Наиболее распространенные и новые способы совершения мошеннических действий в отношении граждан дистанционным способом.

№1: На телефон потерпевшего звонят мошенники. В последнее время для звонков чаще используются мессенджеры: «WhatsApp», « Viber», «Telegram». Неизвестные представляются сотрудниками банков: Центрального банка России, Банка «Россия», ПАО «ВТБ», ПАО «Сбербанк» и др. Они называют себя сотрудниками безопасности, службы финансового мониторинга. С их слов, неизвестный якобы пытается оформить кредит от лица потерпевшего, а также обналичить или перевести денежные накопления. Под этим предлогом мошенники предлагают гражданину обезопасить себя от несанкционированного оформления кредита и перевести свои или заемные средства на «безопасный счет», («зеркальный счет», «в безопасную ячейку»). Потерпевший, оказавшись под психологическим прессом мошенников, которые убеждают его, что он может оказаться в долговой кабале на долгие годы, следует их указаниям. Гражданин оформляет через приложение онлайн-заявку, лично обращается в банк, оформляет кредит на крупные суммы, берет свои накопления и переводит через приложение или наличными через платежный терминал на подконтрольные счета или абонентские номера телефонов мошенников.

Мошенники могут представляться сотрудниками правоохранительных органов (МВД, ФСБ, прокуратура, следственный комитет), при этом номер с которого происходит звонок на экране телефона отражается как настоящий номер данного ведомства. Преступники обращаются к потерпевшему по имени отчеству, просят проверить номер их телефона на официальных сайтах ведомств, чтобы убедить потерпевшего, что он общается с настоящим сотрудником. Могут переслать фотографию служебного удостоверения. Все это делается для того, чтобы потерпевший полностью доверился и следовал их указаниям.

Характерным признаком манипуляции является тот факт, что звонящие ведут с потерпевшими длительное общение по телефону, полностью контролируют их действия, говорят о необходимости неразглашения информации об общении с ними. Требуют при общении с настоящими сотрудниками банка при оформлении кредита - не называть истинные цели, а приводить надуманные поводы (беру деньги на строительство, ремонт, на лечение, срочная покупка).

При общении с потерпевшими преступники оказывают психологическое воздействие путем уговоров, угроз, повышенного тона, перекладывания вины на самого потерпевшего за отказ его следовать указаниям звонящего и потере денежных средств. При этом могут ссылаться при разговоре на статьи Уголовного кодекса Российской Федерации о неразглашение информации, за несоблюдение тайны следствия, за отказ от сотрудничества с правоохранительными органами, могут пугать большими штрафами.

Также, в настоящее время, одним из предлогов, используемых мошенниками при звонке гражданину от имени правоохранительных органов является сообщение о том, что его денежные средства используются неизвестными для спонсирования вооруженных сил Украины, в связи с чем потерпевший является соучастником преступной деятельности и для предотвращения данных действий, а также содействия правоохранительным органам, необходимо перевезти денежные средства на «безопасный счет».

Часто, при звонке потерпевшему мошенники просят установить на смартфон программы удаленного доступа (например: AnyDesk, RustDesk и т.д.) убеждая потерпевшего, что данная программа якобы просканирует мобильный телефон и избавит его от вирусов и доступа третьих лиц. После установки таких приложений гражданин предоставляет мошенникам полный доступ к своему смартфону и всем его функциям и приложениям. В результате чего мошенники получают доступ к онлайн-банку доверчивого гражданина и совершают хищение денежных средств с его банковских счетов.

В последнее время, все чаще регистрируются факты, когда мошенники в процессе переговоров с потерпевшим требуют включить демонстрацию экрана при диалоге в мессенджерах («WhatsApp», « Viber», «Telegram»), в результате чего злоумышленники в ходе общения видят все поступающие sms-сообщения на смартфон потерпевшего и имеют возможность получить информацию о кодах доступа к личным кабинетам онлайн-банков без ведома потерпевшего.

Необходимо запомнить: В банках нет «безопасных счетов», «безопасных ячеек», «зеркальных счетов».

Сотрудники банков и правоохранительных органов все вопросы решают при личной (очной встрече), информация по телефону ими не запрашивается.

Работники государственных органов, организаций и учреждений для официального общения с гражданами не используют мессенджеры.

Настоящие сотрудники банков и правоохранительных ведомств не высылают фотоизображения своих служебных удостоверений, документов со своими личными данными! Не используют никакие кодовые слова и пароли для общения!

