Растет число дистанционных мошенничеств в отношении граждан.

Можно выделить пять способов,которые наиболее часто используют преступники.

✔1. Звонок о несанкционированном списании или блокировке банковской карты.

В этом случае звонят чаще с абонентских номеров, которые начинаются с "8800", "499". Во время разговора мошенники представляются сотрудниками службы безопасности банка или несуществующего "центра мониторинга банковских карт" и сообщают, что произошел сбой системы или снятие денег.

В этом случае нельзя сообщать собеседнику номер карты, срок окончания ее действия и трехзначный CVV-код, расположенный на оборотной стороне карты. Именно эти данные , а также поступающие на номер телефона потерпевшего СМС - коды, позволяют мошенникам через интернет - приложение банка получать доступ к счетам и совершать переводы денежных средств.

✔2. Заказ на сайтах и в социальных сетях какого - либо товара по низкой цене. Мошенники предлагают товары по низким ценам. Если жертва преступников внесла предоплату, посылка вовсе не приходит.

Приобретая товары в сети, необходимо использовать только проверенные интернет - магазины. Перед заказом необходимо проверить информацию о продавце. Пострадавшие от действий мошенников люди часто публикуют информацию о том, что сайт или группа по продаже товаров в соцсети являются мошенническими. Особую настороженность должен вызывать продавец, требующий 100% предоплату. Эти меры необходимо соблюдать и во время покупки авиабилетов с использованием сети Интернет.

✔3. Сайты объявлений (avito.ru, youla.ru и т.д.)

Цена может показаться очень низкой. Этим и планируют воспользоваться мошенники. Покупателя попросят внести предоплату, мотивируя высоким спросом на товар. После внесения суммы на счет злоумышленник отключает телефон или тянет время , а объявление с сайта удаляется.

Жертвой мошенников может стать , и пользователь сайта объявлений, самостоятельно разместивший товар для продажи. В ответ на публикацию звонят неизвестные и представляются покупателями. Мошенник пытается выстроить доверительные отношения с потенциальной жертвой, поэтому сообщает о готовности внести предоплату. Для этого "покупатели" просят сообщить конфиденциальную информацию банковской карты продавца и поступающие СМС - коды. Получив данные, преступники подключаются к счету банковской карты через интернет - приложение банка и выводят средства со счета. Чаще всего мошенники используют номера других регионов.

✔4. Сайты и мобильные приложения знакомств.

Мошенники ведут переписку с подложкой страницы. Во время диалога потенциальную жертву просят перевести деньги на счет телефона, заплатить за интернет, сходить вместе в кинотеатр. При этом злоумышленники отправляют ссылку на оплату, а потерпевшие вводят персональные данные своей банковской карты. В результате деньги списываются, профиль

жертвы блокируется. Предложите собеседнику вариант оплаты наличными или при встрече на месте.

✔5. Звонки с "подменных" номеров.

Мошенники звонят с номеров, закрепленных за государственными органами, и сообщают о поимке киберпреступников. Далее просят сообщить номер карты, срок окончания ее действия и трехзначный код, расположенный на оборотной стороне. Мошенники обещают проверить не оказался ли человек жертвой преступления и вернуть средства.

Злоумышленники звонят с номеров, принадлежащих популярным агрегаторам различных услуг. В этом случае жертве предлагается подключить какие -либо услуги, для чего просят сообщить реквизиты карты и СМС -код. Мошенник через мобильное приложение банка получает доступ к счетам и может совершать переводы денежных средств на другие счета.

Для того чтобы избежать мошеннических действий необходимо знать:

✔1) никогда и никому не сообщайте пин-код банковской карты, пароль от мобильного и интернет - банка, трехзначный код на обороте карты, коды из СМС;

✔2) сотрудники банков никогда не запрашивают информацию о банковской карте. Любой подобный звонок, даже если он совершается с номера, схожего на с официальным номером банка, дело рук мошенников;

✔3) если вам звонят и сообщают о каких-то проблемах с вашим счетом, положите трубку сами наберите номер телефона банка, который указан на обороте карты, и выясните все ли в порядке с вашими деньгами;

✔4) совершая покупки или продажи в интернете, на сайтах с бесплатными объявлениями или интернет-магазинах, будьте осторожны. Не сообщайте лишние данные. Для перевода денег достаточно номера телефона или номер карты;

✔5) не переходите по ссылкам в сообщениях от незнакомых людей, которые пришли к вам по почте, в соцсетях или в СМС;

✔6) знакомый в соц.сетях просит перевести ему деньги? Обязательно перезвоните человеку, от лица которого поступает просьба. Его аккаунт может быть взломан;

✔7) не устанавливайте на мобильные телефоны и компьютеры приложения из непроверенных источников.Есть программы, позволяющие удаленно управлять вашим телефоном или компьютером. Используйте лицензионное антивирусное программное обеспечение;

✔8) поступил звонок, что ваш родственник попал в беду и для решения проблемы срочно требуются деньги? Не паникуйте! Положите трубку и перезвоните родственнику. На самом деле с ним все в порядке. Помните! Попытка дать взятку - преступление;

✔9) в любой ситуации сохраняйте бдительность и критическое мышление!

НЕ ПОЗВОЛЯЙТЕ МОШЕННИКАМ ОБМАНЫВАТЬ ВАС!