Кингисеппская городская прокуратура разъясняет: SMS - фишинг

Телефонное мошенничество сегодня – один из самых распространенных видов преступлений. Сейчас скрыть информацию о себе непросто, мы пользуемся многочисленными сервисами, к которым привязываем банковские карты, оставляем в сети телефонные номера, адреса дома и рабочего офиса при оформлении доставки, вписываем в онлайн-заявки паспортные данные. Технический прогресс упрощает жизнь, но повышает уязвимость.

Мошенникам, получившим доступ к личным данным, часто недостаточно этих сведений, чтобы завладеть деньгами жертвы, так как банки пользуются многоуровневой защитой. Тогда они и звонят людям по телефону, стараясь застать их врасплох, воспользоваться слабостями и даже напугать. Видов мошенничества становится все больше.

Одном из наиболее часто встречающихся видов мошенничества является «SMS-фишинг».

В текстовых сообщениях присылают вредоносные ссылки, при переходе по которым на телефон загружается шпионская программа. Может встречаться и другой вариант – в SMS приходит просьба перезвонить на платный номер, оформить подписку на услугу и т.д.

Как защититься:

- не принимать файлы от незнакомых контактов и не переходить по ссылкам, которые они прислали;

- смотреть на адреса полученных ссылок. Они будут похожи на оригинальные, но в домене найдутся отличия. К примеру, sberbank.ru и sberbank.k.ru;

- не игнорировать предупреждения о сертификате безопасности сайта перед переходом на него.