ГУ МВД России по Челябинской области информирует о появлении новых видов мошенничеств, совершаемых с использованием IT-технологий:

1. Мошенники под различным предлогом заставляют доверчивых школьников разгласить данные своих или родительских банковских карт. Например, на сомнительных сайтах предлагают «бесплатные» игровые предметы, такие как скины в Counter-Strike, Roblox, читы или дополнения для Minecraft или в других популярных играх. Также распространена схема, при которой в социальных сетях или мессенджерах школьникам сообщают о якобы выигрыше в розыгрыше. Однако для получения приза требуется предоставить данные банковской карты. Иногда розыгрыши действительно проводятся известными блогерами, и школьник может участвовать в них, но до официального объявления победителей неизвестные лица могут назваться представителями организаторов и попытаться получить конфиденциальную информацию/платёжные данные. Кроме того, мошенники предлагают школьникам «заработать» в интернете, используя различные схемы, включая финансовые пирамиды и криптовалютные проекты. Подростки, вкладывая деньги в эти проекты в надежде быстро разбогатеть, рискуют потерять свои средства, которые в итоге попадают на счета злоумышленников.

2. Телефонные мошенники обзванивают абонентов под видом сотовых операторов с предложением продлить якобы истекающий договор на номер телефона. Во время разговора злоумышленник отвлекает внимание собеседника обилием технических деталей. Затем на номер абонента приходит сообщение с кодом, которое необходимо ввести для «подтверждения пользовательского соглашения о продлении договора на новый срок». Затем злоумышленник сообщает, что направил клиенту ссылку, где необходимо ввести код «для завершения дистанционного подписания пользовательского соглашения». Этот код — данные для входа в личный кабинет жертвы на портале Госуслуг.

Помимо указанных способов мошенничеств, наиболее используемыми схемами дистанционных мошенничеств на территории Челябинской области являются: