ИНФОРМАЦИОННОЕ ПИСЬМО

о способах хищений денежных средств граждан, проживающих на территории Николаевского муниципального района, о рекомендациях, направленных на недопущение совершения преступлений

Николаевской-на-Амуре городской прокуратурой совместно с ОМВД России по Николаевскому району в рамках работы по противодействию и профилактике отдельных видов преступлений проанализированы обстоятельства хищений денежных средств граждан, совершенных с использованием современных технологий, включая средства связи.

Так, 2020 год характеризовался ростом числа совершенных в отношении жителей района обозначенных преступлений на 79% (с 62 до 111).

Несмотря на предпринятые правоохранительными и иными органами меры по профилактике подобного рода преступлений, оперативная обстановка по этому вопросу остается крайне сложной.

Методы психологического воздействия, которыми пользуются мошенники, а также эмоциональное, легкомысленное и неосторожное поведение граждан в отношении безопасности собственных денежных средств позволяют мошенникам добиваться своих целей среди граждан. При этом как отмечается, ни возраст потерпевших, ни их уровень образования, какой-либо роли не играют, потерпевшим может быть любой.

При этом как показало изучение материалов конкретных уголовных дел, в большинстве случаев потерпевшие были осведомлены об основных способах мошенничества, тем не менее, это не уберегло их от совершения в отношении них преступлений.

Самыми распространенными в 2020 году и истекшем периоде 2021 года способами хищений денежных средств граждан явились:

1. Осуществление злоумышленниками телефонных звонков гражданам.

Как правило, злоумышленники представляются потерпевшим работниками банковской сферы, в большинстве случаев - службы безопасности банков. В ходе телефонных разговоров они сообщают потерпевшим о якобы подозрительных операциях, замеченных на их банковских счетах, попытках снятия денежных средств со счета потерпевшего, либо о произошедшем сбое в программе вследствие чего произошла блокировка счета, либо о зачислении бонусов на счет потерпевшего.

В ходе разговора злоумышленники пытаются войти в доверие к потерпевшим, оперируют специфическими терминами, характерными для работников банковской сферы, ведут себя спокойно, разговаривают вежливо, в некоторых случаях оперируют реальными данными о банковских счетах потерпевших.

Далее в ходе разговора злоумышленники для устранения якобы имеющейся опасности, в том числе незаконного снятия денежных средств со счета потерпевшего, просят последнего сообщить конфиденциальную информацию (номер банковской карты, CVC или CVV код - цифровой трехзначный код, расположенный на обратной стороне карты, которым подтверждается подлинность карты).

В некоторых случаях злоумышленники просят сообщить им пароль, который отражен в СМС-сообщении, которое поступило потерпевшему по телефону.

Имеют тенденцию роста случаи, когда потерпевшие «под диктовку» злоумышленников сами совершают действия, направленные на перевод денежных средств.

Все чаще такого рода преступления совершаются с помощью программных средств, осуществляющих подмену номера телефонов, т.е. при звонке потерпевшему в его телефоне может отражаться номер телефона, который реально принадлежит банку или иной организации.

Например, 03.03.2021 жительнице нашего района (1968 г.р., работник сферы образования) с незнакомого ей номера телефона позвонил злоумышленник, который представился ей сотрудником службы безопасности банка и сообщил, что им пришло сообщение о том, что она желает закрыть свой вклад. Также он добавил, что это действуют мошенники и ее денежные средства необходимо перевести на другой счет.

Сначала потерпевшая поняла, что это действуют преступники и прекратила с ними разговор.

Однако ей снова позвонили и представились сотрудниками банка и сообщили, что ее личный кабинет взломан, и ее денежные средства могут похитить. Также предупредили, что ей дополнительно позвонят с банка и ей необходимо будет подтвердить списание денежных средств. Далее ей позвонили с номера телефона «900», в ходе разговора на вопрос о подтверждении списания она ответила утвердительно и сообщила CVV код (трехзначный код на оборотной стороне банковской карты).

В этот день у потерпевшей было похищено около 500 000 рублей.

Правоохранительными органами также наблюдается тенденция к увеличению числа преступлений, когда преступники, используя подмену номеров телефона, представляются сотрудниками правоохранительных органов (полиция, прокуратура, следственный комитет).

Например, 09.03.2021 жителю нашего района (1997 г.р., работник в сфере связи) с незнакомого номера телефона позвонила женщина, которая представилась работником банка, и сообщила, что неизвестные лица пытаются с его банковского счета похитить 8000 рублей и отправили заявку на получение кредита. Далее потерпевшего соединили с якобы работником службы безопасности банка, который сообщил потерпевшему, что это не первый случай и ему позвонят с полиции.

Далее потерпевшему поступил звонок с неизвестного номера телефона, злоумышленник представился сотрудником полиции, который попросил потерпевшего оказать ему содействие, а также добавил, что уже возбуждено уголовное дело и попросил не разглашать их разговор. Для того чтобы потерпевший поверил ему, злоумышленник попросил его проверить номер телефона, с которого он звонит. Потерпевший проверил указанный номер телефона, с которого звонил злоумышленник, телефон принадлежал одному из управлений МВД по субъекту Российской Федерации.

