

**ПАМЯТКА ДЛЯ ДЕТЕЙ**

**«ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСНОГО**

**ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ»**

***Интернет – это виртуальный мир, но здесь также действуют свои правила и границы, свои «НЕЛЬЗЯ!», «ОСТОРОЖНО!», МОЖНО!» Осторожность пригодится и в офлайне, и в онлайне, поэтому делимся с вами простыми правилами, которые очень важно знать именно детям.***

**НЕЛЬЗЯ!**

**1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей), а также личный логин и пароль.**

**2. Отключать антивирус и его настройки.**

**3. Открывать вложенные файлы электронной почты, когда не знаешь отправителя.**

**4. Заходить на сайты, которые защита компьютера считает подозрительной.**

**5. Грубить, придираться, оказывать давление — вести себя невежливо и агрессивно.**

**6. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей.**

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

**8. Не сохраняйте важные сведения на общедоступном или чужом компьютере.**

**МОЖНО!**

**1. Уважай других пользователей.**

**2. Устанавливать антивирусные программы известных производителей.**

**3. Открывай только те ссылки, в которых уверен.**

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

**5. Придумывай сложный пароль!**

**ОСТОРОЖНО!**

1. **Не все пишут правду. Не всей информации в интернете можно верить.**
2. **Читаешь о себе неправду в Интернете — сообщи об этом своим родителям или опекунам.**
3. **Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха.**
4. **Незаконное копирование файлов в Интернете – воровство.**
5. **Всегда рассказывай взрослым о проблемах в сети - они всегда помогут.**
6. **Используй настройки безопасности, чтобы не потерять свои аккаунты в социальных сетях и других порталах.**

**«ОСНОВНЫЕ ОПАСНОСТИ**

**ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ»**

**КОМПЬЮТЕРНЫЕ ВИРУСЫ**

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. Вирусы могут повредить или полностью уничтожить все файлы и данные, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Основная защита - антивирусные программы!

**КИБЕРБУЛЛИНГ**

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернетсервисов.

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, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт.

2. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.

3. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.

4. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.

5. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.

6. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

**ЦИФРОВАЯ РЕПУТАЦИЯ**

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» - это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу. Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

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 содержимого, сделай его только «для друзей»;

3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

**СОЦИАЛЬНЫЕ СЕТИ**

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей.

2. Защищай свою частную жизнь. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы.

3. Защищай свою репутацию - держи ее в чистоте. Подумай, прежде чем что-то опубликовать, написать и загрузить.

4. Избегай групп и пользователей, говорящих на языке насилия и ненависти, призывающих к тем действиям, которые никогда бы не одобрили твои родители.

5. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8.

6. Для социальной сети, почты и других сайтов необходимо использовать разные пароли.

**ОНЛАЙН ИГРЫ**

Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность. В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков.

2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов.

3. Не указывай личную информацию в профайле игры.

4. Уважай других участников по игре.

5. Используй сложные и разные пароли.

6. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

**ЭЛЕКТРОННАЯ ПОЧТА**

Основные советы по безопасной работе с электронной почтой:

1. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный\_фанат@» или «рок2013» вместо «тема13».

2. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль.

3. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь.

4. Не открывай файлы, и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

6. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».