Приложение №1 к распоряжению ВолгГТУ
от «24» 02 2025 г. № 27

Памятка о наиболее распространенных и новых схемах IT-мошенничества

- Якобы сотрудники портала Государственных услуг РФ (далее – Госуслуги) требуют сообщить код-пароль в телефонном звонке;
- телефонные звонки от «банков» или «правоохранительных органов» (с целью получения личных данных, в т.ч. для входа в Госуслуги или перевода денег на «безопасный счет» и пр.);
- фишинговые сайты (фальшивые сайты инвестиционных платформ, банков, маркетплейсов, госорганов, Госуслуг и пр.);
- социальная инженерия в мессенджерах (социальные сети, мессенджеры, вредоносное программное обеспечение и пр.);
- ложные вакансии и мошенничество с предоплатой (объявление о работе с выгодными условиями о продаже товаров и пр.).

НАПОМИНАЕМ основные методы противодействия IT-мошенничествам, в том числе:
- никому не сообщать код-пароль от портала Госуслуг;
- никогда не передавать свои персональные данные посторонним (пароли и коды из SMS и PUSH-уведомлений, реквизиты личных банковских карт (CVC/ CVV, срок действия карты и пр.));
- проверять достоверность звонков и сообщений, обращаясь напрямую в банк или организацию;
- использовать сложные пароли и двухфакторную аутентификацию для защиты онлайн-аккаунтов;
- устанавливать обновления программного обеспечения, антивирусы и антиспам-фильтры;
- никогда не переходить по подозрительным ссылкам.