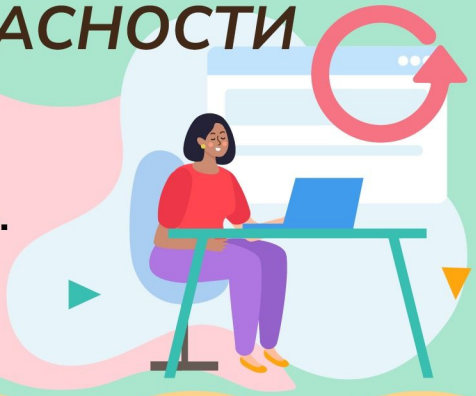
ВАЖНОСТЬ СОБЛЮДЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



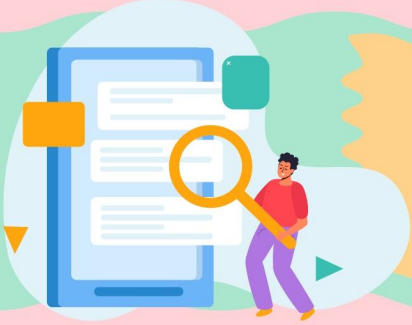
Обновляйте операционную систему и программное обеспечение на своем устройстве. Регулярные обновления помогают закрывать уязвимости и защищать вашу информацию.



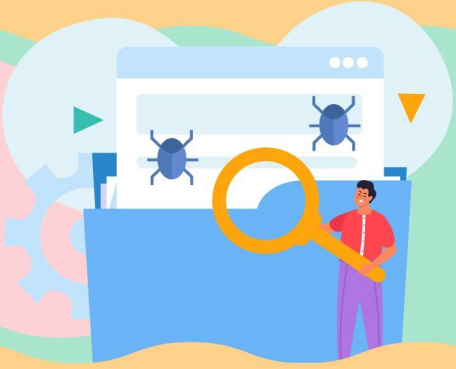
Установите антивирусное программное обеспечение и обновляйте его регулярно. Антивирус поможет защитить вас от вредоносных программ, шпионского ПО и других угроз.



Будьте осторожны при открытии и загрузке вложений в письмах или сообщениях. Не открывайте прикрепленные файлы, если вы не уверены в их безопасности.



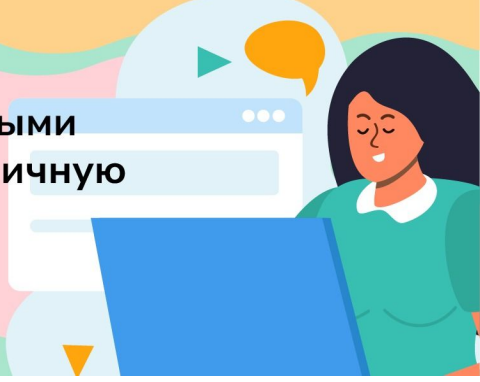
Не переходите по подозрительным ссылкам. Если вам прислали ссылку, неизвестную вам или вызвавшую подозрения, лучше не открывать ее.



Регулярно создавайте резервные копии ваших данных. Используйте внешние накопители или облачные сервисы для хранения важной информации.



Регулярно проверяйте свою систему на наличие вредоносного ПО или других угроз. Установите антишпионское программное обеспечение и выполняйте сканирование системы.



Будьте осторожны при пользовании общедоступными компьютерами или устройствами. Не сохраняйте личную информацию на таких устройствах и не вводите свои учетные данные на непроверенных сайтах.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧАЩИХСЯ

Рекомендации для педагогов



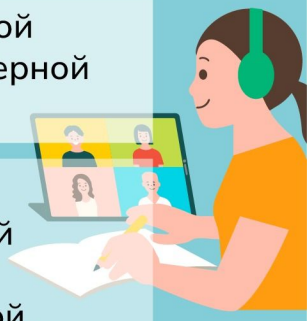
1. Объясните учащимся правила поведения в интернете. Расскажите о мерах, принимаемых к нарушителям, ответственности за нарушение правил поведения в сети.

2. Совместно с учащимися сформулируйте правила поведения в случае нарушения их прав в интернете.



3. Приучайте несовершеннолетних уважать права других людей в интернете. Объясните им смысл понятия *авторское право*, расскажите об ответственности за нарушение авторских прав.

4. Проявляйте интерес к виртуальной жизни своих учеников и при необходимости сообщайте родителям о проблемах их детей.



5. Научите учеников внимательно относиться к информации, получаемой из интернета. Формируйте представление о достоверной и недостоверной информации. Настаивайте на посещении проверенных сайтов.

