Инструкция от мошенников

В Главном управлении МВД России по Челябинской области составили Топ-10 самых распространённых видов мошенничеств. Запомните сами и расскажите своим близким. Как говорится, кто предупреждён – тот вооружён. Будьте бдительны и не попадайтесь на уловки мошенников!



Продление договора услуг сотовой связи

Схема: Злоумышленники звонят от имени сотрудника сотовой связи и сообщают информацию о том, что заканчивается срок действия договора на оказание услуг связи. Для его продления необходимо назвать код из смс.

Защита: сим-карта не имеет срока использования, а обо всех изменениях в тарифе оператор связи информирует сообщениями или уведомлениями через мобильное приложение.

Взлом личной страницы на госуслугах

Схема: Абоненту поступает звонок и на экране телефона появляется логотип портала государственных услуг, что не вызывает сомнений в официальности и правдивости поступающей информации. В ходе общения мошенники под разными предлогами получают данные о паролях доступа к учётной записи, затем меняют их и, используя персональные данные жертвы, оформляют кредиты и обналичивают денежные средства.

Защита: Персональные данные нужно держать в секрете и никому не передавать. Портал госуслуг позволяет получить информацию о документе, удостоверяющем личность, водительском удостоверение и т. д. Предоставив доступ к порталу неизвестным, можно лишиться денежных средств или получить многотысячный кредит.

Перевод на «безопасный счёт»

Схема: Одна из распространённых схем, используемых мошенниками: с вашими счетами происходят странные операции, наверное, это мошенники! Надо обезопасить деньги пока их не перевели себе на счета другие! Жители области переводят свои сбережения, берут многотысячные кредиты и всё перечисляют мошенникам.

Защита: Безопасные счета – это выдумка мошенников. Необходимо прекратить разговор и перезвонить в банк самостоятельно для уточнения информации.

Инвестиции

Схема: В сети интернет через всплывающие окна рекламы появляются объявления о выгодном вложении денежных средств в акции различных компаний. Мошенники убеждают жертву приобрести инвестиционный портфель, а после получения денежных средств, как правило, уже не выходят на связь. Потерпевшие не могут получить свои деньги обратно.

Защита: Для того, чтобы осуществлять инвестирование, необходимо первоначально изучить фондовый рынок, детали вложения денежных средств и возможности их вывода. Не стоит доверять всем, кто представляется финансовыми консультантами и уж тем более вкладывать свои деньги в предложенные неизвестными проекты.

Родственник попал в ДТП

Схема. Одна из наиболее старых, но, как показывает практика, действенных схем. Мошенники звонят на стационарные телефоны, как правило, в позднее ночное и вечернее время и сообщают информацию о том, что «дочь, сын, зять, внук» попали в ДТП. Они торопят родственников с выплатой денег через курьера. Жертвы отдают деньги, и только потом перезванивают родственникам.

Защита: Самое главное – обязательно дозвониться до родственников, а не торопиться отдавать деньги!

Звонок или сообщение от руководителя

Схема: Мошенники создают аккаунт руководителя организации и производят рассылку сообщений сотрудникам с просьбой перевести денежные средства, либо в сообщении содержится просьба ответить на звонок. Мнимый руководитель это делает для того, чтобы жертва доверилась и пошла на контакт, вступила в диалог, и её было проще обмануть.

Защита: Кем бы не представлялись неизвестные, всегда нужно проверять информацию! Обязательно перезвоните руководителю и уточните, давал ли он указания о переводе денег.

Обман при покупке товаров

Схема: Мошенник размещает объявление о продаже товара на популярном сайте. В ходе переписки с покупателем присылает ссылку на один из мессенджеров и потерпевший, переходя по ней, попадает на сайт-двойник оригинального сайта. Потерпевшие вводят банковские реквизиты, и вся информация поступает мошенникам.

Защита: При покупке товара через интернет необходимо внимательно следить за тем, чтобы переписка осуществлялась только на сайте, а не через мессенджеры.

Компенсация за покупку

Схема: Мошенники рассказывают о праве гражданина на компенсацию за ранее приобретённый некачественный товар. Но чтобы получить компенсацию, нужно перевести денежные средства за страховку и другие услуги по доставке денежных средств.