Закончив разговор с лицом, представившимся полицейским, потерпевший продолжил разговор с якобы работником банка.

Злоумышленник попросил потерпевшего снять имеющиеся денежные средства с банковского счета и в целях их сохранения осуществить переводы на номера телефонов, которые якобы являлись номерами банковских ячеек.

Потерпевший выполнил просьбы злоумышленников, направив денежные средства на предоставленные ему номера.

В тот день у потерпевшего было похищено 110 000 рублей.

При сравнительно схожих обстоятельствах в феврале и марте 2021 года были похищены денежные средства у работника здравоохранения (1956 г.р.) и работника аптечной сети (1990 г.р.).

2. Осуществление злоумышленниками переписки в социальных сетях от имени родственников, друзей и близких людей потерпевших.

Как правило, такие преступления происходят по одному и тому же сценарию. Злоумышленниками осуществляется взлом аккаунта гражданина, созданного в социальных сетях (Одноклассники, Инстаграмм, Вконтакте). Далее злоумышленники ведут переписку с имеющимися контактами, представляясь их родственниками, друзьями и знакомыми.

Суть всех сообщений сводится либо к просьбам об оказании финансовой помощи, например, для лечения от болезни, либо предложению о получении какой-либо выгоды, например, доплат к пенсии, разовых выплат и т.д. В ходе переписки злоумышленники также как и в первом случае просят предоставить номера банковских карт, кодов и другие личные данные.

Например, в феврале 2021 года жительнице нашего района (1940 г.р., пенсионер) на ее страницу в социальной сети «Одноклассники» от якобы двоюродной сестры пришло сообщение, суть которого заключалось в том, что один из известных банков проводит акцию и дает пенсионерам по 4000 рублей, которые, якобы уже получила ее сестра.

В этих целях злоумышленник, представляющийся потерпевшей ее сестрой, попросил направить номер банковской карты, CVV код (трехзначный код на оборотной стороне банковской карты), а также пароль, который пришел в СМС-сообщении со службы «900».

После этого с банковского счета были похищены денежные средства. В дальнейшем в ходе разговора со своей сестрой потерпевшая поняла, что это действовали преступники.

3. Хищение денежных средств при совершении покупок в сети Интернет.

Как правило, такие преступления совершаются при покупке товаров и услуг через сеть интернет, социальные сети («Одноклассники», «Инстаграм»), мобильные приложения «WhatsApp». После перевода предоплаты или оплаты полной суммы за товар или услугу, связь с мошенником прекращается, аккаунт потерпевшего блокируется.

Нередко, в целях привлечения внимания потерпевших злоумышленниками продается товар по очень привлекательной цене, которая существенно ниже чем в других магазинах.

Например, жительница района, находясь в декретном отпуске по уходу за ребенком, решила приобрести телефон известного бренда через сеть Интернет.

На популярном сайте купли-продажи различного имущества потерпевшая нашла объявление о продаже телефона по доступной цене, после чего решила его приобрести. Продавец в ходе переписки с покупательницей вошел в доверие к последней, предоставил ложные копии паспортных данных. Денежные средства в размере 20 000 рублей покупательница перевела через обезличенный интернет-кошелек. После перевода денежных средств «продавец» на связь не выходила, телефон покупательница так и не получила.

При этом цена такого телефона в магазине составляла порядка 70 000 рублей.

4. Хищение денежных средств путем обмана, совершаемое путём настойчивого навязывания товаров и услуг.

Такие преступления совершаются путем навязывания товаров и услуг как в ходе телефонных разговоров, так и с помощью рекламы в интернете и телевидении. Предлагаемые злоумышленниками товары и услуги ими позиционируются как способ повышения благосостояния, улучшения здоровья (оформление кредита по выгодной ставке, предложение вложить деньги в инвестиции для того чтобы приумножить имеющиеся средства).

Часто злоумышленники предлагают чудодейственные медицинские препараты, витамины, другие товары, которые якобы помогут излечиться от всех болезней. Нередко хищение денежных средств граждан происходит в ходе общения с экстрасенсами, гадалками, магами и колдунами.

5. Хищение денежных средств при совершении покупок на фондовой бирже ценных бумаг:

Сегодня в период бурного развития Российского фондового рынка практически каждый, имеет право и возможности приобрести ценные бумаги. Для этого потребуется регистрация в брокерской компании и, через своего личного брокера, осуществлять любые операции на фондовой бирже ценных бумаг. Но экономическими знаниями обладают единицы. Операции на бирже сейчас осуществимы многими путями, порой не требующими даже личного контакта покупателя-продавца, это дает большой размах любителям экономических мошенничеств.

Мошенники, используют для осуществления своих черных замыслов, фальшивые ценные бумаги. Жертвами таких мошенников являются не слишком развитые в экономической области люди, но желающие приобрести все и сразу – то есть выгодные акции с преимуществом роста, по умеренной цене.