6. Обеспечьте профилактику интернет-зависимости учащихся через вовлечение детей в различные внеклассные мероприятия в реальной жизни (посещение театров, музеев, участие в играх, соревнованиях), чтобы показать, что реальная жизнь намного интереснее виртуальной.



7. Периодически совместно с учащимися анализируйте их занятость и организацию досуга, целесообразность и необходимость использования ими ресурсов сети для учебы и отдыха с целью профилактики интернет-зависимости и обсуждайте с родителями результаты своих наблюдений.



8. В случае возникновения проблем, связанных с интернет-зависимостью, своевременно доводите информацию до сведения родителей, привлекайте к работе с учащимися и их родителями психолога, социального педагога.

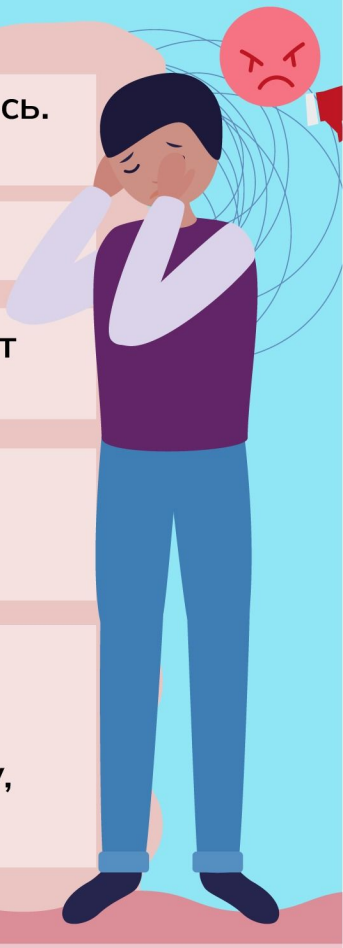
9. Проводите мероприятия, на которых рассказывайте о явлении интернет-зависимости, ее признаках, способах преодоления.

10. Систематически повышайте свою квалификацию в области информационно-коммуникационных технологий, а также по вопросам здоровьесбережения.



11. Станьте примером для своих учеников. Соблюдайте законодательство в области защиты персональных данных и информационной безопасности. Рационально относитесь к своему здоровью. Разумно используйте в своей жизни возможности интернета и мобильных сетей.

ПРИЗНАКИ,
ЧТО ВАШЕГО РЕБЕНКА ТРАВЯТ В ИНТЕРНЕТЕ



- Настроение вашего ребенка за последнее время изменилось. Он грустит, подавлен, капризен или сильно раздражен.
- Плохо спит, потерял аппетит.
- Не так часто, как раньше, пользуется телефоном или может часто проверять его, но ничего не писать.
- Перестал вести свой блог или канал, закрыл страницу в соцсетях, не играет в игры, сменил юзерпик на фигуру, животное или непонятный символ.
- Ребенок избегает общения с родственниками, ровесниками и одноклассниками. Не ходит на дни рождения, на экскурсии, в секции, не хочет ходить в школу, никого не зовет домой.



- Ребенок часто хочет быть один, неохотно отвечает на вопросы и избегает разговоров по душам.
- Падает школьная успеваемость, учителя жалуются, что ребенок «витает в облаках».
- На странице ребенка в соцсетях, в мессенджерах или на игровом сервисе появляются негативные комментарии и оскорбительные картинки.
- На страницах друзей вашего ребенка его фото или мемы с обидными словами или комментариями.
- Вашего ребенка травят очно в школе.





Во всех этих случаях, возможно, ваш ребенок столкнулся с кибербуллингом. Будьте внимательны и не пускайте все на самотек!

ПРИЗНАКИ,
ЧТО ВАШЕГО РЕБЕНКА ТРАВЯТ В ИНТЕРНЕТЕ



В сети ребенок не менее уязвим, чем в реальном мире. Поэтому очень важно не только самим знать правила поведения в виртуальном мире, но и рассказать о них детям.



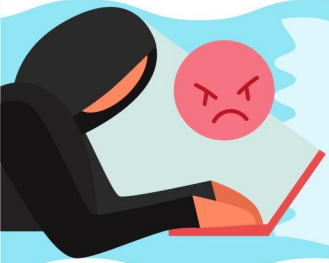
Никому не сообщай личные данные (где живешь, где часто бываешь, номер телефона или школы и т. п.). Личные и другие ценные данные злоумышленники могут использовать для самых разных целей – от финансового мошенничества до буллинга.



