Цифровая безопасность

Время нельзя остановить, а вместе с ним нельзя остановить и прогресс. Изменения терпят все сферы жизни. Главным отличием нашего постиндустриального общества являются новые технологии. Они открывают перед человеком новые возможности, во многом упрощают жизнь. Благодаря им можно узнать любую интересующую информацию, достаточно просто задать в браузере вопрос, благодаря им можно узнать о любых новостях из разных точек мира, познакомиться с новыми людьми на расстоянии.

Сейчас гаджеты и Интернет собирают в себе почти всё самое необходимое. Современные технологии многое заменили в жизни человека, и большая часть времени уделяется именно им. Сейчас кто угодно может сохранять информацию в цифровых заметках, созваниваться с людьми или расплачиваться электронной картой. Но не стоит забывать, что вместе с этим появляются и новые угрозы. Поскольку Интернет развивается очень быстро, нужно убедиться в собственной безопасности нахождения в нём. Помимо всего остального, на просторах Интернета очень много фальшивой информации, и люди часто попадаются в уловки мошенников, к примеру, ненастоящие ссылки или сайты. Под большей угрозой находятся персональные данные человек, информация, которая должна находиться только у самого человека и не передаваться третьим лицам. К ним относятся данные о электронных картах, IP-адрес, пароли и адреса. Конечно, во многих сайтах или приложениях надо регистрироваться, но и вводится туда то, что находится в открытом доступе, например, адрес электронной почты. И запрашивается раннее перечисленное, то, вводя свои данные, человек ставит их под угрозу потери. Вся информация попадает в руки злоумышленников, которые используют её для своих личных целей, к примеру, ради денег.

К сожалению, таких случаев много, и не всегда получается решить их. Поэтому надо с самого начала быть внимательным и осторожным в Интернете, потому что опасность может поджидать в любой момент и в любом месте. Необходимо заранее проверять на подлинность то, куда человек собирается вводить свои данные. Подозрительные сайты и ссылки лучше обходить, а отправителя - в черный список или жалобу. Информации очень много, и необходимо проверять её по несколько раз. При регистрации на проверенных сайтах стоит придумывать сложные пароли, которые будет сложно взломать и которые нельзя повторять. Ещё один самый простой пример меры информационной безопасности — антивирус, но здесь нужно много чего сделать, чтобы обеспечить безопасность. Средства информационной безопасности защищают данные от утечки, а программы, системы и сети — от взлома, порчи файлов и других видов атак. Это нужно и для защиты серверов, никто не хочет, чтобы их сервис терял работоспособность. Поэтому усиливать безопасность должен не только человек, но и сама компания, у которой хранится информация других людей, потому что за утечку конфиденциальных данных пользователей они несут ответственность по закону.

Без мер по информационной безопасности кто угодно мог бы получить доступ к личным сведениям или взломать любой сайт или систему. Интернетом стало бы невозможно пользоваться,

поэтому необходимо усиливать безопасность своих данных, чтобы со спокойствием им пользоваться.

Обучающаяся 10 класса ГБОУ СОШ №29 г. Сызрани