

[Метод.рекомендации по созданию сайтов \(DOCX\)](#)

[Методические рекомендации по ограничению доступа \(DOCX\)](#)

Памятка для педагогов об информационной безопасности, которую они должны донести

Нельзя

1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес);
2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;
3. Грубить, придирааться, оказывать давление - вести себя невежливо и агрессивно;

4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей;

5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь;

Осторожно

1. Не все пишут правду. Читаешь о себе неправду в Интернете - сообщи об этом своим родителям;

2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха;

3. Незаконное копирование файлов в Интернете - воровство;

4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут;

5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях;

Можно

1. Уважай других пользователей;

2. Пользуешься Интернет-источником - делай ссылку на него;

3. Открывай только те ссылки, в которых уверен;

4. Общаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут.

Информационная памятка для педагогов и обучающихся

С каждым годом молодежи в интернете становится больше, а школьники одни из самых активных.

Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которых является способность к самовоспроизведению.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ.

2. Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются на операционную систему).

3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволяет вредоносным программам изменять настройки системы.

4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз данных.

5. Ограничь физический доступ к компьютеру для посторонних лиц;

6. Используй внешние носители информации, такие как флешка, диск или файл из интернета,

7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это а

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, же

2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обеспечишь се

3. При использовании Wi-Fi отключи функцию "Общий доступ к файлам и принтерам". Данная с

4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социаль

5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адр

6. В мобильном телефоне отключи функцию "Подключение к Wi-Fi автоматически". Не допускай

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно,

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения;
3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие видели твои фотографии?
4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информацию;
5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой ты ходишь;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв, цифр и специальных символов;
7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда даже если кто-то узнает один из них, он не сможет получить доступ к другим твоим данным.

Электронные деньги

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые пытаются получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах действуют строгие законы.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные биткоины.

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к деньгам.
2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будут нужны пароли.
3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли состоят из букв, цифр и символов.
4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению э

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных п
2. Не указывай в личной почте личную информацию. Например, лучше выбрать "музыкальный_с
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присыла
4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устой
5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;
6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, котор
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Л
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь п

Кибербуллинг или виртуальное издевательство

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивани

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться;
2. Управляй своей киберрепутацией;
3. Анонимность в сети мнимая. Существуют способы выявить, кто стоит за анонимным аккаунтом;
4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия;
5. Соблюдай свою виртуальную честь смолоду;
6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать;
7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность заблокировать пользователя;
8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать его родителям.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь

Современные мобильные браузеры уже практически догнали настольные аналоги, однако рас

Далеко не все производители выпускают обновления, закрывающие критические уязвимости д

Основные советы для безопасности мобильного телефона:

1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают
2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конеч
3. Необходимо обновлять операционную систему твоего смартфона;
4. Используй антивирусные программы для мобильных телефонов;
5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносно
6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки бра
7. Периодически проверяй, какие платные услуги активированы на твоём номере;
8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь
9. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять

Online игры

Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни

Все эти средства идут на поддержание и развитие игры, а также на самую безопасность: соверш

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля,

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке
2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложит
3. Не указывай личную формуацию в профайле игры;
4. Уважай других участников по игре;
5. Не устанавливай неофициальные патчи и моды;
6. Используй сложные и разные пароли;
7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернета

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состо

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необход
2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленни
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены
5. Установи надежный пароль (PIN) на мобильный телефон;
6. Отключи сохранение пароля в браузере;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Л

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компромети

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже посл

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети
2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимое
3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать

Авторское право

Современные школьники - активные пользователи цифрового пространства. Однако далеко не все осознают свою ответственность.

Термин "интеллектуальная собственность" относится к различным творениям человеческого ума

Авторские права - это права на интеллектуальную собственность на произведения науки, лите

Использование "пиратского" программного обеспечения может привести к многим рискам: от по