## Привлечение к вымышленному расследованию

Мошенники представляются сотрудниками правоохранительных органов (полиция, ФСБ, прокуратура) и сообщают, что в отношении Вас возбуждено уголовное дело в связи с финансированием экстремисткой, террористической деятельности, поскольку с Вашего банковского счета осуществлен перевод денежных средств в недружественное государство. Либо сообщают, что к ним обратились из службы безопасности банка по поводу приостановленной попытки оформления на имя жертвы кредита. В ходе общения мошенники могут присылать якобы фото удостоверений, повесток, постановлений о возбуждении уголовного дела, подписок о неразглашении следственной тайны и т.д. Злоумышленники могут обращаться к жертве в строгом, практически, командном тоне, иногда доходящим до грубости, нередко используют юридические термины.

## Обман с использованием QR-кода

Жертву убеждают, что ее средства находятся в опасности и указывают на необходимость их внести на «безопасный счет». Мошенники направляют к банкомату с функцией приема денежных средств по QR-коду, после чего просят прислать им через мессенджер сгенерированный QR-код для активации «безопасного счета». Полученный QR-код злоумышленники сканируют в своем банковском приложении. Жертва, находясь в заблуждении, собственноручно вносит средства на счета дропов через банкомат.

## Хищение денежных средств через систему быстрых платежей (СБП)

Например, покупатель на сайте в сети Интернет оставляет заявку на приобретение товара. После чего ему поступает звонок якобы от сотрудника магазина, предлагается скидка на товар, но только при условии оплаты через СБП или QR-коду, затем злоумышленник присылает в мессенджер ссылку, ведущую на страницу с формой оплаты по QR-коду. Покупатель подтверждает платеж и денежные средства поступают на счет мошенника. Важно в такой ситуации связаться со службой поддержки онлайн-магазина, через официальный сайт или приложение. Не сохранять для оплаты в личных кабинетах банковские карты, при возможности заведите отдельную карту для оплаты покупок онлайн.

## Звонок мобильного оператора

Злоумышленник под видом мобильного оператора сообщает, что срок действия вашей сим-карты истек либо истекает, а для его продления необходимо сообщить код, который поступит в смс либо пройти по ссылке, в противном случае сим-карта будет заблокирована. Важно знать, что у сим-карты нет срока действия, сотовые операторы перевыпускают сим-карты только по просьбе потребителей в случае физического износа, потери,



необходимости получения сим - карты другого формата. Выполнив требования мошенников и сообщив код из смс, либо пройдя по ссылке Вы отдаете в руки злоумышленников доступ в свой личный кабинет на сайте оператора связи, после чего мошенники имеют возможность устанавливать переадресацию сообщений на нужный им номер, что позволит сменить пароль от мобильного банка и похитить денежные средства. Вторая разновидность таких преступлений – получение злоумышленником кода из смс, и последующего доступа к аккаунту «госуслуг» для оформления заявок на кредиты в банках.

## «Родственник в беде»

Злоумышленник представляется родственником потерпевшего, знакомым либо представителем правоохранительного органа. При этом просит перевести денежные средства, например, для дачи взятки должностному лицу за урегулирование проблем с ДТП, оплаты медобслуживания ввиду обнаружения тяжелого заболевания, и др. Наиболее подвержены данному виду преступлений пожилые граждане. Звонки совершаются в основном рано утром или поздно вечером, когда жертвы менее склонны к критическому мышлению.

## Хищения с использованием искусственного интеллекта

Мошенниками производится взлом либо копирование аккаунта пользователя в мессенджерах Ватсап, Вайбер, Телеграмм, социальных сетей Вконтакте и дальнейшее направление сгенерированных искусственным интеллектом (нейросетью) голосовых сообщений от имени потерпевшего, которое полностью копирует его голос, используя при этом ранее отправленные сообщения владельца аккаунта. А дальше все по типичной схеме – просьба одолжить взаймы, фото банковской карты для перевода денежных средств. В данной ситуации важно убедиться, что вы общаетесь именно с Вашим знакомым путем звонка по мобильной сети. Сделав это, Вы обезопасите себя и предупредите знакомого о том, что от его имени действуют мошенники. Для того, чтобы не потерять контроль над Вашим аккаунтом никогда не переходите по незнакомым ссылкам, не скачивайте программы из неподтвержденных источников, используйте двухфакторную аутентификацию аккаунтов. Будьте максимально внимательны, поскольку следующим этапом использования искусственного интеллекта может явиться генерация видеоизображений и рассылка видеосообщений от имени родных, коллег, знакомых и т.д.

## Сдача налоговых деклараций и справок о доходах

Звонившие представляются сотрудниками Госуслуг, управления по делам Президента РФ, сообщают, что в рамках декларационной компании проверяют персональные данные лиц, сдавших налоговые декларации либо декларации о доходах. Со слов преступников – для подтверждения следует назвать паспортные данные и код из СМС.