



Проверяйте достоверность информации

- Недостоверная информация, найденная в сети Интернет, может стать причиной ошибочных действий, в которых заинтересованы злоумышленники.



Оценивайте профиль виртуальных друзей

- Внимательно оценивайте профиль и действия своих виртуальных друзей, так как среди них могут оказаться мошенники.



Используйте антивирус

- Антивирус поможет выявить вредоносные программы, которые могут нанести вред устройству или привести к потере данных.



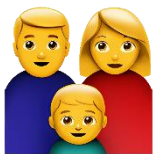
Устанавливайте обновления ОС и ПО

- В программном обеспечении регулярно обнаруживаются новые уязвимости, обновления устраняют опасные недостатки программного обеспечения.



Контролируйте покупки в интернете.

- Под видом онлайн-магазина могут быть мошенники.



Расскажи взрослым

- Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у Вас смущение или тревогу.



Что делать, если заметили подозрительную активность?

При обнаружении необычной активности или попыток взлома аккаунта немедленно примите меры:

- Измените пароль.
- Свяжитесь с поддержкой сервиса.
- Удалите вредоносные программы с устройства.

Полезные советы родителям

- Обучите детей основам цифровой грамотности:
 - Объясните важность конфиденциальности и секретности паролей.
 - Следите за активностью ребёнка в интернете и установите родительские ограничения.
 - Помогите детям отличать доверенные источники от опасных.
 - доверяйте только проверенным источникам.



Помните!

Ваша цифровая гигиена - залог безопасной и комфортной жизни в интернете!

Ваша безопасность зависит от вас самих!

Не вся информация в сети Интернет достоверна!

Информационно-библиографический отдел
центральной библиотеки Канашского МО
Ответственный за выпуск Т.Р. Григорьева
Тел.: 8(83533) 49-7-00;
e-mail: library-shihazan@yandex.ru

**МБУК «ЦБС» Канашского
муниципального округа**

Информационный буклет

«ИНТЕРНЕТ БЕЗ ОПАСНОСТИ: ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ»



Шихазаны, 2026

В современном мире интернет стал неотъемлемой частью нашей жизни. Но как защитить себя и свои данные в этом цифровом пространстве?

Существует множество разнообразных угроз в интернете – от хакерских атак до изощренных мошеннических схем. 96% подростков регулярно сталкиваются с интернет-мошенниками, кибербуллингом, фейками и игровой зависимостью. Но не только дети становятся жертвами сетевых мошенников и агрессоров – знать правила кибербезопасности важно для всех.

Образ киберпреступника постоянно меняется. Сегодня кибермошенничество является поистине массовым явлением. Если не каждый из нас, то хотя бы у каждого есть знакомый, который становился целью кибератаки и пал жертвой кибермошенника.

Что такое цифровая гигиена?

Цифровая гигиена включает комплекс мер, направленных на защиту персональных данных, конфиденциальной информации и устройств от кибератак, мошенничества и кражи данных. Это аналогично обычной личной гигиене, но применительно к онлайн-пространству.

Зачем соблюдать цифровую гигиену?

Цифровая гигиена помогает защитить ваши личные данные, предотвратить мошенничество и обеспечить безопасность онлайн-пространства. Эти правила позволят вам уверенно пользоваться интернетом и избегать рисков.

Основные цели цифровой гигиены:

- Защита личных данных и финансов.
- Предупреждение фишинга и социальной

инженерии.

- Безопасность детей в сети.
- Повышение общей киберграмотности населения.

Основные правила цифровой гигиены



Используйте надежные пароли

- Создавайте уникальные пароли длиной минимум 8 символов, включая буквы разного регистра, цифры и специальные символы.

- Избегайте простых комбинаций вроде «123456» или имени питомца.
- Регулярно меняйте пароли и не повторяйте их на разных сайтах.

- Никому не сообщай свой логин с паролем и не выкладывай их в Интернете-относись к ним бережно.



Включите двухфакторную аутентификацию

- Добавьте дополнительный уровень защиты к своим аккаунтам с помощью SMS-кодов, приложений-аутентификаторов или биометрии.



Обновляйте программное обеспечение

- Устанавливайте обновления операционной системы, браузеров и приложений своевременно. Они часто содержат исправления уязвимостей.



Будьте осторожны с публичными сетями Wi-Fi

- Не передавайте конфиденциальную информацию через общедоступные сети.
- Используйте VPN-сервисы для зашифрованного соединения.



Осторожнее с электронной почтой

- Проверяйте отправителя письма перед открытием вложений или переходом по ссылкам.
- Никогда не сообщайте личную информацию по запросу неизвестных адресатов.



Убедитесь в надежности сайта

- Перед вводом личной информации убедитесь, что сайт защищён протоколом HTTPS.
- Проверьте наличие SSL-сертификата (замочка в адресной строке).



Контролируйте свою активность в социальных сетях

- Ограничивайте доступ посторонних лиц к вашим личным данным.
- Настройте приватность профиля и будьте внимательны к публикациям фотографий и геоданных.



Избегайте подозрительных ссылок

- Никогда не переходите по незнакомым ссылкам, особенно если получили их по электронной почте или SMS от незнакомых адресатов.



Будьте осторожны с публикациями

- Не размещайте фотографии документов, билетов, паспортов и банковских карт. Такие публикации могут привести к краже вашей личности. Чем больше злоумышленник знает о пользователе, тем проще организовать такие атаки.