***Информация о способах совершения мошеннических действий в сфере информационно-телекоммуникационных технологий:***

1. ***Неправомерное получение доступа к сервису «Государственные услуги», с последующем хищением денежных средств путем обмана.***

*Основными способами неправомерного получения доступа к сервису «Государственные услуги», с последующем хищением денежных средств путем обмана являются:*

***На первом этапе******потерпевшему*** *поступает телефонный звонок с предложением, таким как:*

1. *Продление договора на обслуживание абонентского номера телефона.*
2. *Выпуск (перевыпуск) электронного или пластикового полиса обязательного медицинского страхования.*
3. *Перерасчёт пенсии и пенсионных накоплений в ПФР (Пенсионный Фонд России).*
4. *Получение почтового отправления.*
5. *Установка электро, газо, водосчетчиков, замена ключей домофона.*
6. *Доставка цветов, игрушек.*
7. *Сообщение в мессенджерах «Телеграмм», «Ватцап» и прочих, поступающих от руководителя предприятия с просьбой оказать содействие сотрудникам полиции или ФСБ, в поимке преступников.*

***Вариантов может быть много*** *(это не исчерпывающий список) преступники постоянно меняют предлог.* ***При этом во всех случаях преступник просит продиктовать КОД (ввести в скаченном приложении, чате бота Телеграмм и пр.), поступивший в СМС сообщении*** *от портала* ***«Гос.услуги****»****.***

*После того как мошенник получил* ***«Заветный КОД»*** *следует автоматическая блокировка звонка с голосовым сопровождением «Автоматическая блокировка подозрительного звонка, звонок от мошенников» или в ходе разговора после того как мошенники получили* ***«КОД»*** *начинают обсуждать между собой сколько и в каких банках нужно оформить кредитов на* ***«Жертву».*** *После сообщения КОДА, злоумышленники меняют пароли и условия доступа на портал* ***«Гос.услуги****» и войти в него становиться невозможно.*

***ВАЖНО!!!!! Через портал «Гос.услуги» невозможно переоформить машину, продать или купить дом или гараж, оформить кредит, предоставить кому ни было доверенность на представление своих интересов.***

***ЭТО ВСЁ УЛОВКИ МОШЕННИКОВ !!!!***

*Одной из разновидностью первого этапа является сообщение в мессенджерах «Телеграм», «Ватцап» и пр., поступающих от руководителя предприятия с необходимостью оказания содействия сотрудникам полиции или ФСБ в проведении операции по поимке преступников, зачастую на самом предприятии.*

***Началом второго этапа*** *мошеннической схемы является поступающий звонок от сотрудников правоохранительных органов таких как ФСБ, МВД и пр., а так же представителей Центробанка, Росфинмониторинга. Как правило, звонок поступает в мессенджере «Телеграм», «Ватцап»,* ***при этом в описании имени и в «аватарке» звонящего присутствует описание и символы государственных органов.*** *Во время звонка «псевдо сотрудник» сообщает, что на телефон потерпевшего, только что звонили мошенники, которым он по невнимательности сообщил* ***«КОД»*** *(потерпевший сам это осознает). Все это привело к тому, что сейчас на потерпевшего в нескольких банках оформляются кредиты, переоформляется всё его имущество. При этом «псевдо сотрудник» помогает восстановить доступ на портал* ***«Гос.услуги»*** *и, зачастую при входе в личный кабинет, можно обнаружить запросы в различные учреждения и организации, а так же загруженные файлы (как правило это генеральная доверенность).*

***ВАЖНО!!! Все это создает уверенность у потерпевшего, что он действительно ведет разговор с сотрудниками государственных органов, которые стремятся ему помочь сохранить имущество и денежные средства!!!!***

*Звонящие «псевдо сотрудники» часто используют видео звонки, где ведут разговор в форме сотрудников правоохранительных органов на фоне государственной символики, отправляют сканы личных документов, писем Центробанка, подписок о неразглашении факта сотрудничества и пр.*

*Все сводится к тому, что потерпевший должен действовать в соответствии с указаниями* ***«псевдо сотрудников»,*** *оформить кредиты в банках, продать имущество или совершить иные финансовые операции, а все денежные средства положить на* ***«БЕЗОПАСНЫЙ СЧЕТ»*** *(счет Центробанка и пр.) где его денежные средства смогут быть в безопасности, а все совершенные финансовые операции (кредиты, продажа квартиры, машины и т.п.) в будущем будут аннулированы.*

*Как правило денежные средства кладутся на* ***«БЕЗОПАСНЫЙ СЧЕТ»*** *через банкомат, либо путем переводов на указываемые «псевдо сотрудниками» счета.*

***Для «псевдо сотрудников» особенно важно:*** *никому нельзя сообщать об этом, так как кругом мошенники и шпионы, даже близким родным, сотрудникам банка, где оформляются кредиты и сотрудникам полиции, которые могут приехать по их вызову!!!!*

