Сотрудники полиции обращаются к жителям района быть бдительными и не поддаваться на уловки мошенников

Текущее состояние криминогенной ситуации в Алтайском крае характеризуется устойчивой тенденцией роста хищений денежных средств, совершаемых с использованием информационно-телекоммуникационных технологий. За три года количество зарегистрированных преступлений данного вида увеличилось более чем в 2,5 раза: если в 2019 году число таких преступлений ровнялось 4153, то в 2021 зарегистрировано 9397 преступлений. Не стал исключением и 2022 год.

По итогам прошедших четырех месяцев 2022 года число возбужденных уголовных дел данной категории составило 3274 что в целом соответствует аналогичному показателю прошлого года.

Способы совершения преступлений постоянно изменяются, злоумышленники оперативно реагируют на меры профилактики, проводимые правоохранительными органами, кредитно-финансовыми организациями и СМИ.

На сегодняшний день к наиболее массовым видам дистанционных хищений можно отнести преступления, совершаемые следующими способами:

1. Звонок от имени сотрудника банка, сотрудников службы безопасности либо правоохранительных органов.
2. «Ваш родственник попал в беду!».
3. Звонок от специалиста портала «Госуслуги» с информацией о взломе страницы.
4. Инвестирование денежных средств в различные «финансовые пирамиды» и инвестиционные фонды.
5. Купле-продажа товаров на различных торговых площадках в сети Интернет (Авито, Юла, Дром и т.д.).
6. Выплаты компенсаций за ранее приобретенные медицинские препараты, либо участие в «финансовых пирамидах».
7. Дистанционные услуги гадалок, целителей и т.д.
8. Звонок в торговую точку, либо собственника.
9. Вымогательство денежных средств в сети Интернет за нераспространение сведений интимного характера.

Для того, чтобы понять, как работает мошенническая схема, а также не стать жертвой мошенников предлагаю рассмотреть каждый вид преступной деятельности более подробно.

1. Звонок от имени сотрудника банка:

На сегодняшний день один из самых популярных способов хищения денежных средств. Злоумышленники, используя различные софты и программы, позволяющие осуществить замену номера, с которого поступает звонок. В связи с этим принимающая сторона действительно видит телефоны, похожие или полностью повторяющие горячие линии банков, дежурных частей, иных официальных органов и организаций, которые зачастую могут начинаться с цифр 8-800… или 8-495..

Как правило, звонящий, который представляется сотрудником безопасности банка или правоохранительных органов сообщает о том, что на банковском счете замечены подозрительные операции и для того, чтобы «обезопасить» деньги, нужно перевести их на другой счет, либо оформить кредит, чтобы «вычислить преступника».

Так гражданке «З» на сотовый телефон позвонил неизвестный, который представился сотрудником службы безопасности ПАО «Сбербанк» и сообщил, что на ее имя пытаются оформить кредит, чтобы злоумышленники не похитили ее денежные средства, ей необходимо самой оформить кредит и перевести денежные средства на безопасный счет. После чего гражданка «З» оформила кредит на сумму 1 345 000 рублей, обналичила денежные средства и через банкомат перевела вышеуказанную сумму на банковскую карту.

Нельзя поддаваться на подобные настоятельные просьбы. Необходимо положить трубку и сделать ответный звонок. Ответный звонок позволит попасть на настоящую «горячую» линию банка, страховой компании или в дежурную часть полиции. Там подтвердят, что никто не имеет права интересоваться вкладами конкретных граждан.

2. **«Ваш родственник попал в беду!»:**

В данном случае мошенники звонят на домашние телефоны своих жертв и представляясь родственником, знакомым рассказывают, неразборчивым (либо плачущим) голосом говорят что они совершили ДТП, в ходе чего пострадали люди, затем они быстро передают трубку другому человеку, который как правило представляется сотрудником правоохранительных органов и сообщает о том, что потерпевшему нужна дорогостоящая операция и указывают на необходимость передать крупную сумму денег. Потерпевших как правило просят передать денежные средства курьеру, в более редких случаях отправить денежные средства на банковский счет.

28.04.2022 около 19:00 гражданке «В», позвонили на стационарный телефон, звонивший представился сыном и сообщил, что попал в аварию в результате которой пострадала девушка. Затем трубку взял якобы следователь и попросили заплатить за лечение данной девушки 800 000 рублей. Ввиду того, что данной суммы не было, гр. «В» передала прибывшему по ее адресу курьеру денежные средства в сумме 230000 рублей.

Чтобы не стать жертвой данного вида мошеннических действий, необходимо с сотового телефона позвонить своим родственникам. Если сотовый телефон одного из родственников занят, нужно дозваниваться до других. Поскольку злоумышленники осуществляют звонки из-за пределов Алтайского края, то всем пожилым гражданам, в случае отсутствия острой необходимости в междугородних звонках, нужно отключить данную услугу в АО «Ростелеком».

