НЕЛЬЗЯ

1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также 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. Общаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут.

ИНФОРМАЦИОННАЯ ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ

Компьютерные вирусы	**Сети WI-FI**	**Социальные сети**	**Электронные деньги**	**Электронная почта**
Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. 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 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	Советы по безопасности работы в общедоступных сетях Wi-fi: 1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера; 2. Используй и обновляй антивирусные программы и брандмауер. 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	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	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 не просто 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	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

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.	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.	имя и другую личную информации: 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	доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;; 4. Не вводи свои личные данные на сайтах, которым не доверяешь	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 или виртуальное издевательство	**Мобильный телефон**	**Online игры**	**Фишинг или кража личных данных**	**Цифровая репутация**
<u>Основные советы по борьбе с кибербуллингом:</u> 1. Не бросайся в бой. Лучший способ:	<u>Основные советы для безопасности мобильного телефона:</u> Ничего не является по-	<u>Основные советы по безопасности твоего игрового аккаунта:</u> 1. Если другой игрок ведет	<u>Основные советы по борьбе с фишингом:</u> 1. Следи за своим аккаунтом. Если ты	Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая

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	настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги; Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге? Необходимо обновлять операционную систему твоего смартфона; Используй антивирусные программы для мобильных телефонов; Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение; После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies; Периодически проверяй, какие платные услуги активированы на твоем номере; Давай свой номер мобильного телефона только людям, которых ты	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.	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	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. <u>Основные советы по защите цифровой репутации:</u> 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.

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.	знаешь и кому доверяешь; Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.		другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.	