Профилактическая памятка о наиболее распространенных схемах IT-мошенничеств:

1. Сотрудники портала Государственных услуг РФ не требуют сообщать код-пароль в телефонном звонке;
2. Телефонные звонки от «банков» или «правоохранительных органов» (с целью получения личных данных, в том числе для входа в портал Госууслуг, или перевода денег на «безопасный счет»);
3. Фишинговые сайты (фальшивые сайты инвестиционных платформа, банков, маркетплейсов, горорганов, Госуслуг идр.);
4. Ложные вакансии и мошенничество с предоплатой (объявления о работе с выгодными условиями или о продаже товаров).

Основные методы противодействия IT-мошенничеств:

1. Никому не сообщайте код-пароль от портала Государственных услуг РФ;
2. Никогда не передавайте персональные данные посторонним (пароли и коды из SMS и PUSH-уведомлений, реквизиты личных банковских карт (CVC/CVV, срок действия карты и т.д.);
3. Проверять достоверность звонков и сообщений, обращаясь напрямую в банк или организацию;
4. Использовать сложные пароли и двухфакторную аутентификацию для защиты онлайн-аккаунтов;
5. Никогда не переходите по подозрительным ссылкам.

УБК ГУ МВД России по Волгоградской области