Будьте внимательны! При поступлении подобных звонков, несмотря на уговоры преступников о том, что не стоит звонить никому, немедленно свяжитесь с родственником, который попал в «беду».

В разговоре сохраняйте спокойствие и не называйте данные родственника, скажите неизвестному, что будете по данному факту обращаться в правоохранительные органы.