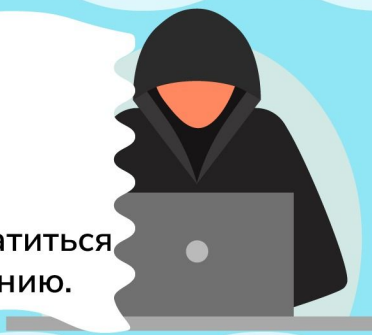
Объясните ребенку, что некоторые объявления или сообщения могут выглядеть как реальные предложения, но это ловушка. С их помощью злоумышленники выманивают деньги и данные людей, распространяют вредоносные приложения и фишинговые ссылки.



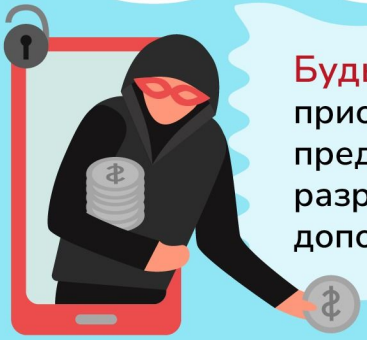
Используй сложные и разные пароли для всех аккаунтов, настрой двухфакторную аутентификацию. Надежный пароль должен состоять минимум из 12 знаков с заглавными и строчными буквами, цифрами и спецсимволами. Чем сложнее и надежнее пароль, тем меньше у злоумышленников возможностей добраться до учетной записи и получить доступ к личным и важным данным.



Если тебя кто-то оскорбляет в сети, не отвечай ему – добавь обидчика в черный список. Если оскорбления очень серьезные или твоей жизни и здоровью угрожают, не бойся рассказать об этом родителям.



Не разговаривай с незнакомцами. Так как общение происходит в виртуальном пространстве (мессенджерах или онлайн-играх), очень сложно понять, кто является собеседником на самом деле. Эту анонимность и используют злоумышленники: входя в доверие, они могут попытаться получить доступ к личной информации, обогатиться за счет пользователя или склонить ребенка к более близкому общению.



Будь внимателен даже в игре! Злоумышленники могут предлагать приобрести игровую валюту по крайне низкой цене или особые предметы, причем последние могут быть вовсе не предусмотрены разработчиками. А еще могут предлагать скачать неофициальные дополнения к игре или саму игру задолго до ее выхода.

СОБЛЮДЕНИЕ ПРАВИЛ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

Рекомендации для родителей



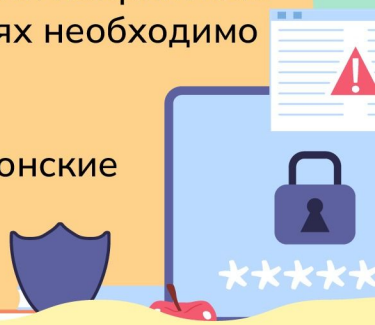
- Открыть диалог с детьми о правилах безопасного поведения в интернете. Объяснить, что они не должны предоставлять онлайн личную информацию незнакомым людям, а также соглашаться на встречу с ними в реальной жизни.

- Установить ограничения в использовании интернета. Например, детям следует разрешить проводить определенное время в интернете, а также осведомиться об их действиях в онлайне.

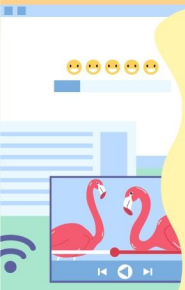


- Научить детей безопасно использовать пароли. Они должны понимать, что пароль необходимо хранить в тайне, не делиться им с другими людьми и использовать уникальные и сложные комбинации символов.

- Обсудить с детьми, что делать, если они получают странные или неприятные сообщения в интернете. Они должны знать, что в таких случаях необходимо незамедлительно сообщить об этом взрослым.



- Убедиться, что у детей установлены антивирусные и антишпионские программы на компьютере или других устройствах, которые они используют для доступа в интернет.



- Осведомить детей о видах мошенничества в интернете, таких как фишинговые атаки или мошенничество по электронной почте. Они должны знать, как распознавать подобные схемы, и быть осторожными при открытии подозрительных ссылок или приложений.



- Подчеркнуть важность безопасности в социальных сетях. Дети должны понимать, что нельзя размещать слишком личную информацию, фотографии или видео, которые могут попасть в «неправильные руки».

- Регулярно проверять активность в интернете детей. Родители должны иметь доступ к истории браузера и аккаунтам своих детей в социальных сетях, чтобы обнаружить возможные нарушения безопасности.



- Напоминать детям о значении «неизвестного», «подозрительного» или «слишком хорошего, чтобы быть правдой» в интернете. Они должны знать, что могут обращаться за помощью к родителям или учителям, если что-то вызывает у них сомнения или тревогу.