Кибербезопасность

Стремительное распространение интернет- технологий в повседневной жизни стало отличительной чертой нашего времени. Интернет, как одно из наиболее значимых явлений прогресса, радикально изменил и продолжает изменять жизнь современного человека.

Как любое явление действительности он несёт с собой массу последствий, причём как положительного, так и отрицательного характера. Признавая колоссальную роль Интернета в развитии человечества, инициаторы относительно молодого праздника постарались обратить внимание общественности как раз на те стороны и особенности всемирной паутины, которые играют негативную роль в жизни человека.

Обеспечение безопасности в Интернете – одно из наиболее актуальных требований современности и прогресса. Безопасный и позитивный интернет – это не только специальные защитные программы. Это, в первую очередь, обилие позитивного контента, знания обычных пользователей об основах безопасности и общественный консенсус относительно норм поведения в Сети. Это также и общественно-государственное партнерство, направленное на повышение уровня интернет- безопасности обычных пользователей.

Кибербезопасность — типы угроз

Процесс отслеживания новых технологий, тенденций в области безопасности и анализа угроз — сложная задача. Однако это необходимо для охраны информации и других активов от киберугроз, которые принимают различные формы. Киберугрозы могут включать:

- Вредоносное ПО — это разновидность вредоносного программного обеспечения, которое может быть использовано для нанесения вреда пользователю компьютера с помощью любого файла или программы. Например: компьютерные вирусы, троянские программы и шпионское ПО.
- Атаки программ-вымогателей — это тип вредоносного ПО, при котором злоумышленник блокирует системные файлы жертвы — обычно с помощью шифрования — и требует оплаты за их расшифровку и разблокировку.
- Социальная инженерия — это атака, основанная на взаимодействии человека с целью заставить пользователей нарушить процедуры безопасности для получения конфиденциальной информации, которая обычно защищена.
- Фишинг — это форма мошенничества, при которой рассылаются мошеннические электронные письма, похожие на электронные письма из надежных источников. Однако целью этих писем является кража конфиденциальных данных, например с кредитной карты или логин и пароль для входа в систему.