**Памятка для обучающихся об информационной**

**безопасности детей**

**НЕЛЬЗЯ**

1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, атакже фотографии свои, своей семьи и друзей);

2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;

3. Грубить, придираться, 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 или опекунам.

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 и других порталах.

**МОЖНО**

1. Уважай других пользователей.

2. Пользуешься интернет-источником — делай ссылку на него.

3. Открывай только те ссылки, в которых уверен.

4. Обращаться за помощью к взрослым — родители, опе-

куны и администрация сайтов всегда помогут.

5. Пройди обучение на сайте «Сетевичок» и получи паспорт

цифрового гражданина!

**Информационная памятка для обучающихся**

**для размещения на официальных интернет-ресурсах**

 С каждым годом молодежи в интернете становится больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

**Компьютерные вирусы**

 Компьютерный вирус — это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев

распространяются вирусы через интернет.

 ***Методы защиты от вредоносных программ:***

1. Используй современные операционные системы,

имеющие серьезный уровень защиты от вредоносных

программ.33

2. Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей

операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его.

3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере.

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

5. Ограничь физический доступ к компьютеру для посторонних лиц.

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

7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

**Советы по безопасности работы в общедоступных**

**сетях Wi-fi:**

1. Не передавай свою личную информацию через общедоступные сети Wi-Fi. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера.

2. Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твое устройство.

3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе.

4. Не используй публичный wi-fi для передачи личных данных, например для выхода в социальные сети или в электронную почту.

5. Используй только защищенное соединение через HTTPS, а не HTTP, т. е. при наборе веб-адреса вводи именно «https://».

6. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

**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 и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы.

3. Защищай свою репутацию — держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить.

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информацию: имя, место жительства, место учебы и прочее.

5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение.

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

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

**Основные советы по безопасной работе с электронными деньгами:**

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой Платежный пароль или зайдешь на сайт с незнакомого устройства.

2. Используй одноразовые пароли. После перехода на

усиленную авторизацию тебе уже не будет угрожать

опасность кражи или перехвата платежного пароля.

3. Выбери сложный пароль. Преступникам будет непросто угадать сложный пароль. Надежные пароли —

это пароли, которые содержат не менее 8 знаков и

включают в себя строчные и прописные буквы, цифры

и несколько символов, такие как знак доллара, фунта,

восклицательный знак и т. п. Например, $tR0ng!;.

4. Не вводи свои личные данные на сайтах, которым

не доверяешь.

**Основные советы по**

 **безопасной работе**

 **с электронной**

**почтой:**

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых

сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге.

2. Не указывай в личной почте личную информацию.

Например, лучше выбрать «музыкальный\_фанат@» или

«рок2013» вместо «тема13».

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS.

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

взлому пароль.

5. Если есть возможность написать самому свой личный

вопрос, используй эту возможность.

6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах.

7. 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.

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

***Кибербуллинг — преследование сообщениями, со-***

***держащими оскорбления, агрессию, запугивание; хулиган-***

***ство; социальное бойкотирование с помощью различных***

***интернет-сервисов.***

**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. Управляй своей киберрепутацией.

3. Анонимность в сети мнимая. Существуют способы

выяснить, кто стоит за анонимным аккаунтом.

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

5. Соблюдай свою виртуальную честь смолоду.

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

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

8. 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.

**Основные советы для безопасности мобильного теле-**

**фона:**

1. Ничто не является по-настоящему бесплатным. Будь осторожен, ведь, когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.

2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

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 вредоносное программное обеспечение.

6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.

7. Периодически проверяй, какие платные услуги активированы на твоем 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 это.

**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. 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 заразить.

**фишинг** – получение конфиденциальных данных пользователей — логинов и паролей.

**Основные советы по борьбе с фишингом:**

1. Следи за своим аккаунтом. Если ты подозреваешь,

что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее.

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 злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем.

4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты.

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. Лучше уточни

у них, отправляли ли они тебе эти файлы.

 **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.

**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.

**Сетевичок.рф — твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. А также принять участие в конкурсах и стать самым цифровым гражданином!**

**Муниципальное казённое общеобразовательное учреждение «Средняя общеобразовательная школа №7»**

**БРОШЮРА**

**для обучающихся**

Подготовила:

учитель информатики

Усачева И.В.

**ноябрь, 2018 год**

**Полезные интернет-ресурсы**:

[**классный-журнал.дети**](https://www.xn----7sbbxnehfnd6aha6a2i.xn--d1acj3b/)
Интерактивный журнал для детей 7-12 лет. На его страницах живут рисованные герои Пантукль и Жукабра, которые помогают юным читателям весело и с пользой проводить время на сайте. Список развивающих книг, раздел об интернете, кино и экологии, анекдоты и конкурсы — все, чтобы ребенок узнавал новое и не скучал в процессе.

[**профессии.дети**](http://xn--e1agavegjay.xn--d1acj3b/)
Мультимедийный онлайн-сервис профориентации детей и подростков. Здесь собраны видеоинтервью с представителями разных профессий, которые рассказывают о плюсах и минусах своей работы, о качествах и навыках, которые понадобятся специалисту в этой области.

[**персональныеданные.дети**](http://xn--80aalcbc2bocdadlpp9nfk.xn--d1acj3b/)
Повышаем информационную грамотность и рассказываем детям и подросткам о важности [защиты личной информации](http://rocit.ru/knowledge/social-networks/social-media-privacy) в интернете. Портал создан Роскомнадзором.

[**математика-просто.дети**](http://xn----7sbaaxtolczaknpedi.xn--d1acj3b/)
Здесь есть уроки по алгебре и геометрии. А на форуме можно задать вопрос по математике или помочь другому пользователю построить график, решить задачу или теорему.

[**карусель.дети**](https://www.karusel-tv.ru/)
Сайт федерального телеканала «Карусель», вещающего для детей 3-14 лет. К разработке концепции, тем и форматов эфира привлекают детских психологов и педагогов. Ищите здесь познавательные и развлекательные передачи, а также отечественные и зарубежные мультфильмы и кино.

[**здоровые.дети**](https://healthy-kids.ru/)
Самая актуальная информация о здоровье детей и подростков. Цель ресурса — сформировать культуру здорового образа жизни у детей. Кстати, в 2016 году сайт стал лауреатом премии Рунета.