**Прокуратура Ленинского района г. Ульяновска разъясняет варианты онлайн-мошенничества.**

Типичные варианты мошенничества с банковскими картами онлайн:

1. При продаже товара или покупке с рук мошенники – потенциальные покупатели или продавцы – просят не только номер карты, но и секретные данные. Этого делать ни в коем случае нельзя!
2. Ваш друг в социальных сетях просит одолжить деньги или отправляет Вам странную ссылку. В таком случае свяжитесь с другом и уточните, действительно ли ему нужна помощь, а также узнайте о достоверности той информации, которую он направил.
3. На Вашу электронную почту приходит письмо с информацией о выигрыше или с предложением работы, которую Вы не искали. В таком случае используйте спам-фильтры, чтобы не попасться на подобную уловку мошенников, а также внимательно изучайте то, что приходит на Вашу почту с незнакомых электронных адресов.
4. Вы перешли на известный сайт, например, ГИБДД или ФНС, однако, заметили некие изменения, которые не замечали ранее – лишняя буква в строке браузера, измененный номер телефона для связи с той или иной службой. При переходе на тот или иной сайт/портал внимательно изучайте его содержание, а также добавьте в закладки браузера те сайты, которыми Вы часто пользуетесь.

Помните о том, что нельзя сообщать посторонним лицам CVV или CVC-коды, ПИН-код банковской карты, срок действия, пароли из банковских уведомлений.

В случае совершения в отношении Вас мошеннических действий сразу же сообщите об этом в правоохранительные органы.