***2. Инвестиции, заработок в Интернете***

*В сети Интернет, в социальных сетях, в мессенджерах размещается информация либо* ***реклама о легко доступных способах заработка, путем инвестирования денежных средств в различного рода финансовые пирамиды****,* ***биржи, инвестиционные организации и т.д. обещающие за короткий промежуток времени получение пассивного дохода.*** *Не стоит также доверять лицам, рекламе представляющиеся реальными организациями – такими как Газпром-инвестиции Сбербанк-инвестиции, и т.д.* ***В настоящее время реальным и безопасным способом вложения денежных средств являются общеизвестные БАНКИ.***

***Нужно понимать, что бесплатный сыр только в мышеловке.*** *Иногда, с целью заманивания потерпевших в свои преступные сети, при внесении небольших сумм денежных средств, мошенники создают видимость заработка и переводят небольшие денежные средства, создавая ощущение работоспособности финансовой схемы заработка, но это лишь до того момента пока потерпевший не переведет (вложит) крупную сумму денежных средств. Далее связь с потерпевшим прекращается. Так,* ***мошенники предлагают скачать специальное приложение в котором создают псевдо личные кабинеты для инвесторов. В данных кабинетах отображаются внесенные потерпевшими денежные средства. В течении некоторого времени инвестор зарабатывает значительные денежные средства, но для вывода этих денежных средств сначала нужно оплатить страховку, налог и прочие «обязательные платежи», а для этого необходимо дополнительно внести денежные средства.***

 ***ВАЖНО!!! Не нужно никому переводить денежные средства с целью их вложения. Руководствуйтесь принципом: если вопрос касается денежных средств и Интернета, то это почти наверняка мошенники. Зачастую потерпевшие переводят денежные средства на различные счета, в итоге попросту теряют денежные средства.***

*Также мошенники размещают объявления о дополнительном заработке, прикрываясь известными торговыми сетями ОЗОН, Валдберис. Суть заработка заключается в том, что необходимо выкупать товар который сообщают мошенники, за который якобы в последующем будут возвращены денежные средства, а также бонус за выполнение заданий. Всё общение осуществляется в мессенджерах, в основном в Телеграмм.*

***Будьте внимательны, не доверяйте легким способам заработка!!!***

***3. Покупка-продажа товаров в сети Интернет***

***Часто регистрируются случаи мошеннических действий на сайтах бесплатных объявлений (Авито, Юла) либо на сайтах Интернет магазинов.*** *С целью завладения денежных средств мошенники размещают объявления о продаже различных товаров от распространенных до редких. Мошенники предлагают потерпевшим внести предоплату за товар, оформить доставку, скидывают ссылку на которую необходимо пройти для оформления доставки либо совершения оплаты товара.*

*Чтобы уберечься от преступных действий, лучший способ покупки это лично встретиться с продавцом и увидеть товар, после чего произвести оплату.*

***ВАЖНО!!!!******Не переходите по просьбе продавца в мессенджеры для обсуждения покупки-продажи и тем более не переходите по ссылкам****.* ***Значительно низкая цена товара, также может указывать на мошенников.***

*Не редки случаи когда мошенники копируют сайты известных Интернет-магазинов, полностью копируя сайт. Зачастую приходят сообщения о скидках и акциях (в день рождения, годовщине события и пр.). Во всех таких случаях необходимо обращать внимание на доменное имя в адресной строке (начинается на www).* ***Мошенники не могут использовать настоящее доменное имя, для этого регистрируют схожее по названию****.*

*Во всех случая перепроверяйте всю поступающую информацию самостоятельно, используя поисковые системы, сайты отзывов и пр.*

1. ***Сообщения от знакомых с просьбой перевести денежные средства или открыть какой-либо файл.***

*В последнее время значительно увеличилось количество преступлений данного вида.*

*В данном случае в мессенджере приходит сообщение с просьбой занять денег на время. Знакомый просит перевести денежные средства не на свою карту, а карту знакомого, корпоративную или др., так как на свою карту деньги перевести нельзя по различным причинам (лимиты по карте кончился, карту заблокировали и пр.) Часто для убедительности отправляется голосовое сообщение от знакомого, сгенерированное нейросетью.*

***ВАЖНО!!! При поступлении сообщения о просьбе перевода денежных средств, всегда перепроверяйте информацию – перезвоните на обычный телефон и пр.***

*Участились случаи поступления сообщений с просьбой открыть какой-либо неизвестный файл с текстом «посмотри это ты на фото?», «Вы выиграли в лотерею», «проголосуй за ребенка» и пр.*

***ВАЖНО!!!Никогда не открывайте неизвестные файлы, в них содержатся вирусы и их распространяют только злоумышленники.***