Памятка
по противодействию фишингу в социальных сетях и мессенджерах
(«социальная инженерия»)

Термин *«социальная инженерия»* обозначает способ получения злоумышленником нужной информации или управления действиями человека без использования технических средств. Основная задача социального инженера — «подобрать ключ» к каждому конкретному человеку и сыграть на его чувствах и эмоциях так, чтобы он забыл про осторожность и совершил необходимые злоумышленнику действия.

Любой ресурс, в том числе Telegram-канал или личный аккаунт, может быть подделан или взломан, поэтому необходимо всегда критически относиться к публикуемой там информации, даже если это хорошо знакомый вам контакт, которому в реальной жизни вы можете безоговорочно доверять.

Жертвой атаки с использованием социальной инженерии может стать каждый человек. Универсального средства защиты от них не существует

Только личная бдительность и критический подход позволит распознать угрозу социальной инженерии и признаки манипуляции Вашими действиями.

Вот простые правила, которые следует неукоснительно соблюдать всем пользователям:

- ➢ Никому и никогда не сообщайте логины и пароли от своих учетных записей. Используйте надежные и уникальные пароли для различных сервисов.
- ➢ Не скачивайте вложения и не переходите по подозрительным ссылкам в письмах, полученных даже от известных Вам лиц.
- ➢ Всегда проверяйте с помощью других доступных каналов связи (телефонного звонка, сообщения в мессенджере), что отправитель письма — именно тот, за кого себя выдает.
- ➢ Блокируйте компьютер, когда уходите от своего рабочего места.
- ➢ Установите на компьютер и смартфон антивирусную программу и регулярно ее обновляйте. Антивирусы умеют распознавать фишинг и недоверенные ресурсы.
- ➢ Тщательно рассматривайте ссылки на предмет несоответствий и опечаток в адресе. Даже если адрес, указанный в ссылке, выглядит верно, по возможности лучше найти указанный сайт в поисковике, перепроверить его адрес или ввести вручную.
- ➢ Не игнорируйте предупреждения браузера, если он сообщает о переходе на недоверенный ресурс или на сайт с некорректными сертификатами безопасности.
- ➢ Соблюдайте традиционные правила кибербезопасности и цифровой гигиены: не сообщайте никому конфиденциальные данные и тем более не оставляйте их в открытом доступе (например, номер телефона в соцсетях), используйте сложные пароли и двухфакторную аутентификацию для входа в приложения и личные кабинеты, делайте резервные копии особенно ценных файлов и документов.

К любому объекту информационных технологий – файлу, веб-ресурсу, электронному письму, программе и т. д. – нужно относиться как к подозрительному до тех пор, пока не доказано обратное.

В случает, если вы подверглись фишинговой атаке, вам необходимо незамедлительно направить заявку в адрес технической поддержки университета!

Адрес для входа в личный кабинет портала самообслуживания: support.adygnet.ru
E-mail технической поддержки: support@adygnet.ru или 777@adygnet.ru
Телефон технической поддержки: 8 8772 210 313 + 777 - добавочный (техподдержка)