DAAC digital

# Оценка готовности

пользователей и IT инфраструктуры к противодействию методам социальной инженерии

daacdigital.com

# Ваши сотрудники каждый день на передовой борьбы с киберугрозами

Социальная инженерия – это метод атак, направленный на совершение сотрудниками организации определенных действий или разглашение конфиденциальной информации.

Особую опасность социальная инженерия представляет для финансовой сферы, где путем несложных психологических манипуляций мошенники вынуждают свою жертву сообщить им ценную конфиденциальную информацию или осуществить денежные переводы. При этом злоумышленники активно используют все современные каналы коммуникации с жертвой, начиная с телефонных звонков и заканчивая социальными сетями.

# Оцените Вашу готовность защищаться

DAAC Digital поможет ответить на важные вопросы с помощью уникальной услуги, разработанной на основе накопленного опыта в процессе проведению аудитов информационной безопасности и технических консультаций в реально существующих Организациях различных секторов экономики.

- Пользуются ли ваши пользователя уязвимыми либо скомпрометированными паролями?
- Какие учётные данные утекли в сеть и доступны злоумышленниками для целевой атаки?
- Какой процент пользователей вашей Организации уязвим для фишинговых атак?
- Что именно попадает в почтовые ящики пользователей и насколько система электронной почты соответствует требованиям ваших бизнес процессов?

# Что именно мы предлагаем

1

**Проведение симуляции фишинговой атаки**

для 100 пользователей Организации, для выявления количества персонала, потенциально подверженного данному виду атак

2

**Проведение симуляции Ransomeware атаки**

в процессе моделирования сценариев заражения программами-вымогателями и криптомайнинга для демонстрации уязвимости рабочих станций.

3

**Оценка результативности корпоративной политики безопасности паролей**

в процессе их практического тестирования на наличие 10 типов распространённых угроз, таких как: выбор слабых паролей, использование не уникальных паролей, использование одинакового пароля для различных систем, а также использование сохранённых в браузерах Chrome, Firefox и Edge.

4

**Выявление скомпрометированных паролей пользователей Организации,**

ставших доступными злоумышленникам благодаря известной утечке данных или нахождению на их общедоступных ресурсах, связанных с доменом вашей Организации.

5

**Выявление утекших адресов электронной почты**

и прочих чувствительных идентификационных данных Организации, доступных злоумышленникам в Интернете для запуска проектов социальной инженерии, целевого фишинга и атак программ-вымогателей.

6

**Оценка безопасности конфигурации почтового шлюза**

в процессе обработки 40 типов тестовых сообщений, содержащих прикрепленные файлы защищенные паролем, файлы с макросами, исполняемые файлы или полученные от поддельных доменов.

**Ориентировочная стоимость услуги: $3000**

Для более подробной информации свяжитесь с нами и мы применим все наши знания и опыт, чтобы помочь Вам повысить уровень безопасности в Вашей организации.

DAAC digital

**Moldova**
**www.daacdigital.com**
info@dsi.md

**Uzbekistan**
**www.daacdigital.uz**
info@daacdigital.uz

**Romania**
**www.daacsystems.ro**
info@daacsystems.ro