ВНИМАНИЕ!

Информация для ознакомления **с наиболее распространенными и новыми схемами IT- мошенничеств:**

- сотрудники портала Государственных услуг РФ не требуют сообщить код-пароль в телефонном звонке;

вызывают опасения:

- телефонные звонки от «банков» или «правоохранительных органов» (с целью получения личных данных, в том числе для входа в Госуслуги, или перевода денег на «безопасный счет» и пр.),
- фишинговые сайты (фальшивые сайты инвестиционных платформ, банков, маркет-плейсов, госорганов, Госуслуги и пр.),
- социальная инженерия в мессенджерах (социальные сети, мессенджеры, вредоносное программное обеспечение и пр.),
- ложные вакансии и мошенничество с предоплатой (объявления о работе с выгодными условиями или о продаже товаров и пр.).

Основные методы противодействия IT- мошенничествам:

- никому не сообщайте код-пароль от портала Государственных услуг РФ;
- никогда не передавайте персональные данные посторонним (пароли и коды из SMS и PUSH-уведомлений, реквизиты личных банковских карт (CVC/CVY, срок действия карты и пр.);
- проверяйте достоверность звонков и сообщений, обращаясь напрямую в банк или организацию,
- используйте сложные пароли и двухфакторную аутентификацию для защиты онлайн-аккаунтов,
- устанавливать обновления программного обеспечения, антивирусы и антиспам-фильтры;
- никогда не переходите по подозрительным ссылкам.