**1. 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 SMS.

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

**2. Взлом личной страницы на Портале государственных услуг.**

Схема: Абоненту поступает звонок и на экране телефона у абонента появляется фото логотипа 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 учетной 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 государственных услуг позволяет получить информацию о документе, удостоверяющем личность, водительском удостоверение и тд. Предоставив доступ к Порталу неизвестным, можно лишиться денежных средств или получить многотысячный кредит.

 **3. Перевод на «безопасный счет».**

Схема: Одна из распространенных 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, оформляют на себя многотысячные кредиты и все перечисляют мошенникам.

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

 **4. 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, а 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.

 **5. Родственник попал в ДТП.**

Схема. Одна из старых схем, появившаяся вновь. 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. Как правило, жертвы отдают деньги, а только потом перезванивают родственникам.

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

 **6. 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 ее было проще обмануть.

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

 **7.Обман при покупке через сайты объявлений.**

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. Не зная того сами, потерпевшие вводят банковские реквизиты, и вся информация поступает мошенникам.

Защита: при покупке товара через вышеуказанные сайты, необходимо внимательно следить, что переписка осуществлялась только на сайте, а не через Вацап, Вайбер и др. мессенджеры.

 **8.Компенсация за покупку некачественных товаров**

Схема: В рамках этой схемы мошенники рассказывают о праве гражданина на компенсацию за ранее приобретенный некачественный товар. Но для того, чтобы получить компенсацию нужно перевести денежные средства за страховку и другие услуги по доставке денежных средств.

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

 **9. Взлом страницы в социальных сетях.**

Схема: Мошенники взламывают страницы в социальных сетях и обращаются к друзьям жертвы с просьбой о переводе денежных средств, сообщая информацию различного характер о финансовой помощи. Не задумываясь, потерпевшие переводят денежные средства, а через несколько дней только перезванивают знакомым и уточняют информацию. А ходе разговора выясняется, что страничка взломана и никакая финансовая помощь не нужна.

Защита: прежде чем переводить денежные средства, обязательно свяжитесь с тем, кому они предназначены, задайте уточняющие вопросы, ответы на которые может знать только ваш собеседник. К сожалению, мошенники для обогащения используют любые поводы.

**10.Мошенничество с использованием изменения голоса**

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

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

***Общие правила, 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.