Недопустимо устанавливать в своих гаджетах, мобильных устройствах, компьютерах по указанию звонящего какие - либо приложения, программы, создавать виртуальные карты, скайпы (программы уделенного доступа).

Недопустимо называть коды, пароли из поступивших смс-сообщений, пуш-уведомлений со своих телефонов посторонним. Таким образом Вы предоставляете вход для мошенников в личные кабинеты банковских приложений, приложений госуслуг, оператора связи и пр., где от вашего имени мошенник может осуществить переводы денежных средств, оформление кредита.

При входящем звонке на телефон, когда роботизированная программа запрашивает сведения об оформлении кредита, предлагает ответить на вопросы односложно: «да», «нет», необходимо прекратить общение.

При разговоре с неизвестными не сообщайте им никаких сведений, реквизитов. При повторных звонках отключите телефон. Если есть сомнения в сохранности имеющихся на счетах денежных средств – обратитесь в банк, позвоните в полицию.

№2: Мошенники могут представляться сотрудниками Госуслуг и работниками оператора сотовой связи. Звонящий утверждает, что вот буквально завтра заканчивается ваш контракт (договор) на мобильную связь. Если его не продлить, вы не сможете звонить, отправлять смс и пользоваться мобильным интернетом. Номер у вас отберут и передадут другому человеку. Мошенник говорит, что и рад бы автоматически продлить договор, но по новому закону он обязан подтверждать паспортные данные абонентов. В офис приезжать не обязательно: все можно сделать через госуслуги. Достаточно продиктовать код из смс. Потерпевший, будучи введенным в заблуждение диктует коды от портала «Госуслуги», коды входа в личный кабинет сотового оператора, коды для входы в личные кабинеты банков, которые мошенники используют для хищения денежных средств.

№3: Дополнительный заработок в сети Интернет. Потерпевшие нередко самостоятельно посредством сети Интернет ищут возможности дополнительного заработка, в результате чего попадают на интернет сайты мошенников предлагающих быстрый заработок путем торгов на различных биржевых (трейдинговых) платформах, которые в свою очередь являются фишинговыми (поддельными). Потерпевший оставляет на интернет-сайте свой абонентский номер, после чего ему поступает звонок от имени трейдера – куратора данной платформы, при этом мошенниками используются названия платформ, которые являются популярными в настоящее время (например «Газпром Инвестиции», «Тинькофф Инвестиции» и т.д.), при этом мошенники не имеют ничего общего с реальными платформами. В ходе общения, мошенники предлагают обучить гражданина особенностям торгов на платформе, гарантируют высокую доходность от вложенных средств (до 300%) в ходе общения потерпевшие устанавливают различные приложения, регистрируются на сайтах, направленных мошенниками, где отражается ложная информация о счетах потерпевшего на платформе, информация о торгах и полученной прибыли. Затем, под предлогами пополнения инвестиционного счета мошенники убеждают граждан осуществлять переводы денежных средств на различные реквизиты. При желании потерпевшего осуществить вывод денежных средств «заработанных» в ходе торгов, мошенники требуют оплатить страховку (налог, комиссию), а после чего, вдруг возникают непреодолимые проблемы с сайтом: сбой программы, технические задержки и т.д. В итоге мошенники перестают выходить на связь.

Еще к распространенным мошенническим действиям относятся схемы, когда аферисты предлагают удаленную работу и гарантируют хороший доход

за выполнение несложных заданий или повышения рейтинга продавца на маркетплейсе, – к примеру, оформляя заказы на сайте маркетплейса, а затем отменяя их. Якобы это повышает рейтинги выбранных продавцов и самой торговой площадки, и маркетплейс готов оплачивать такие услуги. Как правило, такие сообщения приходят в мессенджере с иностранного абоненского номера.

У потерпевшего может создаться ощущение, что он действительно помогаете продавцам, а они в свою очередь платят ему за это вознаграждение. На самом же деле поначалу небольшие деньги потерпевшему переводят мошенники или другие жертвы этой схемы, которые тоже думают, что выполняют задания. Активность в чате преступники обычно имитируют с помощью ботов — это они присылают скрины с подтверждением операций. Так создается видимость, что другие участники постоянно совершают сделки и получают прибыль. С помощью этих уловок аферисты втираются в доверие, усыпляют бдительность и разжигают желание получить больше вознаграждения. Потерпевшего убеждают выбрать задание более высокого уровня и перевести за услугу или товар более крупную сумму. После чего обманщики исчезают, удаляют чаты и переписки, а других способов связаться с ними нет.