Мошенники могут незаконно завладеть ценными бумагами. Преступник может заключить сделку, расплатой за которую назначит ценные бумаги. Получив расчет, они не поспешат выполнить свои обязательства, а просто исчезнут. Если ценные бумаги недокументированные, то мошенник может предоставить регистратору фальшивую бумагу о праве собственности. Он может, посредством использования фальшивых бумаг об оплате сделки, приобрести их прямо у эмитента. Они обманным путем реализуют ценные бумаги, им не принадлежащие. Они могут так же выпускать необеспеченные ничем бумаги и сбывать их под видом ценных, в этом случае так же широко распространено мошенничество с использованием сети Интернет.

В ходе анализа обращений граждан установлено, что неустановленные лица, действовавшие от имени Компании, используя средства мобильной связи, предлагали гражданам дополнительный заработок, путем торговли на финансовом рынке. После регистрации граждан на сайте неустановленные лица вводят в заблуждение, обещая получение больших доходов на торгах. Граждане перечисляют денежные средства на указанные неустановленными лицами наличные счета, открытые в кредитных организациях. После попытки вывода денежных средств, перечисленных физическими лицами на торговые счета, представители компании не выходили на связь. Впоследствии связь с инвесторами прекращалась, и они теряли возможность вернуть денежные средства.

Например, жителю района с незнакомого номера телефона позвонила женщина, которая представилась менеджером инвестиционной компании «FinOperate» и предложила заработать на инвестировании в их брокерскую фирму. Для этого необходимо установить на персональный компьютер программу «Any Desk» для дальнейшей установки программы «Meta Trader 5», посредством которой можно совершать сделки на торговой площадке. После регистрации на сайте «FinOperate» злоумышленница начала давать потерпевшему общую информацию, как покупать акции, как происходит конвертация валюты и куда будут поступать его деньги.

Далее злоумышленница предложила потерпевшему осуществить оплату в размере 50000 рублей, для открытия брокерского счета на сайте брокерской компании, и продиктовала реквизиты, на которые необходимо отправить денежные средства, в результате потерпевший перевел указанную сумму. В дальнейшем на электронную почту потерпевшего пришло письмо, в котором говорилось, что на его имя успешно открыт счет. Зайдя на сайт «FinOperate» в сети Интернет потерпевший увидел счет, на котором было 699,64 евро.

На следующий день потерпевшему поступил звонок с неизвестного номера телефона, злоумышленник представился брокером брокерской компании «FinOperate» и сообщил ему, что будет работать с потерпевшим.

В дальнейшем все действия потерпевший совершал совместно со злоумышленником, который предлагал, какие позиции инвестировать, инвестировать в более крупные позиции, а именно, купить крипто валюту «биткоин», как и где можно приобрести выгодную валюту, как получить с нее прибыль, как производить вывод денежных средств и т.д.

В результате мошеннических действий потерпевший перевел на счет злоумышленников более 900 тысяч рублей.

РЕКОМЕНДАЦИИ ГРАЖДАНАМ:

- в случае поступления звонка с банка прекратить разговор, повесить трубку, самим перезвонить в банк по официальным номерам телефонов;
- ни при каких обстоятельствах, вне зависимости от того, кто и что будут говорить в ходе телефонного разговора, не сообщать номер банковской карты, цифровой трехзначный код, расположенный на обратной стороне карты, пароль (код), который поступает по СМС-сообщению;
- никогда и ни при каких обстоятельствах не сообщайте кому-либо пин-код от своей банковской карты, не храните сведения о пин-коде рядом с банковской картой, не пишите пин-код на оборотной стороне банковской карты;
- в случае утраты банковской карты, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов мобильного телефона;
- в торговых точках, ресторанах и кафе все действия с банковской картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты карты при помощи специальных устройств и использовать их в дальнейшем для хищения денежных средств;
- при поступлении сообщений в социальных сетях от родственников, друзей и других близких людей, в которых они предлагают какую-либо выгоду, или просят о финансовой помощи, необходимо самим перезвонить им и удостовериться в реальности сообщенных сведений;
- доверяйте только проверенным сайтам или производите оплату только при получении товара;

- если Вы получили звонок от якобы близкого родственника или знакомого с информацией о том, что он попал в неприятную ситуацию, в результате которой в отношении него будет возбуждено уголовное дело, или он будет арестован и, для решения «вопроса» нужно передать сотруднику правоохранительных органов определённую денежную сумму, следует удостоверится в том, что говорящий, действительно является тем, за кого себя выдаёт для чего задать уточняющие вопросы: «А как я выгляжу?» или «Когда и где мы виделись последний раз?», т.е. задавать вопросы, ответы на которые знаете только вы оба.

Если Вы разговариваете якобы с представителем правоохранительных органов, спросите, из какого он отделения полиции. После звонка следует набрать «02», «102» (для сот. телефонов), 8 (4212) 387-387 (телефон доверия УМВД России по Хабаровскому краю), узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда.

Необходимо помнить, что Ваша личная и финансовая безопасность в первую очередь зависит от Вас самих, а не от других лиц.

Николаевская-на-Амуре городская прокуратура

ОМВД России по Николаевскому району

от 19.03.2021 № 1-04-2021

Копия для направления и распространения,
оригиналы в прокуратуре и ОМВД