Чек-лист правил кибергигиены, чтобы оставаться в безопасности.

Для соблюдения цифровой гигиены используйте правила из приведенного ниже чек-листа по кибербезопасности. Следование этим правилам поможет вам обеспечить соответствие передовым практикам.

Хранение паролей в безопасности.

- Не использовать один и тот же пароль для нескольких учетных записей.
- Регулярно менять пароль.
- Использовать пароли длиной не менее 12 символов (в идеале, длиннее).
- Использовать пароли, в состав которых входят заглавные и строчные буквы, символы и цифры.
- Не использовать простые пароли. В пароле не должны использоваться комбинации последовательных цифр (1234) и личная информация, которую может угадать тот, кто вас знает, например, дата рождения или имя домашнего животного.
- Менять установленные по умолчанию пароли на устройствах интернета вещей (IoT).
- Не записывать пароли и не сообщать их другим людям.
- Использовать менеджер паролей, чтобы создавать, хранить и управлять всеми паролями с помощью единой защищенной учетной записи.

Использование многофакторной аутентификации.

- Настроить защиту с использованием многофакторной аутентификацией для всех основных учетных записей (электронная почта, социальные сети, банковские приложения) с помощью таких приложений, как Google Authenticator или Authy.
- Сохранять резервные коды многофакторной аутентификации в диспетчере паролей.

Регулярное резервное копирование данных.

- Хранить файлы в безопасности и обеспечивать защиту от потери данных, создавая резервные копии важных файлов в автономном режиме, на внешнем жестком диске или в облаке.

Обеспечение конфиденциальности.

- Не публиковать в социальных сетях личную информацию, такую как домашний адрес, личные фотографии, номер телефона, номера кредитных карт.
- Не публикуйте в интернете точный адрес или фотографии, которые позволят понять, где вы живете. Например, очень легко определить место по виду из окна. Делиться текущей геолокацией рекомендуется только с самыми близкими
- Некоторые сервисы запрашивают доступ к фотографиям, геолокации, микрофону и контактам. Давайте разрешение только тогда, когда без него не обойтись. Например, мобильной игре не обязательно знать, где вы находитесь
- Избегать викторин, игр и опросов в социальных сетях, где запрашивается конфиденциальная личная информация.
- Если вы перестали пользоваться сервисом или перешли на другой — удалите свой аккаунт, прежде чем избавиться от приложения навсегда, чтобы не оставлять ему свои персональные данные
- Иногда нужно зайти в свою учетную запись на чужом компьютере. Главное — не забыть разлогиниться после завершения работы и не давать устройству или браузеру запоминать входные данные
- Заблокировать компьютер и телефон с помощью пароля или PIN-кода.
- Стараться не разглашать личную информацию при использовании общедоступных сетей Wi-Fi.
- Не забывать, что использование виртуальной частной сети (VPN), особенно при использовании общедоступных сетей Wi-Fi, помогает обеспечить максимальную конфиденциальность.
- Совершать все онлайн-транзакции на безопасных веб-сайтах, веб-адреса которых начинаются с https://, а не с http://, а слева от адресной строки есть значок замка.
- Рассказывать о конфиденциальности в интернете близким и друзьями, чтобы они также могли соблюдать правила безопасности.

Обновление приложений, программного обеспечения и прошивок.

- Регулярно обновлять приложения, веб-браузеры, операционные системы и прошивки, чтобы использовать последние версии, в которых устранены или исправлены возможные уязвимости безопасности.

- По возможности настраивать функции автоматического обновления программного обеспечения.
- Удалять неиспользуемые приложения.
- Загружать приложения только из надежных или официальных источников.

Обеспечение безопасности роутеров.

- Изменить имя, заданное по умолчанию для домашней сети Wi-Fi.
- Изменить имя пользователя и пароль роутера.
- Поддерживать актуальность прошивки.
- Отключить удаленный доступ, универсальную настройку сетевых устройств (Universal Plug and Play) и настройку защищенного Wi-Fi.
- Создать отдельную сеть для гостей.
- Проверить, поддерживает ли роутер шифрование WPA2 или WPA3 для защиты конфиденциальности информации, передаваемой через вашу сеть.

Защита от атак социальной инженерии.

- Не переходить по подозрительным ссылкам, в которых вы не уверены.
- Не открывать письма, выглядящие подозрительно.
- Не загружать подозрительные вложения в сообщения электронной почты и текстовые сообщения, которых вы не ждете.
- Не переходить по объявлениям, обещающим бесплатные деньги, призы и скидки.
- Хорошая идея, чтобы перестраховаться и не рисковать всеми деньгами в случае утечки данных. Такой счет можно пополнять только на сумму, которой хватит на подписки и онлайн-шопинг.

Использование сетевых экранов.

- Использовать сетевой экран для предотвращения доступа к компьютеру или сети со стороны вредоносных программ через интернет.
- Проверять правильность настройки сетевого экрана.

Шифрование устройств.

- Шифровать устройства и другие носители, содержащие конфиденциальные данные, включая ноутбуки, планшеты, смартфоны, съемные диски, ленты для резервного копирования и облачное хранилище.

Очистка жестких дисков.

- Перед утилизацией или продажей компьютера, планшета или смартфона, необходимо выполнить очистку жесткого диска, чтобы не допустить доступ третьих лиц к вашим персональным данным.

Обеспечение надежной антивирусной защиты.

- Использовать надежное антивирусное программное обеспечение, выполняющее проверку на вирусы и прочие вредоносные программы с последующим их удалением.
- Постоянно обновлять антивирусное программное обеспечение.