**«Как не стать жертвой телефонного и интернет-мошенничества».**

В случае, если вам обещают по телефону отсрочку по кредиту, компенсацию, пособие или услуги, но при этом просят данные банковской карты, пароль из sms-сообщения или перевести деньги на банковский счет – вероятно, это попытка похить ваши денежные средства.

Злоумышленники могут рассылать электронные письма со ссылками, ведущими на фишинговые сайты (сайты, подделанные под стиль известных организаций и Интернет-ресурсов, но на самом деле данные сайты направлены на то, чтобы завладеть вашими персональными данными). Не открывайте подозрительные письма, а если все-таки сделали это – не переходите по предложенным ссылкам.

Итак, правила безопасности, которые необходимо соблюдать:

- не сообщайте никому и не вводите на подозрительных сайтах цифры с банковской карты, пароли из sms-сообщений и пин-код.

- набирайте телефоны организаций вручную, а если пользуетесь сайтом – убедитесь, что он настоящий путем проверки адресной строки, она должна в точности соответствовать оригинальному названию.

Помощник прокурора Байкаловского района

юрист 3 класса М.А. Сергеева