Информация
о появлении новых и наиболее распространенных способах совершения преступлений
с использованием информационно-телекоммуникационных технологий

ГУ МВД России по Челябинской области информирует о появлении новых способов совершения дистанционных мошенничеств:

1. Мошенники под различным предлогом заставляют подростков школьного возраста разглашать данные своих или родительских банковских карт.

На сомнительных и неофициальных сайтах предлагают «бесплатные» игровые предметы, имущество и ценности. Например, «скины» (визуальные образы) в популярных играх «Counter-Strike», «Roblox», либо определенные дополнения и некие коды активации для игры «Minecraft». Аналогичным образом организовано информирование учеников в социальных интернет-сетях или мессенджерах о якобы выигрыше в проведенном розыгрыше. Однако для получения указанных «призов» требуется предоставить данные банковской карты.

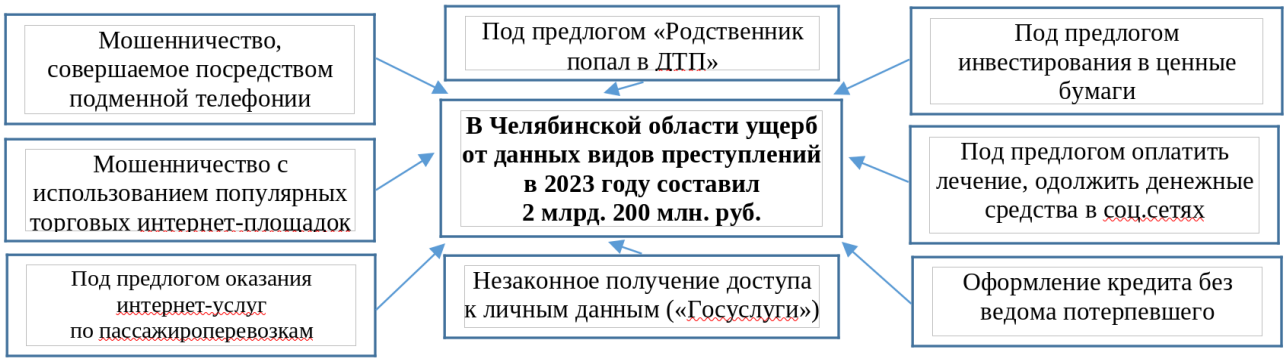
Имеют место случаи, когда розыгрыши действительно проводятся известными «блогерами» (публичными медийными персонами, создающими и публикующими в сети «Интернет» определенный контент) и школьник может участвовать в них. Однако до официального объявления победителей такого конкурса злоумышленники могут назваться представителями организаторов и попытаться получить конфиденциальную информацию (платежные данные).

Кроме того, мошенники предлагают ученикам возможность «заработать в Интернете», используя различные схемы, в том числе финансовые пирамиды и криптовалютные проекты. Подростки, вкладывая деньги в эти проекты, в надежде легкого заработка, рискуют потерять свои средства, которые в итоге попадают на счета злоумышленников.

2. Еще одной распространяющейся мошеннической схемой является обзвон мошенниками абонентов под видом представителей операторов связи с предложением продлить якобы истекающий договор на обслуживание номера телефона.

Во время разговора злоумышленник отвлекает внимание собеседника обилием информации и технических сведений. Затем на номер абонента приходит сообщение с кодом, которое необходимо ввести для «подтверждения пользовательского соглашения о продлении договора на новый срок». Впоследствии злоумышленник сообщает, что направил клиенту ссылку, где необходимо ввести код «для завершения дистанционного подписания пользовательского соглашения». Этот код - данные для входа в личный кабинет потенциальной жертвы на портале «Госуслуги», где возможно получить конфиденциальную персональную информацию.

Кроме того, в настоящее время наиболее распространенными способами совершения дистанционных преступлений остаются:



ГУ МВД России по Челябинской области