Защита: Компенсации, когда нужно сначала внести свои деньги за ранее приобретённые товары, не существует. Просто прекратите разговор.

Взлом страницы в соцсетях

Схема: Мошенники взламывают страницы в социальных сетях и обращаются к друзьям жертвы с просьбой о переводе денежных средств. Не задумываясь, доверчивые пользователи переводят денежные средства «знакомым», и только спустя время перезванивают и уточняют информацию. В ходе разговора выясняется, что страничка взломана и никакая финансовая помощь не нужна.

Защита: Прежде чем переводить денежные средства, обязательно свяжитесь с тем, кто их просит, задайте уточняющие вопросы, ответы на которые может знать только ваш собеседник. К сожалению, мошенники для обогащения используют любые поводы.

Изменение голоса

Схема: Мошенники генерируют голос жертвы, используя голосовые сообщения, взломав чужой аккаунт. Затем с помощью алгоритмов искусственного интеллекта, так называемых deepfake, они записывают заранее подготовленную речь, только уже голосом родственника или друга своей потенциальной жертвы. Так, с помощью программ подмены номеров, deepfake и методов социальной инженерии мошенник выдаёт себя за члена семьи, родственника или руководителя и звонит с целью получения денег.

Защита: Используйте в разговоре определённое слово, которое будет своеобразным паролем и знать которое должен ограниченный круг людей. Перезвоните самостоятельно тому, кому требуется финансовая помощь и уточните информацию.

Как распознать телефонных мошенников:

- Незнакомцы выходят на вас сами
- С вами говорят о деньгах
- Вас просят сообщить конфиденциальную информацию
- Вас выводят из равновесия
- На вас давят

Важно!

- В любой ситуации сохраняйте спокойствие, проявляйте бдительность и следуйте советам полицейских.

Новости

«Обезопасила» миллионы

Жительница Озёрска перевела мошенникам более двух миллионов рублей.

В Озёрске 60-летняя жительница, выполняя указания телефонного собеседника, взяла два кредита и сняла личные сбережения, которые затем перевела на счета мошенников. В УМВД России по г. Озёрску потерпевшая рассказала, что злоумышленник связался с ней по мессенджеру и представился сотрудником правоохранительных органов. Он заявил, что по её счетам проходят сомнительные операции. Чтобы спасти накопленные денежные средства, а также предотвратить несанкционированные попытки оформления кредита, собеседник убедил пенсионерку снять личные накопления и оформить займы в двух банках, а затем перевести денежные средства для сохранности на «безопасные счета». Общая сумма ущерба составила более двух миллионов рублей, из которых более одного миллиона составили личные накопления. Следственным отделом Управления МВД России по ЗАТО г. Озерск возбуждено уголовное дело по статье «Мошенничество».

Вымогали деньги

Курчатовский районный суд Челябинска вынес приговор семерым участникам организованной преступной группировки «Халиулинские» по делу о вымогательствах, хулиганстве, незаконном приобретении и ношении оружия. Главарём банды оказался уроженец нашего города.

Жертвами, согласно материалам, в основном были предприниматели, у которых члены группировки забирали от нескольких сотен тысяч рублей до миллиона. Самый строгий приговор – 6 лет и 3 месяца колонии строгого режима – получил уроженец Кыштыма Иван Югай. Формально он работал в Челябинске руководителем отдела продаж у одного предпринимателя. Но на самом деле, по версии следствия, был главарём банды. До вступления приговора в законную силу Югай останется под стражей.

В суде установлено, что с 2017 года по май 2020 года члены ОПГ «Халиулинские» терроризировали предпринимателей, нападая на них, вымогая деньги и похищая имущество. Задержали банду после налёта на пункт приёма металлолома. Спецоперацию по задержанию проводили сотрудники угрозыска совместно с ФСБ и при силовой поддержке Росгвардии.

Другим участникам ОПГ суд назначил меньшие сроки. Руслану Саматову назначили четыре года и месяц колонии строгого режима. Ещё два фигуранта – Павел Клевакин и Азат Бабаев – получили по шесть лет и три месяца колонии общего режима, а Нодирбек Аманбаев и Илья Жижкун – четыре года и три года семь месяцев колонии общего режима соответственно. Самый мягкий срок – четыре года условно с испытательным сроком три года – у Максима Сокова.