



Безопасный интернет!

Памятка родителям для защиты ребенка от нежелательной информации в сети

Объясните своему ребенку, что:

- при общении использовать только имя или псевдоним (ник);
- номер телефона, свой адрес, место учебы нельзя никому сообщать;
- не пересылать свои фотографии;
- без контроля взрослых не встречаться с людьми, знакомство с которыми завязалось в Сети.

Обязательно расскажите о правах собственности, о том, что любой материал, выставленный в Сети, может быть авторским. Неправомерное использование такого материала может быть уголовно наказуемым.

Поясните, что в сети, несмотря на кажущуюся безнаказанность за какие-то проступки, там действуют те же правила, что и в реальной жизни: хорошо - плохо, правильно - не правильно.

Используйте современные программы, которые предоставляют возможность фильтрации содержимого сайтов, контролировать места посещения и деятельность там.

Научите детей следовать нормам морали, быть воспитанными даже в виртуальном общении.



Внимательно относитесь к вашим детям!

- Будьте в курсе того, чем занимаются ваши дети в Интернете. Попросите их научить Вас пользоваться различными приложениями, которыми вы не пользовались ранее.
- Помогите своим детям понять, что они не должны предоставлять никому информацию о себе в Интернете — номер мобильного телефона, домашний адрес, название/номер школы, а также показывать фотографии свои и семьи. Ведь любой человек в Интернете может это увидеть.
- Если Ваш ребенок получает спам (нежелательную электронную почту), напомните ему, чтобы он не верил написанному в письмах и ни в коем случае не отвечал на них.
- Объясните детям, что нельзя открывать файлы, присланные от неизвестных Вам людей. Эти файлы могут содержать вирусы или фото/видео с нежелательным содержанием.
- Помогите ребенку понять, что некоторые люди в Интернете могут говорить неправду и быть не теми, за кого себя выдают. Дети никогда не должны встречаться с сетевыми друзьями в реальной жизни самостоятельно без взрослых.
- Постоянно общайтесь со своими детьми. Никогда не поздно рассказать ребенку, как правильно поступать и реагировать на действия других людей в Интернете.
- Научите своих детей как реагировать, в случае, если их кто-то обидел или они получили/натолкнулись на нежелательный контент в Интернете, так же расскажите куда в подобном случае они могут обратиться.
- Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации.

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 заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

ЗАЩИТИМ ДЕТЕЙ ОТ ВРЕДНОЙ ИНФОРМАЦИИ

Телевизор

- уберите телевизор из детской комнаты;
- разрешайте смотреть ребенку только те фильмы и передачи, которые видели сами и считаете полезными для его развития;
- настройте пароли на телевизоре для доступа к тем каналам, которые могут быть вредны ребенку;
- при совместном просмотре телевизора разъясняйте детям положительные и отрицательные примеры, представленные на экране;
- отдавайте предпочтение просмотру советских фильмов и мультфильмов;
- создайте свою домашнюю видеотеку.



Компьютер

- создайте для ребенка отдельный профиль на компьютере и настройте права доступа – для этого воспользуйтесь функцией Windows «родительский контроль». (Подробная инструкция: <http://o5uw4zdp05zq.nvuwg4tponxwm5bomnxw2.cmle.ru/ru-ru/windows/set-parental-controls#1TC=windows-7> и <http://o53xo.mnugk4tomvsw4zlufzzhk.cmle.ru/windows-roditelskiy-control.html>).
- определите время, которое ребенок может проводить за компьютером;
- с помощью программных средств контролируйте время, которое ребенок проводит за компьютером;
- раз в неделю проверяйте историю действий ребенка за компьютером (Инструкция: <http://obrs223on53wyzlem5ss44tv.cmle.ru/content/kak-posmotret-istoriyu-na-kompyutere>).



Интернет

- установите программное обеспечение (ПО), ограничивающее возможности посещения сайтов, не предназначенных для детей;
- создайте список полезных с вашей точки зрения сайтов и занесите их в строку быстрого доступа;
- раз в неделю проверяйте историю посещаемых ребенком страниц в Интернете (Инструкция: <http://pbqwwzlsfvuxtou.cmle.ru/dlya-chajnika/kak-posmotret-istoriyu-brauzera>);
- еженедельно уделяйте время для совместной деятельности вас и вашего ребенка в Интернете с целью обучения полезному использованию этого ресурса;
- настройте в качестве основных поисковиков «семейный поиск Яндекс» (family.yandex.ru), «безопасный поиск Google» и «безопасный режим YouTube».



