Информационная справка

За 7 месяцев 2025 года количество пострадавших на территории Пушкинского района от действий мошенников составило не менее 400 граждан.

Согласно проведенным экспертизам установлено, что злоумышленники, представляясь сотрудниками правоохранительных органов, Центрального банка России, оказывают на потерпевших массированное психологическое воздействие, удерживают их в состоянии постоянного напряжения и страха, манипулируют и запугивают их. Используемые злоумышленниками программы и сервисы администрируются из-за рубежа, в связи с чем организаторы зачастую недоступны для правоохранительных органов России, а поручения об оказании международно-правовой помощи в западные страны остаются без ответа. Вместе с тем, нами устанавливаются исполнители, действующие на территории г. Санкт-Петербурга и России, однако, их привлечение к уголовной ответственности является недостаточным для прекращения преступлений данной категории.

Самыми распространенными способами совершения преступлений являются:

- **осуществление телефонного звонка от имени любого должностного лица правоохранительных органов** (МВД, ФСБ, прокуратуры), Центрального банка России, службы безопасности конкретного банка. В ходе разговора мошенники, зная ФИО потерпевшего и наличие у него банковского счета в конкретном банке, то есть обладая персональными данными потерпевшего, сообщают ему о попытке хищения денежных средств с его счета, чем вводят его в тревогу относительно утраты нажитого имущества. При этом, оказывая психологическое воздействие, сообщают единственный выход из сложившейся ситуации - перевести деньги на «безопасный государственный счет» на период установления и задержания виновного лица, после чего убеждают потерпевшего снять деньги со своего счета и зачислить их в банкомате на продиктованный счет. В подтверждение своих слов о причастности к государственным органам, преступники демонстрируют потерпевшему с помощью различных мессенджеров документы государственных органов или служебные удостоверения, которые в действительности являются фиктивными. Аналогичным способом преступники убеждают потерпевших оформить на свое имя кредит, денежные средства перевести на «безопасный счет», после чего они похищаются.
- **представляясь сотрудниками МВД, либо ФСБ**, преступники обманывают граждан, сообщая им о наличии угрозы потери квартиры, убеждают их в том, что они участвуют в мероприятиях по поимке

мошенников путем продажи квартиры и временного помещения вырученных от продажи денег на «безопасный счет», которые на самом деле похищаются.

- **хищение денег граждан путем совершения звонка от имени близкого родственника или знакомого**, якобы попавшего в беду (совершившего дорожно-транспортное происшествие или иное преступление), с требованием передачи денежных средств для избежания уголовной ответственности, которые в последующем преступники похищают через подставных лиц (таксистов, курьеров), как правило не осведомленных о совершаемом преступлении.
- «**удаленная работа, дополнительный быстрый заработок**». Потерпевший, желая получить «легкие деньги» вступает в групповые чаты, в которых предлагается, например, осуществлять бронирование номеров в гостиницах и предоставлять скриншоты об оплате, осуществлять покупку/продажу товаров, «раскручивать» аккаунты социальных сетей, для данных целей мошенники предоставляют жертвам банковские реквизиты для перевода либо ссылки на фишинговые сайты, при этом создавая активность таких чатов с помощью ботов и видимость, что другие участники тоже совершают покупки и получают прибыль. При этом поначалу потерпевшие получают якобы «прибыль», тем самым мошенники усыпляют бдительность и убеждают потерпевших вкладывать и выбирать задания более высокого уровня на крупную сумму, но когда суммы покупок/оплаты достигают значительных размеров, то мошенники, завладев денежными средствами жертв, удаляют чаты и переписки, меняют абонентские номера.
- **«запись на диспансеризацию, установка приложения для записи к врачам, программы-вирусы»**. Мошенники обзванивают потерпевших, представляются сотрудниками медицинских учреждений, приглашают пройти диспансеризацию, на которую возможно записаться по телефону, необходимо лишь для подтверждения записи к врачам сообщить код из смс, с помощью которого получают доступ к Госуслугам, где мошенники получают массу персональной информации, которую в последующем могут использовать в других мошеннических схемах. В случае программ – вирусов потерпевшие теряют доступ к своему устройству и под угрозой оказываются все приложения с персональными и платежными данными, в том числе банковскими.
- **«Инвестиции»**. Существуют многочисленные способы вовлечения потерпевших в инвестирование: знакомство в социальных сетях, где поначалу идет отстраненная переписка мошенника с жертвой на общие темы, постепенно с переходом о вопросе дополнительного заработка и во влечении в «инвестирование»; различные рекламы и объявления в

сети Интернет о вложении в криптовалюту и гарантии невероятной прибыли от инвестиций. Далее мошенники в ходе общения в мессенджерах, в ряде случаев в действительности рассказывают основные принципы торговли, для того чтобы притупить бдительность жертвы. Человек, мечтая получить огромные доходы, начинает перечислять денежные средства на мифический инвестиционный фонд, зачастую жертвы даже не обращают внимания, что перечисляет денежные средства на банковские счета физических лиц – дропов. В последующем потерпевший не получает никакой прибыли, при этом ему сообщают о заблокированном счете и для того, чтобы вывести денежные средства необходимо разблокировать счет, путем перечисления денежных средств на определенный процент от «полученной прибыли», ради чего потерпевшие даже оформляют кредиты, перечисляя снова и снова денежные средства мошенникам.

