Реестр распространенных мошеннических схем

Схема
«Звонок из банка» Потерпевшему поступает телефонный звонок от имени сотрудника банка, который сообщает сведения об оформлении кредитной заявки на имя собеседника, настаивает на получении данного кредита в целях закрытия заявки и невозможности дальнейшего получения мошенниками второго кредита в рамках отведенного для клиента кредитного лимита, полученные денежные средства собеседник просит оперативно перевести на «безопасный, резервный, специальный» счёт для обеспечения их сохранности. В результате потерпевший переводит деньги мошенникам, телефонный номер оказывается недоступным, контакт прерывается.
«Родственник в беде» Вторым способом мошенничества из числа распространенных является мнимое спасение родственника, попавшего в сложную жизненную ситуацию, а именно: поступает телефонный звонок, собеседник представляется сотрудником правоохранительных органов, сообщает, например, о дорожно-транспортном происшествии, произошедшем по вине его близкого родственника и о возможности избежать уголовной ответственности за определенное вознаграждение. Деньги просят передать сотруднику, который прибудет к потерпевшему. О разговоре просят никому не сообщать, чтобы еще больше не навредить родственнику или ссылаясь на тайну следствия. В данной схеме для передачи денежных средств в большинстве случаев используются курьеры.
«Инвестиции» Следующим способом мошенничества является желание граждан получить быструю прибыль от инвестиционной деятельности. Потерпевший в интернете находит организацию, от имени которой распространяется информация об осуществлении легальной деятельности финансового посредника (форекс-дилера). Лицо, выступая от имени такой компании, злоупотребляя доверием граждан к легальным финансовым институтам, обещая им получение высоких доходов путем торговли на международном финансовом рынке, предлагает перечислить денежные средства на счета определенных организаций, после чего денежные средства похищаются, общение с гражданами прекращается.

«Сайты – двойники» для входа в онлайн-банкинг Вы вводите его название в поисковике и переходите по ссылке, внешний интерфейс страницы очень схож с тем, который Вы привыкли видеть, далее вводите свои данные для входа в онлайн-банкинг или данные банковской карты. После ввода всех данных появляется сообщение об «ошибке оплаты». Аналогичная ситуация может возникнуть с сайтами-«двойниками» известных онлайнритейлеров, маркетплейсов.
«Фейковые объявления» на известных сайтах: «Авито», «Юла» и др. размещаются объявления о продаже техники, автозапчастей, сдаче загородного дома в аренду на выходные/праздники. При выходе на продавца им предлагается перейти для обсуждения деталей сделки и цены в другой мессенджер, перевести оплату за товар/аренду в полном объеме (или частично) через мобильный банк. После чего Ваш номер заносится в «чёрный список», технику/запчасти Вы не получаете, объекта недвижимости, запланированного Вами к аренде, не существует.
«Измена Родине» В связи с проведением СВО, преступники звонят клиенту банка по телефону и представляются сотрудниками ФСБ. После этого они утверждают, что сотрудник банка выкрал персональные данные клиента и теперь от его лица переводит деньги на поддержку украинской армии. При этом злоумышленники убеждают человека, что, если срочно не предпринять никаких действий, тот может быть привлечен к уголовной ответственности за измену Родине. Так мошенники вынуждают жертву подключиться к ложной службе безопасности банка и перевести деньги на их счета. В результате жертва не только переводит злоумышленникам собственные средства, но и, находясь в состоянии повышенной тревоги, берет кредиты и также перечисляет эти суммы мошенникам
«Сообщения в соцсетях» В популярных социальных сетях приходят сообщения от друзей, знакомых с просьбой занять в долг, при этом присылают банковские карты с именем знакомого, но с другим номером карты либо сообщения о проведении каких-либо акций с выигрышем денежных средств.
«Установите приложение» Выявлен случай, когда преступник представляется работником банка и во избежание оформления кредита на имя потерпевшего, просит установить приложение «RustDeskRemoteDesktop», после чего удаленно неизвестные лица оформляют на потерпевшего кредит и переводят средства на различные счета. Приложение «My account»

