Виды наиболее распространенных способов совершения мошеннических действий в отношении жителей города и района и дополнительные меры профилактического противодействия.

- Звонок сотрудника банка, ЦБ РФ., МВД РФ, ФСБ РФ, СК РФ, и т.д. Преступники представляются сотрудниками банков, правоохранительных органов, Центрального Банка России, предлагают защитить средства от несанкционированного списания под различными предлогами, либо аннулировать заявку на кредит якобы оформленный на потерпевшего мошенниками, или получения денежной компенсации, выясняют конфиденциальные сведения банковских карт потерпевших, одноразовые пароли, понуждают жертву для противодействия мошенникам оформить кредиты в банках и САМОСТОЯТЕЛЬНО перевести денежные средства на предоставленные счета, после чего выводят деньги на подконтрольные счета;

Способы противодействия: Если Вам позвонили с банка и сказали, что Ваши финансы в опасности, не стесняйтесь, прекратите разговор, положите трубку и перезвоните на номер горячей линии банка, который указан на обратной стороне банковской карты. Ни при каких случаях не сообщайте звонящему личные сведения о себе и тем более сведения о Вашей банковской карте!

- Покупка билетов (бронирование поездки) в месенджере «BlaBlaCar» злоумышленники, используя заинтересованность и доверчивость жителей города под предлогом бронирования поездки и оплаты в качестве подтверждения направляют на ия заявителя (ссылку двойник) для оплаты поездки, в которой гражданами вводятся все сведения о банковской карте и сообщаются СМС-коды, в результате чего злоумышленники получают доступ к интернет кабинету банка и производят хищение денежных средств.

Способы противодействия: не производить оплату поездки до момента посадки в автомобиль к попутчику (пользоваться общественным транспортом)

- размещение объявлений на сайтах, специализирующихся по размещению информации о продаже различного рода имущества, продажа автомобиля, найма жилого помещения, трудоустройства (Авито.ру», «Домофонд», «Дром.ру» и др.), схема мошенничества такова: на интернет-сайтах бесплатных объявлений мошенники размещают информацию о продаже движимого и недвижимого имущества (в том числе предоставление услуг). Покупатель, заинтересовавшись предложением, звонит «продавцу» и просит о встрече. Ссылаясь на занятость или отсутствие в городе, «продавец» откладывает встречу с покупателем, при этом предлагает внести предоплату, т.к. товар может достаться более «расторопному» покупателю, в других случаях под предлогом оплаты за товар, в случаях, когда потерпевший самостоятельно выставляет товар на продажу через вышеуказанные сайты бесплатных объявлений, злоумышленник получает доступ к банковским картам потерпевшего, информацию о которых сообщает в следствии своей доверчивости сам потерпевший, и по средствам услуги «Мобильный Банк» злоумышленник совершает хищения денежных средств со счетов банковских карт потерпевшего.

Способы противодействия: проверять порядочность продавца на сайте бесплатных объявлений; обращать внимание на реальную стоимость товара, который приобретается, за частую стоимость товара мошенниками занижена, что делает товар более привлекательным; не сообщать своих данных и данные своих банковских карт не под каким предлогом; следовать инструкциям «Как не стать жертвой мошенничеств», которая размещена на самих сайтах бесплатных объявлений.

- использование преступниками вирусного программного обеспечения в результате, которого с банковских карт потерпевших происходит списание денежных

средств, а именно поступает потерпевшим СМС-сообщения, при прочтении вирусом проникает в программное обеспечение в связи, с чем происходит доступ злоумышленника к «Мобильному Банку» потерпевшего.

Способы противодействия: использовать антивирусные программы, установленные на мобильные устройства; скачивать приложения «Мобильный Банк» с официальных интернет страниц банков; не открывать и не проходить по ссылке, полученных в подозрительных СМС-сообщения, которые рассылаются под предлогом «Посмотри своё фото» и т.п.

- **приобретение различных товаров** на непроверенных интернет ресурсах (интернет магазины, социальные сети и др.).

Способы противодействия: приобретать товары только в проверенных интернет-магазинах; перед покупкой изучите отзывы о интернет-магазине, услугами которого хотите воспользоваться; опасайтесь сайтов «двойников» официальных сайтов, когда в названии могут быть отличия; обращать внимание на реальную стоимость товара, который приобретается, за частую стоимость товара мошенниками занижена, что делает товар более привлекательным.

- **использования преступниками схемы** в отношении лиц приобретавших в 2007-2010 годах биологически активные добавки (БАДы), а именно предлог возмещение по решению суда страховки лицам, ранее приобретавшим, вышеуказанные товары положена компенсация, в связи, с чем граждане, доверившись данному предлогу, отправляют денежные средства по системе денежных переводов «Колибри» «Золотая Корона».

Способы противодействия: сам факт выплат компенсации или страхов вымышлен, и используется как предлог, рассчитанный на доверчивость потерпевших, проявляйте бдительность.

- **рассылка СМС-сообщений о блокировании (осуществление оплаты)** банковских карт находящихся в пользовании потерпевших и доверчивость самих потерпевших, которые передают информацию о своих банковских картах преступникам, которые в последующем используют данные номера для вывода денежных средств, посредством использования различных платежных систем в сети интернет.

