Предлагаем поговорить на тему, которая может коснуться каждого. Речь **о финансовом и кибермошенничестве**.

Больше 70% жителей России убеждены, что никогда не попадутся на обман телефонных мошенников. Но самоуверенность не защищает сбережения. Когда человек считает себя неуязвимым, это может сыграть на руку аферистам.

Даже несмотря на то, что люди знают, что не стоит верить звонкам с незнакомых номеров и рассказам лжесотрудников службы безопасности, они все равно рискуют попасться на уловки мошенников и потерять деньги.

Большинство хищений происходит с помощью злоупотребления доверием. То есть мошенники специально оказывают психологическое воздействие на человека, заставляют его самого раскрывать конфиденциальную, секретную информацию.

Обычно, прежде чем выйти на контакт, злоумышленники стараются узнать о человеке как можно больше. Нередко люди и сами публикуют в соцсетях номера телефонов, электронные адреса и даже выкладывают фотографии своих банковских карт.

Этой информации недостаточно, чтобы украсть деньги. Но вполне хватит, чтобы начать разговор и усыпить бдительность. Когда махинаторы обращаются к людям по имени и отчеству, сами называют номер карты или другие конфиденциальные данные, кажется, что они действительно представляют знакомую организацию или человека.

Мошенники могут найти подход практически к любому человеку, используя различные техники. Они почти всегда безошибочно определяют, с кем разговаривают: с доверчивым или скептически настроенным человеком, с тревожным или спокойным. Исходя из этого они выбирают стиль коммуникации и тон разговора.

Также злоумышленники выясняют данные человека с помощью фишинговых сайтов.

Фишинг – это один из видов интернет-мошенничества, своеобразная «ловля на живца» с помощью массовых рассылок СМС-сообщений или сообщений по электронной почте, содержащих ссылки на ложные сайты.

Имитируя интернет-ресурсы государственных ведомств, справочно-правовых систем, популярных компаний, они рассчитывают, что пользователи не заметят подделку и введут важную информацию: например личные или финансовые данные, логин и пароль, контактные сведения. Получив данную информацию, мошенникам будет легче обмануть человека.

Аферисты стали чаще выманивать деньги в соцсетях и мессенджерах с помощью поддельных видеосообщений. Они создают виртуальные копии реальных людей и рассылают сообщения от их имени. Мошенники взламывают чужой аккаунт, берут из него фотографии, видео- и аудиозаписи человека и загружают их в нейросеть. Искусственный интеллект анализирует черты лица, движения, голос и создает дипфейк – цифровой образ, максимально похожий на свой прототип. Затем преступники записывают ролик с виртуальным двойником. Он говорит, что оказался в беде, например, серьезно заболел, попал в аварию или лишился

работы, и просит помочь ему деньгами. Это фальшивое видео обманщики рассылают родным, друзьям и коллегам человека и добавляют свои реквизиты для перевода денег.

Прежде чем переводить какие-то суммы, лучше позвонить знакомому и убедиться, что ему действительно нужна помощь. Если нет возможности поговорить по телефону или лично, в сообщении задайте человеку вопрос, ответ на который знает только он.

Я бы обратил внимание на факты вовлечения населения, проживающего на территории республики, в особенности – молодежи, в преступные финансовые схемы в качестве подставных лиц, так называемых «дропов», на которых оформляются банковские карты и расчетные счета.

Часто люди даже не догадываются, что участвуют в чем-то нелегальном. Обычно аферисты предлагают людям несложную подработку. Они распространяют информацию о вакансии через соцсети, мессенджеры, сайты объявлений и даже с помощью листовок на улицах. Приглашают всех желающих — для трудоустройства не нужны какие-либо знания и опыт, достаточно банковской карты или онлайн-банка. Поэтому дропперами могут стать самые разные люди — от школьников до пенсионеров.

Чтобы человек не заподозрил, зачем на самом деле нужны его карты и счета, мошенники используют разнообразные легенды.

Одна из таких – «Получи должность администратора лотереи». Человеку говорят, что он должен перечислять призовые деньги победителям розыгрыша или отправлять прибыль участникам инвестиционного проекта. Обычно организаторы дают путаные объяснения, почему не могут сделать переводы сами. Но зачастую людей, которые ищут хоть какую-то подработку, такие детали даже не интересуют. В реальности на номер счета или карты «администратора» приходят ворованные деньги. Затем их нужно переслать другим дропперам, участвующим в цепочке, или самим преступникам.

Еще одна популярная легенда – «Выручи менеджера банка». Мошенники представляются банковскими сотрудниками, которым нужно выполнить план по выдаче карт. Они предлагают заработать, к примеру, от 1 500 до 5 000 рублей за совершение нехитрых действий. Нужно оформить карту и сразу отдать ее «сотруднику» или предоставить ему доступ к онлайн-банку. За друзей, которые тоже откроют карту, дают бонус. В такие схемы легко втягиваются подростки – они могут открывать собственные карты уже с 14 лет. При этом преступникам даже не надо просить человека что-либо делать, все операции они проводят сами. Главное – завладеть картой или доступом к онлайн-банку.