3. **Звонок от специалиста портала «Госуслуги» с информацией о взломе страницы.**

На сегодняшний день, на портале «Госуслуги» есть возможность подать заявки для получения кредитов в различных банка. Данной возможностью пользуются злоумышленники. Они также, с использованием возможностей программ по замене абонентского номера осуществляют телефонные звонки гражданам, под предлогом того, что страница на портале якобы была взломана, получают пароли от личного кабинета и направляют заявки во все возможные банковские организации о от имени гражданина на получение кредита. Позже при получении кредита, под предлогом перевода денежных средств на безопасные счета, вынуждают граждан отправит все денежные средства.

Так 13.04.2022 неустановленные лица позвонили с абонентского номера +7499-719-42-11 гражданину «П», жителю и представившись специалистом портала «Госуслуг», в дальнейшем со страницы гражданина «П» была подана заявка на получение кредита на сумму 1 540 000 рублей в АО «АльфаБанк». Данные денежные средства потерпевший получил в банке и отправил их на счет злоумышленников.

При поступлении звонков от сотрудников портала «Госуслуг», независимо от того, в чем они пытаются вас убедить, разговор необходимо сразу прекратить, на входящие вызовы не отвечать. Помните, что сотрудник портала никогда не будет производить звонки на Ваш абонентский номер. В последствии нужно зайти в свой личный кабинет, убедиться, что все в порядке, в случае необходимости позвонить в службу поддержки по телефону указанному на странице и удостовериться еще раз. Использовать портал «Госуслуги» нужно только через приложение, не нужно заходить в него через Ваш стандартный браузер.

4. **Инвестирование денежных средств в различные «финансовые пирамиды» и инвестиционные фонды.**

В современном Интернет-пространстве систематически появляется реклама о том, что можно произвести инвестирование суммы денежных средств и в дальнейшем через короткий промежуток времени будет получена многократная прибыль, при этом для достоверности, злоумышленниками используются названия широко известных брендов, таких как «Газпроминвестиции», Тинькоффинвестиции» и т.д. Потерпевший проявляет свою заинтересованность, оставляет контактные данные и в дальнейшем с ним начинаю созваниваться якобы менеджеры и предлагать вложить свои денежные средства. При вложении определенной суммы денежных средств, потерпевшему указывается на то, что он уже якобы заработал крупную сумму и нужно вложить еще денег, чтобы была возможность вывода заработка. Так продолжается до тех пор, пока гражданин не перестает платить и понимает, что его обманывают.

24.05.2022 в отдел полиции обратилась гражданка «В» о том, что с февраля 2022 до мая 2022 она под предлогом высокоэффективных вложений денежных средств перевела 1 940 000 руб. В сети Интернет нашла сайт, занимающийся инвестициями, в последствии переводила денежные средства.

В случае если возникает необходимость в инвестировании денежных средств, то необходимо осуществлять данную деятельность либо в отделении банка, с оформлением соответствующего договора, либо скачав официальное приложение кредитно-финансовой организации. Не переходить по ссылка об инвестиционных фондах, размещенных в сети Интернет.

5. Покупка различных товаров через сайты, социальные сети в сети интернет:

Как правило злоумышленники размещают объявления на различных сайтах: Авито, Юла, Авто.ру, Дром.ру и других о продаже различных товаров по более выгодной цене. В беседе с потенциальным потерпевшим просят перевести задаток, так как у него много предложений и ждать он не будет, либо же в мессенджерах присылают ссылку, переходя по которой потерпевший вводит данные своей банковской карты и денежные средства списываются автоматически

07.05.2022г. в отдел полиции поступило заявление гражданина «Л». 06.05.2022 года потерпевший выставил объявление о продаже мужских полуботинок на сайте "Авито", выставил объявление о продаже за 6000 рублей. Через некоторое время ему поступило сообщение от пользователя "Alla" с предложением оформить доставку через курьера Яндекс, на что он скинул свой сотовый телефон и попросил её связаться мессенджере "Batcap", позже ему поступило сообщение в виде ссылки и сообщили, что данная ссылка оформляется, чтобы курьер приехал и забрал посылку. Гражданин «Л» зашел по указанной ссылке, ввел свои банковские данные, ему пришел код, который он ввёл и с его с банковского счета "Сбербанк" было списано 6000 рублей.

Чтобы не стать жертвой мошенников необходимо запомнить следующее:

- Никому не говорите коды из СМС от банка и трехзначный код расположенный на обороте карты.

- Никогда не переходите по ссылкам и QR-кодам от незнакомых людей.

- Оплачивайте товар заранее только в тех случаях, если оформляете сделку на самой торговой площадке. Не переводите деньги напрямую на карту или телефон незнакомого человека.