№4: Поступление сообщения с аккаунта знакомого с просьбой одолжить денежные средства под различными предлогами (моя карта заблокирована, срочно нужно оплатить товар, не могу зайти в онлайн-банк и т.д.). Потерпевший переводит денежные средства по направленным реквизитам, после чего ему становится известно, что аккаунт знакомого был взломан.

Аккаунты взламывают несколькими способами. Один из них: потерпевшему присылают сообщение с просьбой проголосовать за кого-то или за что-то с обязательным переходом по ссылке. По этому действию этот аккаунт регистрируется на другом устройстве с якобы полученным разрешением.

После взлома аккаунта мошенники проводят молниеносную рассылку по базе последних контактов жертвы с просьбой отправить деньги под предлогом непредвиденных материальных сложностей. При этом сообщения приходят от оригинального пользователя с номером телефона, именем и аватаркой настоящего контакта. В сообщении мошенник пишет, что карта не привязана к номеру телефона, поэтому присылает только номер карты, что не даёт возможность проверить имя и первую букву фамилии.

Нередко мошенники начинают разговор с банального «как дела?» и практически сразу переходят к жалобам на жизнь и просят в долг. Или со словами «лови фотки с дня рождения!» вместо ссылки на фотографии присылают вредоносный вирус. Он крадет с гаджета персональные данные, логины и пароли от личных кабинетов, в том числе от банковских.

Чтобы быстрее войти в доверие, мошенники могут присылать голосовые и видеосообщения, которое подделывают с помощью нейросетей.

Поддельные сообщения выглядят как настоящие и практически полностью копируют манеру речи человека, от лица которого просят деньги. Получателям кажется, что видео или голосовое действительно записал их близкий, поэтому

подозрений обычно не возникает. Иногда мошенники монтируют поддельные сообщения из старых голосовых сообщений, которые нашли в переписке. Их нарезают на отдельные фразы, а затем склеивают подходящие фрагменты

№5: Продажа товаров на сайтах бесплатных объявлений. Например мошенник связывается с продавцом (потерпевшим) и сообщает о своем желании приобрести товар, при этом предлагает внесение предоплаты. После этого, под предлогом проблем с переводом (перевожу со счета ИП, перевожу с чужого банка, нужен отчет и т.д.) убеждает потерпевшего сообщить коды из sms-сообщений, поступающих из банков при помощи которых злоумышленник похищает денежные средства со счета потерпевшего.

Также, существуют следующие схемы обмана: при продаже товара, покупатель (он же мошенник) просит оформить так называемую «безопасную сделку» (гарантия продавца или покупателя) предлагаемую сервисом, на котором размещено объявление. Для чего мошенником направляется потерпевшему фишинговая ссылка на интернет-ресурс (внешнее оформление схоже с сервисом, на котором размещено объявление), где для получения денежных средств от покупателя требуется внести данные банковской карты и поступивший код. После чего денежные средства с банковской карты потерпевшего списываются, а покупатель-мошенник на связь больше не выходит.

Мошенники часто рассылают людям заманчивые предложения по электронной почте, через соцсети и мессенджеры — обычно они активизируются перед праздниками и в периоды распродаж. В их сообщениях всегда есть ссылка, по которой можно купить товар с дополнительной скидкой. Но вместо сайта реального магазина она ведет на сайт-двойник. С его помощью преступники воруют деньги и данные карт доверчивых покупателей.

№6: Участились случаи совершения мошенничеств путем предложения «промокодов» для приобретения игровой валюты. Мошенники часто скрываются под маской интересных собеседников на форумах и в группах в соцсетях. Они заводят с подростками виртуальную дружбу на почве общих интересов и втираются в доверие ради будущей выгоды. В таких случаях действия совершаются в отношении несовершеннолетнего, которому предлагают взять банковскую карту своего родителя и сообщить неизвестному в сети Интернет номер карты, а также поступающие коды из sms-сообщений. Либо сфотографировать (сделать скрин) экрана мобильного телефона и следовать указаниям мошенника, который руководя действиями ребенка осуществляет переводы денежных средств на счета мошенников. При этом сам несовершеннолетний, в силу своего возраста, зачастую не осознает производимые операции и не понимает сути происходящего.

