# Что такое мобильное мошенничество?

**Телефонное** **мошенничество-** вид **мошенничества** в области информационных технологий, в частности, несанкционированные действия и неправомерное пользование ресурсами и услугами, хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, модификации информации или другого вмешательства в работу средств обработки или передачи данных информационно-телекоммуникационных сетей.

Вариантов их огромное множество, но основных видов не так много:

* «Вы выиграли приз…». При этом просит прислать подтверждающую СМС, внести «регистрационный взнос» через интернет-кошелек, купить карточку предоплаты и перезвонить, назвав код. Получив «взнос», мошенник исчезает, а обещанный приз тоже растворяется.
* «Мама, я попал в аварию», когда мошенник отправляет СМС или звонит с неприятной новостью, «жертва» в панике забывает проверить достоверность полученной информации и переводит средства на счета злоумышленников.
* «Блокировка карты». На мобильный телефон приходит СМС «Ваша банковская карта заблокирована. По вопросам разблокировки обращайтесь по телефону…». «Жертва» перезванивает по указанному номеру и «сотрудник банка», которым является мошенник, предлагает пройти к банкомату и совершить несколько операций под диктовку. Результат не заставит себя долго ждать - деньги с карты перейдут на счет мошенников.
* Рассылка вирусов, который помогает злоумышленникам подобраться к банковской карте, привязанной к мобильному телефону, и перевести все деньги на свой счет.

В июне 2021 года Министерство внутренних дел России перечислило шесть основных видов телефонного мошенничества. Самой популярной схемой признано «фейковое» сообщение о родственнике, который попал в беду.

Чтобы не стать жертвой мошенников, стоит не принимать вызовы от незнакомых и скрытых номеров. Можно установить на телефон приложение, которое ищет владельца номера в интернете.

* Не отвечайте на СМС и не открывайте ММС от неизвестных абонентов, в том числе поздравительные сообщения и открытки.
* В случае получения сообщения или звонка о происшествии с родственником, знакомым или другом в беде необходимо попробовать связаться с ним через мессенджеры или позвонить ему. Если же на сообщения и звонки человек не отвечает, то нужно проверить, как давно он был в социальных сетях, а также связаться с людьми, которые чаще всего с ним общаются или могут находиться рядом.
* Никогда не сообщайте никаких персональных данных, даже если вам звонят и представляются сотрудником банка, полиции, мобильных операторов и т. д. Попросите представиться, назвать ФИО, звание-должность, поинтересуйтесь, какой адрес у отделения, офиса, уточните наименование организации. Затем узнайте телефон этой организации и перезвоните.
* Не указывайте настоящий номер телефона и не расплачивайтесь основной картой на малоизвестных сайтах. Не паникуйте, если вам пишут о блокировке счета. Позвоните в банк по номеру на сайте или на карте.