Способы противодействия: при поступлении указанных СМС-сообщений обращайтесь на телефоны горячих линий, которые указаны на оборотной стороне банковских карт, не звоните по номерам указанных в СМС-сообщениях, даже если номер телефона схож с номером, который используется банком как горячая линия для клиентов (отличия могут быть в одной-двух цифрах).

- **звонки от лиц, которые представляются сотрудниками правоохранительных органов** и сообщают о том, что близкий родственник стал фигурантом уголовного дела связанного с избиением человека, которое повлекло к причинению тяжкого вреда здоровья или виновником ДТП, в результате, которого пострадал человек, и в ходе телефонного разговора злоумышленник предлагает решить вопрос путем дачи денежных средств потерпевшему, который в последующим откажется от своего заявления.

Способы противодействия: в первую очередь позвоните родственнику, о котором будет идти речь в ходе телефонного разговора со злоумышленником, в случае если не удалось дозвонится до него сообщите о данном факте в полицию, злоумышленники в данном случае пользуются правовой неграмотностью лиц преклонного возраста, или эмоциональным состоянием лиц, которым стало известно о вымышленной трагедии, которая случилась с их родственником, всегда сохраняйте спокойствие и не подавайтесь на уговоры, угрозы злоумышленников, даже если с вами пытается говорить по телефону «лжеродственник».

- **оформление онлайн займов/кредитов на непроверенных сайтах в сети интернет,** злоумышленники, используя заинтересованность и доверчивость жителей

города под предлогом оформления кредит на необходимую сумму, и под предлогом оплаты страховки, а далее курьерской доставки документов совершают хищения денежных средств.

Способы противодействия: для получения займов/кредитов обращаться в офисы банков, либо использовать проверенные сайты, которые специализируются на онлайн-займах.

- **участие в розыгрышах ценных призов** (автомобили, сотовые телефоны и др. электронная техника), информация о которых распространяется в социальных сетях («ВКонтакте», «Одноклассники.ру», «Инстаграмм» т.п.), на различных интернет сайтах, в виде СМС-рассылки и за участие, в котором необходимо осуществить оплату определенной суммы за страховку, пересылку, либо оплата курьерской доставки выигранного приза.

- **звонки от «лжеродственников», знакомых, друзей с просьбой перевести денежные средства для избежание административной ответственности за нарушение ПДД, а именно: лишения права управления сотрудниками ГИБДД**, которые в ходе остановки и проверки документов выявили факт нахождения в алкогольном опьянении.

Способы противодействия: в первую очередь позвоните родственнику, о котором будет идти речь в ходе телефонного разговора со злоумышленником, в случае если не удалось дозвонится до него сообщите о данном факте в полицию.

- **рассылка сообщений со страниц (взломанных, «скопированных») в социальных сетях «ВКонтакте», «Одноклассники.ру», «Инстаграмм» т.п.** от имени друзей, родственников с просьбой занять денежные средства в долг на непродолжительное время.

Способы противодействия: в первую очередь свяжитесь с родственником, другом и т.п. от имени которого обращаются с просьбой занять денежные средства.

Данные перечень мошенничеств, совершаемый с использованием средств мобильной связи далеко не исчерпывающий, с каждым днем злоумышленники разрабатывают все новые и новые преступные схемы обмана граждан.

Кроме того, развитие дистанционных платежных сервисов, основным инструментом которых являются банковские карты, имеет ключевое значение для решения задач формирования инновационной модели развития безналичных расчетов, обеспечения доступности платежных услуг для населения в отдаленных и труднодоступных местностях, снижения издержек хозяйствующих субъектов и государства.

Расширение сферы безналичных расчетов привело к интенсивному развитию киберпреступности и повлекло за собой возникновение своеобразной криминальной индустрии, необходимой для совершения хищений денежных средств, в том числе с использованием банковских карт.

Технологии, используемые злоумышленниками для совершения хищений, постоянно совершенствуются и становятся доступными широкому кругу лиц, которые могут не обладать глубокими знаниями в области информационных технологий. Повышение доступности мошеннических схем и инструментов для их реализации ожидаемо влечет за собой рост числа несанкционированных переводов денежных средств с лицевых счетов банковских карт граждан.

- **фишинговые интернет сайты** мошенники создают в сети Интернет поддельную (фишинговую) веб-страницу, внешне не отличимую от официального сайта коммерческой организации, на которую перенаправляют ее клиента. Ничего не подозревающий клиент вводит свои персональные данные, тем самым предоставляя мошенникам часть информации, необходимой для входа в его личный кабинет. После этого мошенники просят ввести разовый код подтверждения, который выслал банк, а затем перечисляют денежные средства на свои счета. Нередко потерпевшему поступает

звонок с номера, очень похожего на банковский, и мошенник, представившийся сотрудником банка, сообщает информацию о сбое в системе и ошибочных сообщениях, уверяя, что всё в порядке, а при необходимости подтверждения каждой операции по переводу денежных средств разовыми паролями, приходящими на телефон от реального банка, просит вводить их в поле, запрашиваемое страницей. После этого клиенту может прийти SMS-сообщение якобы от банка об отмене ошибочных операций, но только с целью того, чтобы отсрочить момент обнаружения хищения. В ряде случаев мошенники создают абсолютную копию сервера авторизации, на котором клиент вводит данные своей карты при оплате покупки. Вместо подлинного сайта потерпевший попадает на фишинговый и после ввода им реквизитов банковской карты доступ к ней получают преступники.