Информация о правилах кибергигиены

Кибергигиена — это набор действий, направленных на защиту личной и финансовой информации при использовании компьютера или мобильных устройств. Регулярное использование надежных паролей и их изменение, обновление программного обеспечения и операционных систем, очистка жестких дисков и использование комплексного антивирусного ПО помогают избежать современных киберугроз. Кибергигиена включает в себя формирование полезных привычек в области кибербезопасности, которые помогают предотвратить становление жертвой кибератак и минимизировать риски сетевых угроз.
Кибергигиену часто сравнивают с личной гигиеной: в обоих случаях речь идет о регулярных мерах предосторожности для поддержания безопасности и благополучия.
Для соблюдения кибергигиены следуйте приведенным ниже правилам кибербезопасности. Это поможет защитить ваши данные от кражи и их использования в незаконных целях.

1. Надежный пароль
- Не сохраняйте пароли в браузере для предотвращения их утечки при доступе к вашему устройству.
- Используйте уникальные пароли для каждой учетной записи, чтобы минимизировать риски в случае утечки данных.
- Создавайте пароли длиной не менее 8 символов, а лучше — больше. Чем длиннее пароль, тем сложнее его взломать.
- Включайте в пароль комбинации заглавных и строчных букв, цифр и символов для повышения его сложности.
- Избегайте простых паролей, таких как последовательности цифр (например, 1234) или личные данные, которые могут быть легко угаданы (например, дата рождения или имя домашнего животного).
- Не записывайте пароли и не передавайте их другим лицам, чтобы избежать утечек информации.
- Используйте менеджер паролей для безопасного хранения, создания и управления паролями через единую защищенную учетную запись.

2. Сохранность данных
- Не размещайте в социальных сетях личную информацию, такую как домашний адрес, номер телефона или данные кредитных карт.
- Проверьте настройки конфиденциальности в социальных сетях и убедитесь, что они соответствуют вашему уровню безопасности.
- Избегайте участия в викторинах, играх и опросах в социальных сетях, которые требуют предоставления личных данных.
- Осторожно подходите к разрешениям для приложений, чтобы избежать излишнего доступа к личной информации.
- Блокируйте свои устройства (компьютер, телефон) с помощью пароля или PIN-кода для дополнительной защиты данных.

3. Передача данных по сети
- Избегайте разглашения личной информации при подключении к общедоступным сетям Wi-Fi, так как они могут быть небезопасными.
- Используйте виртуальную частную сеть (VPN), особенно при подключении к общедоступным сетям Wi-Fi, чтобы гарантировать максимальную конфиденциальность.

- Будьте внимательны к адресу в браузере — злоумышленники могут создать копию сайта с подменой нескольких символов.
- Проверяйте протокол, используемый сайтом. Современные сайты используют https, что обеспечивает безопасность, в отличие от устаревшего http. Также убедитесь, что ваш роутер поддерживает безопасные протоколы, такие как WPA2 или WPA3.
- Обучайте близких и друзей правилам конфиденциальности в интернете, чтобы они тоже могли защищать свои данные.

4. Безопасность приложений
- Регулярно обновляйте приложения, веб-браузеры, операционные системы и прошивки, чтобы пользоваться последними версиями, в которых устранены уязвимости и ошибки.
- Настройте автоматическое обновление программного обеспечения, чтобы всегда иметь актуальные версии без необходимости вручную проверять обновления.
- Загружайте приложения только из проверенных и официальных источников, чтобы избежать установки вредоносных программ.

5. Защита от атак социальной инженерии
- Не переходите по подозрительным ссылкам, если не уверены в их безопасности.
- Не открывайте письма, которые выглядят подозрительно или приходят от незнакомых отправителей.
- Не скачивайте подозрительные вложения в электронных письмах или текстовых сообщениях, особенно если вы не ожидали их получения.
- Не доверяйте объявлениям, обещающим бесплатные деньги, призы или значительные скидки — это часто уловки мошенников.