Обновляйте ПО. Автоматически обновляйте операционную систему, браузер и другие программы.

Используйте контент-фильтры и родительский контроль. Эти инструменты помогают блокировать нежелательный контент и ограничивать время в интернете.

Избегайте публичного Wi-Fi для чувствительных операций. Не входите в онлайн-банкинг или социальные сети через незащищённые сети

Что делать при проблемах

Сообщите взрослым. Если вас запугивают, просят личные данные, предлагают встречу или что-то беспокоит в интернете — немедленно расскажите об этом родителям или педагогам.

Обратитесь за помощью. Можно воспользоваться «горячими линиями»

Рекомендации для родителей

Обсуждайте с детьми их онлайн-активность, спрашивайте, с кем они общаются и что смотрят.

Используйте программы родительского контроля для фильтрации контента и ограничения времени в интернете.

Научите детей доверять интуиции: если что-то в интернете вызывает дискомфорт, нужно прекратить взаимодействие.

Объясните, что не всё в интернете — правда, и важно критически оценивать информацию.

«Безопасность в сети Интернет»

Основные угрозы в интернете

Киберхулиганы. Повторяющиеся сообщения с угрозами, присылаемые по электронной почте, в социальных сетях и чатах. Использование информационных средств с целью запугивания, домогательства или угрозы.

Злоупотребление общим доступом к файлам. Несанкционированный обмен музыкой, видео и другими файлами может быть незаконным или повлечь загрузку вредоносных программ.

Неприличный контент. Материалы и страницы, которые сами по себе не содержат вирусов, но информация на них представляет опасность (например, пропаганда насилия, наркотиков, суицида).

Вторжение в частную жизнь. Риск утечки конфиденциальных сведений при заполнении онлайн-форм.

Нежелательная почта (спам). Массовая рассылка рекламы или массовых сообщений без согласия получателя.

Вредоносные программы (вирусы, трояны). Могут повредить компьютер или украсть данные.

Фишинг. Попытки хищения личных данных (паролей, номеров банковских карт и т. д.) через поддельные сайты или письма.

Правила безопасного поведения

Не разглашайте личные данные. Никогда не указывайте в интернете имя, адрес, номер телефона, пароли, данные банковских карт, любимые места отдыха и т. п..

Используйте надёжные пароли. Создавайте сложные пароли для аккаунтов и не сохраняйте их в открытом виде.

Не открывайте подозрительные файлы и ссылки. Не скачивайте и не запускайте файлы от незнакомых отправителей, не переходите по сомнительным ссылкам.

Настройте приватность аккаунтов. В социальных сетях ограничьте доступ к публикациям и личной информации только для доверенных лиц.

Избегайте общения с незнакомцами. Не принимайте запросы на добавление в друзья от незнакомых людей, не соглашайтесь на личные встречи с интернет-знакомыми.

Проверяйте источники информации. Не распространяйте непроверенные данные и не доверяйте всему, что пишут в интернете.

Используйте лицензионное ПО. Избегайте пиратских версий программ и непроверенных приложений.

Будьте вежливы. Соблюдайте сетевой этикет: не грубите, не оскорбляйте других пользователей.

Технические меры защиты

Установите антивирус и брандмауэр. Регулярно обновляйте антивирусные программы и базы вирусов.