Актуальной остается легенда под условным названием «Стань внештатным сотрудником полиции». Обманщики выдают себя за сотрудников правоохраны и убеждают человека помочь следствию. По легенде, полицейские уже нашли преступников, но хотят поймать их с поличным. Для этого доброволец должен притвориться соучастником

мошенников и получить на свою карту украденные деньги. Затем нужно не переправлять их аферистам, а снять и отдать следователям. За работу гарантируют вознаграждение. Если человек хорошо себя проявит, то обещают официальное трудоустройство в МВД. Но по факту доброволец не изображает дроппера, а становится им. Ему приходят ворованные деньги, и он передает их самым настоящим преступникам.

В некоторых случаях речь даже не идет о работе. Человеку приходит на счет большая сумма, а затем ему звонит или пишет незнакомец и утверждает, что перевел деньги по ошибке. Просит вернуть их по номеру телефона или карты. На самом деле перевод приходит от человека, которого мошенники уже обманули. Теперь они хотят, чтобы получатель денег перекинул сумму им. Иногда за эту услугу могут предложить вознаграждение. Если человек согласится, то, сам того не ведая, окажется дроппером.

Обратите внимание!

Обманутый мошенниками человек переводит деньги дропперу. Именно его он считает преступником – сообщает о случившемся в свой банк и подает на него заявление в полицию. Собрать больше информации о нем удается по номеру телефона, банковской карты или счета.

Уголовным кодексом предусмотрена ответственность для дропперов (лиц передающих свои электронные средства платежа другим людям для совершения преступлений).

Кроме того, хочу обратиться к молодежи. В республике есть примеры, когда, школьники выступала в качестве курьеров, забирали денежные средства у обманутых и после чего перечисляли их на указанные им счета, при этом оставляя себе небольшую сумму. Предупреждаю, что даже не знание факта совершения преступления не освобождает от уголовной ответственности, кроме того, с курьера будут взысканы все денежные средства, не только которые он оставил себе и остальную часть суммы.

Поэтому призываю всех слушателей не доверять звонкам неизвестных вам лиц и перепроверять информацию в официальных источниках.

Говоря в целом о финансовом мошенничестве, необходимо понимать, что в большинстве случаев люди отдают свои деньги мошенникам сами, находясь под заблуждением. С каждым днем появляются все новые и новые мошеннические схемы. Несмотря на внешнее многообразие мошеннических легенд, злоумышленники всегда 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 т.д.

Чтобы не попасться на уловки мошенников, рекомендую:

– прервать разговор, если позвонил незнакомый человек и завел речь о деньгах;

– при возникновении сомнений относительно сохранности денег на счете самостоятельно набрать номер телефона банка, который указан на карте или на официальном сайте финансовой организации;

– сохранять бдительность и не действовать второпях;

– никогда не сообщать личные и финансовые данные посторонним лицам, под каким бы предлогом их ни пытались узнать;

– не переходить по подозрительным ссылкам, которые поступают по смс, в почте или мессенджерах.

Хочу до Вас донести одну простую истину. Все эти схемы «помощь МВД, ФСБ поймать преступников и для этого вам нужно перевести деньги на безопасный счет или передать следователю» являются мошенническими. Даже если кого-то из Вас привлекут к оперативно-розыскному мероприятию, то для начала вас пригласят в здание соответствующего ведомства, где пол дня будут оформлять соответствующие документы с приглашением понятых с подробными инструкциями и самое главное денежные средства для операции Вам предоставит правоохранительный орган, а не будут использовать ваши деньги. ЗАПОМИТЕ ни один правоохранительный орган не будет просить вас перевести или снять ваши денежные средства.

Если мошенникам все же удалось совершить хищение, человеку необходимо выполнить три основных действия.

Во-первых, немедленно заблокировать банковскую карту с помощью мобильного приложения, личного кабинета на сайте банка, через контакт-центр банка или в любом его отделении.

Во-вторых, в течение суток необходимо написать заявление в отделении банка о несогласии с операцией и взять выписку по счету.

В-третьих, нужно как можно скорее написать заявление в ближайшем отделении полиции.

Обращение в полицию необходимо для того, чтобы повысить вероятность привлечения злоумышленника к ответственности.

Действенный способ избежать денежных потерь – критически воспринимать любые предложения. Мошенники специально торопят, чтобы лишить человека возможности принять взвешенное решение в спокойной обстановке. Они требуют немедленно перевести деньги, срочно оплатить какую-либо услугу, «как можно скорее» назвать секретный номер, пароль или код. Если вы чувствуете явное давление, когда пытаетесь принять какое-либо финансовое решение, это верный признак, что вы имеете дело с мошенниками.

Ребята будьте бдительны.

Спасибо! До новых встреч!