Преступления, совершаемые с использованием информационно телекоммуникационных технологий, являются актуальной проблемой, затрагивающей многих граждан, проживающих на территории Брянской области. С каждым годом количество зарегистрированных случаев дистанционных хищений растет.

Жертвами таких преступлений становятся граждане любого возраста и финансового положения, однако, наиболее подвержены риску мошенничества лица пожилого возраста.

Мошенники используют различные схемы и способы обмана граждан. Они легко адаптируются под кризисные ситуации и применяют методы социальной инженерии, чтобы реализовывать свой преступный умысел. Как правило, выбор способа мошенничества зависит от целей, который ставят перед собой мошенники, от наличия у них соответствующих ресурсов, времени на подготовку и их квалификации.

Среди наиболее распространенных способов совершения преступлений остаются звонки и сообщения из банков, правоохранительных органов, операторов сотовой связи, а также от знакомых или родственников с целью хищения денежных средств под различными предлогами (отмена оформления несанкционированного кредита, перевода денежных средств за границу, переоформление сим-карты в связи с окончанием срока ее действия для получения доступа к «Госуслугам»).

Наряду с этим мошенники активно используют социальные сети и мессенджеры (WhatsApp, Telegram) для создания фейковых аккаунтов компаний и служб поддержки, рассылки фишинговых ссылок для сбора конфиденциальной информации, в том числе логинов, паролей, а также для использования возможностей искусственного интеллекта в части создания поддельных диалогов.

Злоумышленники не упускают возможности использования кризисов и актуальных событий для создания поддельных сайтов помощи, объявлений о ложных благотворительных акциях, а также для участия в различных инвестиционных проектах.

Отдельной категорией граждан, все чаще попадающей под внимание мошенников, становятся участники специальной военной операции (далее - СВО) и их родственники. Мошенники используют как «классические» способы обмана, так и новые, с учетом специфики СВО. Преступники, пользуясь недостатком правовой грамотности граждан и их эмоциональной уязвимостью, осуществляют звонки, представляясь сотрудниками «спецслужб», сообщая, что их родственник попал в плен, и требуя денежные средства за его освобождение. Кроме того, создаются поддельные сайты

военных организаций или «Госуслуг» для сбора персональных данных граждан под предлогом получения выплат. Также создаются фальшивые фонды и сайты для сбора денег на экипировку и прочие нужды для военнослужащих.

Чтобы противостоять мошенникам необходимо соблюдать простые правила:

- не сообщать персональные данные, реквизиты банковских карт, логины и пароли, коды из смс и пуш-уведомлений;
- не переводить деньги на счета незнакомых людей;
- не устанавливать на телефон приложения из ненадежных источников. Использовать проверенное программное обеспечение на телефоне, в том числе антивирусы и программы для проверки и блокировки нежелательных звонков;
- если сообщают, что родственники попали в беду, связаться с ними напрямую;
- не верить обещаниям гарантированного высокого дохода в короткие сроки;
- игнорировать подозрительные звонки и сообщения из банков, от операторов сотовых услуг и иных организаций. Перезвонить на официальный номер либо обратиться лично в организацию. Важно помнить, что ни банки, ни полиция, ни другие организации не решают вопросы по телефону, особенно, в срочном порядке.