- **взлом аккаунтов профиля социальных сетей мессенджеров** (ВКонтакте, WhatsApp, Telegram), так при получения доступа к персональным данным жертвы, мошенники рассылают сообщения неопределенному кругу лиц от имени потерпевшего в указанных сервисах, с просьбой «срочно одолжить денежные средства» путем их перевода на номера банковских карт указанные мошенниками, либо с предоставлением фотографии банковской карты, на которой указаны данные потерпевшего, однако номер банковской карты полностью подконтролен мошеннику.
- **«Вами выдана доверенность на Госуслугах на оформление кредитов, продажу квартиры, распоряжение счетами, срочно берите встречные кредиты для аннулирования кредитов, продавайте имущество и перечисляйте все денежные средства на «безопасный счет»»**. При данной схеме мошенники для убедительности предоставляют на электронную почту поддельные доверенности, в которых указано, что потерпевший якобы в действительности доверил некому гражданину оформление кредитов/продажу квартиры/машины, также присылают копии документов с логотипами Банка России, гербовые печати, документы сотрудников Банка и иных должностных лиц, при этом разговор жертвы и мошенника может длиться достаточно продолжительное время, а в некоторых случаях и до нескольких дней. Мошенники убеждают жертву оформить кредиты, снять все свои сбережения, закрыть вклады в банках и осуществить переводы денежных средств на «безопасные счета», уверяя, что после поимки преступника денежные средства/имущество в полном объеме вернутся потерпевшему. Мошенники убеждают потерпевшего не сообщать ничего родственникам, заказывают жертвам такси для перемещения от дома до банков, при этом указывая в какой именно банк обратиться за

кредитом либо осуществить снятие денежных средств в крупной сумме, указывают в каком именно банкомате осуществить внесения денежных средств на «безопасный счет». Некоторые потерпевшие, будучи под влиянием обмана, по указаниям мошенников перемещаются в другие города в тайне от родственников, не контактируя с родственниками некоторое время, отдают мошенникам все свои сбережения, вплоть до срочной продажи квартир и иной недвижимости с последующим перечислением вырученных денежных средств от сделки мошенникам.

- **«Фишинговые сайты, письма, сообщения»**. Фишинг — вид интернет-мошенничества, цель которого получить доступ к данным пользователя: логинам и паролям, номерам карт, банковским счетам. Преступники присылают фишинговые письма, которые могут быть очень похожи на настоящие сообщения от банков, компаний, органов власти или Госуслуг. Но ссылка в таком письме ведёт на поддельный сайт. Став жертвой фишинга, можно лишиться денег или доступа к своим учётным записям, пустить хакера в корпоративную сеть работодателя. Фишинговыми бывают не только письма, приходящие на электронную почту. Это могут быть сообщения в мессенджерах, социальных сетях и смс. Злоумышленники имитируют письма от администрации социальных сетей, интернет-магазинов. При переходе по ссылке вы окажетесь на сайте, который оформлен как настоящий интернет-сервис и при оплате например приобретаемого товара денежные средства зачисляются на счета мошенников.
- **«пролонгация абонентского договора с оператором сотовой связи/взлом Госуслуг»**. Схема заключается в том, что гражданину звонит якобы представитель сотового оператора, у которого обслуживается номер телефона гражданина. Мошенники говорят, что номер старый, обслуживается, например, больше десяти лет, и его необходимо "пролонгировать". Иначе номер будет передан новому абоненту и уверяют что возможно сделать это по телефону, без траты времени на посещения салона связи. В том числе Пролонгировать абонентский номер предлагается через сайт «Госуслуги». И всего лишь нужно продиктовать код из пришедшего сообщения, продиктовав код у мошенников появляется доступ к личному кабинету Госуслуг жертвы. И далее различные негативные последствия, самые нежелательные из которых - микрозаймы и кредиты на имя гражданина.
- **«продление Полиса ОСАГО»**. Мошенники рассылают письма на электронные почты, смс сообщения о заканчивающемся сроки полиса ОСАГО с ссылками на сайты для продления действия полиса. Как правило у жертвы в действительности подходит срок действия полиса. Так, потерпевший переходит на сайт якобы страховой компании – фишинговый сайт, где после заполнения некоторых полей, в том числе

реквизитов банковской карты, подтвердив операцию по оплате, деньги списываются, а на электронную почту приходит файл с полисом похожего на действительный, однако при его проверке в базе РСА такого полиса найдено не будет.

- **«покупка/продажа товаров на торговых площадках».** Мошенничество с помощью торговых площадок, на примере самой распространенной - Авито. Имеется несколько популярных видов мошенничеств:
  1) Вы — покупатель и нашли объявление о продаже товара, которое Вас заинтересовало. На ваше предложение купить товар продавец отвечает, что к нему уже выстраивается очередь из покупателей — и если вы точно хотите получить вещь, то должны отправить ему на карту предоплату. После продавец предоставляет реквизиты для перевода и завладев денежными средствами скрывается.
  2) Вы — продавец. «Покупатель - мошенник» готов купить ваш товар, не глядя, и хочет отправить вам на карту задаток или даже полностью оплатить вещь. Он просит номер карты, а затем требует назвать цифры из СМС, которое пришло вам из банка — якобы это нужно для банковского перевода.
  3) покупатель - мошенник спрашивает у вас номер карты, чтобы отправить вам деньги за товар при личной встрече, однако деньги на счет не поступают, в подтверждении своих добросовестных намерений покупатель - мошенник демонстрирует подложные квитанции о переводе, списание с его счета денег, сообщает свои данные паспорта и ФИО, но в большинстве случаев все эти данные фальсифицированы, также ссылаются на сбой работы банка и убеждают что денежные средства поступят возможно позже, так мошенник завладевает имуществом, не имея намерений производить оплату.
  4) Вы - покупатель. Продавец предлагает вам общаться не в собственном мессенджере «Авито», а в другом — например, в WhatsApp. Он находится в другом городе и готов отправить вам товар, но вместо сервиса «Авито Доставка» хочет воспользоваться сторонней курьерской службой доставки — Boxberry, «СДЭК» и другими. Продавец спрашивает ваши личные данные: ФИО, адрес и номер телефона - для отправки товара, но только в случае оплаты всей стоимости товара путем перевода на банковские реквизиты указанные мошенником. Затем злоумышленник предоставляет поддельную квитанцию и трек номер отправления транспортной компании, таким образом получив денежные средства путем обмана, не намереваясь отправлять товар. Также бывают случаи, когда присылают ссылку на курьерскую службу, и вы оплачиваете картой товар. Через некоторое время вам сообщат, что произошла

ошибка или внештатная ситуация, и вы не сможете получить свой товар. Вам предложат возврат средств — для этого снова придётся ввести данные карты на сайте курьерской службы. Под предлогом возврата средств мошенники ещё раз спишут деньги с вашей карты. Сайт и служба поддержки «курьерской компании» — поддельные. Ещё один вариант развития событий, это когда «Продавец» якобы готов отправить вам товар с помощью сервиса «Авито Доставка» и для удобства общения он предлагает вам перейти в сторонний мессенджер — WhatsApp или Telegram — и в нём присылает ссылку на форму «Авито Доставка», чтобы вы оплатили товар картой. И идентичная схема когда Вы — продавец, «Покупатель» готов купить у вас товар с помощью «Авито Доставки». В мессенджере «Авито» он спрашивает ваш адрес электронной почты — туда вам приходит письмо из сервиса «Авито Доставка». В письме содержится форма, где нужно указать данные вашей карты для получения денег от покупателя, однако сайт фишинговый и денежные средства похищает мошенник.

Типичные фразы мошенников:

- «Продиктуйте пароль из СМС»;
- «На вашу карту пришел крупный денежный перевод»;
- «Назовите данные банковской карты»;
- «На вашей карте замечена подозрительная активность»;
- «Ваша сим-карта была заблокирована»;
- «Это служба безопасности банка. С вашего счета списали деньги»;
- «Это сотрудник полиции. Переведите свои деньги на безопасный счет».

С целью избежания хищения денежных средств необходимо соблюдать ряд правил, а именно:

- Не разглашать персональные данные в ходе телефонного разговора;
- Не осуществлять предоплату по объявлениям с сайтов;
- Не сообщать любые данные банковских карт или код из СМС;
- Не переводить денежные средства незнакомым людям.

Рекомендуется:

- Не переходить по сторонним ссылкам, поступившим на мобильный телефон с помощью СМС сообщений или в мессенджерах;
- Быть внимательными. Не терять самообладание во время телефонного разговора;
- Прервать телефонный разговор с мошенниками;
- Связаться с родственниками, сообщить им о поступившем звонке, посоветоваться с ними;
- Заблокировать подозрительного абонента.