№7: Нередко аферисты рассылают письма и сообщения, в которых обещают подарки, или от имени популярных блогеров запускают рекламу «беспроигрышных лотерей». Но затем за доставку приза или какие-то другие дополнительные услуги просят оплатить небольшую комиссию. Для этого надо пройти по ссылке и ввести данные банковской карты. Но на самом деле ссылка

ведет на фишинговый сайт, и вместо выигрыша доверчивый пользователь получает убытки. Когда конкурс рекламирует блогер, нужно убедиться, что это настоящий аккаунт, а не подделка. Проще всего проверить время создания профиля — если первые посты появились совсем недавно, скорее всего, это фейк. Но иногда и настоящие аккаунты угоняют. Если розыгрыш только начался, стоит подождать пару дней и проверить страницы блогера в других соцсетях и мессенджерах. Возможно, он сам стал жертвой мошенников и предупредит об этом своих подписчиков через другие каналы.

№8: Мошенники все чаще делают подростков соучастниками своих преступных схем. К примеру, когда аферисты воруют или выманивают у кого-то деньги, то стараются не светить свои счета. Сначала они переводят украденные суммы на счета школьников, а затем просят за вознаграждение обналичить деньги или перекинуть их своим сообщникам. Такие промежуточные счета называют дропперскими, а самих посредников — дропперами.

Обычно подростки даже не подозревают, что помогают мошенникам. Зачастую они узнают о дропперской схеме как о простой игре, в которой можно заработать: чем больше денег перекинешь, тем больше получишь. А если приведешь друзей, то сможешь рассчитывать на дополнительную премию. Иногда подростка даже не просят ничего никому перечислять. Достаточно только оформить карту и за вознаграждение передать ее человеку, который выдает себя за выполняющего план продаж сотрудника банка.

Соглашаясь на такие предложения, школьник может нажить серьезные проблемы. Когда его данные попадут в базу дропперов, заблокируются все его карты. И даже если он откроет новую карту в другом банке, она тоже не будет работать. Кроме того, за помощь мошенникам подростку грозит уголовная ответственность.

№9: Подростки с 14 лет могут бесплатно оформить на Госуслугах Пушкинскую карту, на которую государство каждый год начисляет небольшую сумму. С ее баланса можно оплачивать билеты в театры, музеи, кино и на концерты. Пополнять карту, переводить или снимать с нее деньги невозможно.

Но мошенники уверяют, что есть способы перекинуть средства с Пушкинской карты на обычную банковскую. Через каналы в телеграмме или тик-токе они продают некие инструкции, в которых обещают подробно рассказать о разных вариантах вывода денег. Руководство обычно стоит недорого — порядка 100 рублей. Потратить такую сумму многим не жалко, но советы, конечно, не работают.

Иногда аферисты обещают, что сами перекинут деньги с Пушкинской карты — за комиссию. При этом стоимость услуги может доходить до 50% от суммы перевода. Но, получив предоплату, обманщики исчезают.

№10: В конце учебного года активизируются мошенники, которые предлагают купить ответы на вопросы государственных школьных экзаменов — ОГЭ и ЕГЭ. Как правило, они создают группы в соцсетях и телеграмм-каналах.

Аферисты утверждают, что у них есть верные ответы, и обещают прислать их за несколько часов до экзамена. Ученикам предлагают заплатить от 1000 до 20 000 рублей за один или сразу несколько предметов. Но когда подросток переводит нужную сумму, ему приходят решения прошлогодних заданий или какой-то случайный набор ответов. Зачастую мошенники просто исчезают.

Признаваться в том, что хотел обманом сдать экзамен, вряд ли кто-то захочет. Так что преступники понимают, что их жертвы даже не попытаются вернуть деньги.

№11: В летний период мошенники могут выдавать себя за наблюдателей экзаменационной комиссии. Они пишут школьникам в мессенджерах и убеждают, что камеры засекли списывание во время ЕГЭ или ОГЭ — за это подростку грозит штраф.

Чтобы его оплатить, нужно перейти по ссылке из сообщения. Но в реальности она ведет на фишинговую страницу. Если в открывшейся форме оплаты выпускник введет данные банковской карты, мошенники украдут с нее деньги.

Обманщики находят контакты выпускников в украденных базах данных, а также на различных форумах, в группах или телеграмм-каналах, которые посвящены выпускным экзаменам или поступлению в вузы.