

Кибергигиена - ключ к защите от киберугроз в современном обществе

В России с 2022 года продолжается масштабная государственная программа по повышению цифровой грамотности населения. Эта инициатива призвана обучить граждан навыкам безопасного и эффективного использования цифровых технологий в повседневной жизни.

Ключевым компонентом программы является образовательный курс "Кибергигиена", который разработан совместными усилиями Министерства цифрового развития РФ, государственной корпорации "Солар" и Санкт-Петербургского государственного университета телекоммуникаций. Этот курс нацелен на обучение как взрослого, так и детского населения базовым принципам цифровой безопасности.

В рамках программы "Кибергигиена" граждан учат, как защищать свои персональные данные в интернете, как распознавать и противостоять различным киберугрозам, таким как фишинг, вредоносные программы и мошенничество. Особое внимание уделяется безопасному поведению в социальных сетях, мессенджерах и при работе с электронной почтой.

Помимо теоретической части, программа включает в себя и практические занятия, где участники могут отработать навыки цифровой гигиены на реальных примерах. Это позволяет им лучше усвоить полученные знания и применять их в повседневной жизни.

«Реализация программы "Кибергигиена" является важным шагом в укреплении цифровой грамотности российских граждан. По мере развития технологий и распространения интернета такие образовательные инициативы становятся все более актуальными, помогая защитить пользователей от растущих киберугроз». - отмечает министр цифрового развития и связи Амурской области Денис Земнухов.

Узнать о кибергигиене можно:

- На портале «Кибербезопасность — это просто» (<https://www.gusslugi.ru/cybersecurity>) на Госуслугах. Здесь можно познакомиться с важными правилами поведения в интернете. Скачать карточки и поделиться ими с близкими, пройти тест на знание киберграмотности. Раздел посетили более 3 млн. пользователей;

- На сайте «КиберЗОЖ» (<https://киберзож.рф/>) собраны главные полезные привычки для работы в интернете. Здесь вы узнаете какие пароли лучше не использовать, как определить фишинговое письмо и почему стоит подключить двухфакторную аутентификацию;

- На сайте «Прокачай скилл защиты» (<https://прокачайскиллзащиты.рф/>) в игровой форме рассказывают что такое социальная инженерия, как не подхватить цифровой вирус и какие пароли создавать, чтобы их не взломали;

- На сайте «Кибербуллинг» (<https://кибер-буллинг.рф/>) молодые люди узнают что делать с агрессией в интернете, как общаться с недоброжелателями и как известные блогеры справляются с неприятными ситуациями в сети;

- На сайте «Выучи свою роль» (<https://выучисвоюроль.рф/>) подробно рассказывают какие уловки используют телефонные мошенники и как им противостоять. Здесь можно не только узнать, но и потренироваться правильно отвечать на такие звонки с помощью чат-бота.