Не стать жертвой телефонных мошенников

Мошенники под видом работников банка, операторов сотовой связи или государственных органов обращаются к гражданам, создают стрессовую ситуацию, сообщают о проблеме, а потом предлагают помощь в ее решении (вишинг). При этом чтобы войти в доверие, могут выслать фото служебных документов или даже выйти по видеосвязи в мессенджере.

Распространен способ, когда злоумышленники, используя различные вымышленные ситуации, убеждают потенциальных жертв загрузить направленный в мессенджере файл или установить определенное мобильное приложение. В обоих случаях мошенники получают возможность удаленно управлять устройством, на котором оно установлено. Таким образом, они получают доступ к личным данным пользователей, в том числе имеют возможность оформить онлайн-кредит. Также злоумышленники убеждают оформить кредиты в банках, а деньги перевести на «защищенный» счет.

Чтобы не попасть на уловки телефонных мошенников, важно соблюдать правила безопасности:

- всегда нужно быть начеку и не доверять незнакомцам;
- ни под каким предлогом не устанавливать непроверенные;

программы и файлы, полученные в мессенджере от неизвестных;

- не передавать кому бы то ни было деньги и не переводить их на банковские счета по указанию незнакомых.

Первый заместитель начальника Горецкого РОВД
начальник криминальной милиции
подполковник милиции С.В. Питяков