«Госуслуги» Поступает звонок с неизвестного номера, мошенник представляется сотрудником службы «Госуслуги» и сообщает, что неизвестные преступники пытаются оформить кредит на имя потерпевшего, и для сохранности необходимо перевести деньги на резервный счет.
«Вложение в драг.металл» Поступает звонок с неизвестного номера, преступник представляется финансовым аналитиком и предлагает вложить денежные средства в металл (например – серебро) под высокий процент.
«Сообщение от коллеги, руководителя» Потерпевшему приходит сообщение в мессенджер с незнакомого номера. Преступник представляется коллегой или руководителем, и предупреждает о скором звонке из правоохранительных органов. Нередки случаи, когда посредством мессенджера вместо текстового сообщения приходит голосовое сообщение, в котором с использованием нейро сетей злоумышленники воспроизводят голос знакомого или руководителя. Далее преступники представляются сотрудниками ПО и настоятельно призывают к сотрудничеству, после этого звонят якобы представители финансовых организаций и просят перевести деньги на определенную карту.
«Звонок от оператора связи» Под видом специалистов известных телекоммуникационных компаний мошенники стараются получить доступ к аккаунту человека на «Госуслугах». Злоумышленник звонит жертве и утверждает, что действующий договор заканчивается и его необходимо продлить, иначе номер передадут другому абоненту. При этом мошенники уверяют, что все можно сделать по телефону и не идти в офис, достаточно продиктовать код из СМС, перейти по ссылке, где ввести еще один код. Таким образом человек путем обмана предоставляет мошенникам данные для входа в личный кабинет «Госуслуги».
«Энергосбыт» Поступает звонок на телефон потерпевшего, представляются сотрудниками «Энергосбыта», предлагают заменить сячетчики, после чего на телефон поступает СМС с кодом, который мошенник просит назвать. Далее поступает звонок якобы от «Госуслуг», сообщают что мошенники хотят взломать личный кабинет и что необходимо перевести все денежные средства на «безопасный счет».
«Авито, Юла» гражданин размещает объявление о продаже в приложении «Юла» или «Авито». После этого на его сообщение откликается якобы потенциальный покупатель, который предлагает продолжить общение посредством мессенджера и указывает свой сотовый телефон. Далее злоумышленник пишет что товар его устраивает и

предлагает воспользоваться услугой «безопасная сделка» в приложении и отправляет ссылку в мессенджере, по которой нужно пройти и получить предоплату, а остальную сумму обещает отдать наличными при встрече. Потерпевший переходит по данной ссылке, где его персональные данные автоматически вводятся и снимаются все денежные средства с банковской карты.
«ИркутскЭнерго» Злоумышленники звонят гражданам и представляются сотрудниками «ИркутскЭнерго», сообщают о, чтобы, положенных льготах. Для их получения необходимо назвать данные СНИЛС и ИНН. После получения указанной информации, потерпевшему на телефон поступает звонок с другого номера, где мошенники представляются работниками РОСКОМНАДЗОР и сообщают, что мошенники пытаются похитить со счета денежные средства гражданина. Под влиянием обмана гражданин переводит свои денежные средства на счета мошенников
«Звонок из страховой компании» Злоумышленники звонят гражданам и представляются сотрудниками страховой компании и сообщают об окончании действия медицинского полиса, и что для его продления необходимо назвать код из СМС-сообщения, в котором также указан телефон «Госуслуг» для связи. Далее гражданин называет код мошенникам и перезванивает на номер телефона из СМС. Потерпевшему отвечают мошенники, якобы сотрудники портала «Госуслуги» и сообщают что мошенники взломали его личный кабинет и пытаются оформить на его имя кредиты и необходимо перевести деньги на безопасный счет. Под влиянием обмана гражданин переводит свои и кредитные денежные средства на счета мошенников.
«Вирус Mamont» Посредство мессенджера «Телеграмм» мошенники рассылают ссылки используя недосказанные сообщения, с целью заинтересовать человека перейти по ссылке. При переходе на подобную ссылку (открытие файла) на используемом устройстве распространяется вирус, который в автоматическом режиме завладевает личными данными и рассылает спам-сообщения от имени владельца устройства. Кроме того, данный вирус передает личные данные гражданина мошенникам, с последующей возможностью оформления кредитных договоров, хищения денежных средств со счетов