- Обсуждайте все детали сделки только в чате торговой площадки. Не переходите для общения в другие мессенджеры.

6. Выплаты компенсаций за ранее приобретенные медицинские препараты, либо участие в «финансовых пирамидах».

Злоумышленники, с использованием возможностей программ по замене абонентского номера, осуществляют телефонные звонки гражданам, от имени служащих торгово-производственных компаний, либо сотрудников прокуратуры. В ходе диалога указывается на то, что потерпевшему положена крупная финансовая компенсация, либо за ранее приобретенные недоброкачественные медицинские препараты, либо за давние вклады в «финансовые пирамиды», однако чтобы получить данные выплаты, нужно оплатить услуги страховки и так далее.

02.04.2022 у гражданки «С» похитили 23 000. Позвонили неизвестные представились сотрудниками фирмы по производству БАД, спросили довольна ли она продукцией, на что потерпевшая сказала, что их таблетки не помогают, после чего ей предложили компенсацию 450 000 рублей, однако нужно оплатить страховку в 30 000 рублей, что потерпевшая и сделала.

При поступлении таких звонков никакого дальнейшего общения проводить не нужно, ни одна компания не будет производить выплаты без соответствующего судебного решения. Не нужно переводить свои денежные средства неизвестным лицам.

7. Дистанционные услуги гадалок, целителей и т.д.

Данный способ по прежнему сохраняет свою актуальность. Граждане в сети Интернет, а также на телевидении находят объявления об услугах гадалок, целителей, предсказателей и т.д. В дальнейшем якобы за оказанные им услуги переводят крупные суммы денежных средств.

8. Звонок в торговую точку, либо собственника.

При данном способе злоумышленники производят звонки в торговые точки города, где в кассе есть наличность и представляясь директором организации, либо ее владельцем, просят срочно перевести денежные средства на расчетный счет, якобы в счет оплаты за товар или услугу.

Чтобы не стать жертвами мошенников в данных случаях, работникам торговой сферы, нужно всегда осуществлять звонок непосредственному руководителю, не выполнять не возложенные на них функции, не переводить денежные средства. Руководству данных торговых организаций при трудоустройстве работников, необходимо проговаривать данные вопросы заранее.

9. Вымогательство денежных средств в сети Интернет за нераспространение сведений интимного характера.

В последнее время, данный способ хищения денежных средств набирает популярность. Очень часто данные преступления совершаются в отношении молодых девушек и парней. В социальных сетях и различных мессенджерах происходят знакомства, ведутся переписки откровенного содержания, в том числе и с откровенными фотографиями, которые в дальнейшем становятся инструментом шантажа и вымогательства денежных средств, взамен за нераспространение данных фото в сети Интернет.

По итогам рассмотрения вышеуказанных способов можно выделить основные правила, которые необходимо соблюдать при использовании банковских карт и посещения сети Интернет.

1. Ни при каких обстоятельствах нельзя передавать посторонним лицам сведения о своих счетах и банковских картах, а также не совершать никаких действий со своими картами и вкладами, о которых просят незнакомые лица по телефону; тем более не

выполнять никаких действий в банкомате со своей банковской картой под диктовку неизвестного лица.

Сотрудники банков не звонят клиентам и не сообщают о блокировке карт, такие действия совершают только мошенники.

2. Не переходите по направляемым Вам ссылкам или QR-кодам для оплаты товаров или услуг.

3. Не предоставляйте доступ третьим лицам к своим персональным данным, компьютерам, телефонам, на которых имеется удаленный доступ к вашим денежным средствам.

4. Если в ходе телефонного разговора вам представляются сотрудниками силовых структур, просят действовать по указанию сотрудников банков и т.д., не выполняйте данные действия, это мошенники.

5. Если Вам звонят и сообщают, что положена компенсация за что-либо и просят предварительно провести оплаты – это мошенники.

6. Делая выбор и совершая покупку в сети интернет нужно внимательно изучать страницу продавца, помните о том, что товар Вам может быть не поставлен, либо поставлен ненадлежащего качества.

7. Инвестирование денежных средств необходимо осуществлять только через официальное представительство кредитно-финансовой организации или через официальное приложение.

При возникновении любых вопросов либо сомнений необходимо проконсультироваться непосредственно в отделении банка, позвонить на горячую линию кредитной организации, уточнить сведения по телефону доверия полиции, обратиться в ближайшую дежурную часть или даже к сотруднику полиции, которого вы увидели на улице.

Будьте бдительны! Не отдавайте свои деньги мошенникам!

Если Вы стали жертвой мошенников, то необходимо как можно скорее обратиться в отделение банка а также в ближайший орган внутренних дел!

МО МВД России «Петропавловский»