Социальные сети

- определите время, когда ребенок может заходить в социальные сети с домашнего компьютера;
- ограничьте количество аккаунтов ребенка в соцсетях одним или двумя;
- создайте свой аккаунт, «подружитесь» с ребенком в социальной сети и раз в неделю со своего аккаунта проверяйте страницу ребенка на наличие недопустимых фотографий, постов, фраз (это вам позволит и лучше узнать интересы ребенка: любимую музыку, фильмы, книги и т.д.);
- ограничьте количество сообществ, в которые может вступать ваш ребенок, ДЕСЯТЬЮ, из которых ПЯТЬ выбирайте сами. Это позволит упорядочить «ленту новостей» ребенка и наполнить ее полезным контентом как минимум наполовину;
- ознакомьтесь с рекомендациями Microsoft по безопасному использованию социальных сетей детьми

(<http://o53xo.nvuwg4tponxwm5bomnxw2.cmle.ru/ru-ru/security/family-safety/kids-social.aspx>).



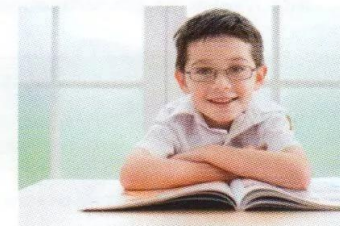
Телефон (планшет)

- раз в неделю проверяйте телефон (планшет) на наличие установленных приложений (в том числе игр); обсуждайте их необходимость, учите ребенка поддерживать порядок в телефоне;
- заблокируйте уведомления в телефоне из социальных сетей, чтобы ребенок не хватался за телефон каждый раз, когда кто-то присылает ему сообщение ВКонтакте или в Одноклассниках (инструкция для iOS: <http://pfqwe3dznmxgg33n.cmle.ru/notification-center-ios7-setup/> для Android: <http://ojsxm2lfo4wxg33gor3wc4tffzzhk.cmle.ru/how-to-disable-notifications-in-android-4-1.htm>);
- подключите к сим-карте ребенка услугу «детский интернет», чтобы заблокировать доступ к опасному контенту (Мегафон, МТС, Билайн);
- ограничьте месячный трафик через телефон/планшет 1 Гб (объем трафика зависит от тарифа).



Печатные издания

- вместе с ребенком выберите несколько периодических изданий и подпишитесь на них (либо регулярно покупайте);
- читайте (или как минимум просматривайте) книги, журналы, газеты, которые читает ваш ребенок.



Методы защиты от вредоносных программ:

- Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- 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;
- Ограничь физический доступ к компьютеру для посторонних лиц;
- Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
- Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ устанавливаться на твоём персональном компьютере;
- Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
- Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «Wireless Fidelity», который переводится как «беспроводная точность». До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «Wi-Fi». Такое название было дано с намеком на стандарт высший звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работе в общедоступных сетях Wi-fi:

- Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
- Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от загрузки вируса на твоё устройство;
- При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
- Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
- Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
- В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

- Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
- 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;
- 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;
- Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
- Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
- При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
- 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.

Электронные деньги

Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги. Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах. В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов – анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

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

Основные советы по безопасной работе с электронными деньгами:

- 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;
- Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
- 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 доллара, фунта, восклицательный знак и т.п. Например, \$tR0ng!;;
- Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя пользователя@ имя домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

- Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
- Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;
- Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
- Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
- Если есть возможность написать самому свой личный вопрос, используй эту возможность;
- 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;
- 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;
- После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Кибербуллинг или виртуальное издевательство

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

Основные советы по борьбе с кибербуллингом:

- 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;
- Управляй своей киберрепутацией;
- Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
- Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
- Соблюдай свой виртуальную честь смолоду;
- Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;



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

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений. Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

- Ничего не является по-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 знаешь и кому доверяешь;
- Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online игры

Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. 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 самую безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов. 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:

- Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
- Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скриншотов;
- Не указывай личную информацию в профайле игры;

- Уважай других участников по игре;
- Не устанавливай неофициальные патчи и моды;
- Используй сложные и разные пароли;
- Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься «любимым» делом. Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как фишинг (от fishing — рыбная ловля, password — пароль).

Основные советы по борьбе с фишингом:

- 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;
 - Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
 - 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;
 - 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;
 - Установи надежный пароль (PIN) на мобильный телефон;
 - Отключи сохранение пароля в браузере;
- 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

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 окружающие 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:

- Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
- В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;
- 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 знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин «интеллектуальная собственность» относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права — это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование «пиратского» программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установленный не легальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.



НЕЛЬЗЯ

- Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей)
- Нельзя открывать вложенные файлы электронной почты, когда не знаешь отправителя
- Нельзя рассылать самому спам и «информационную грязь»
- Нельзя грубить, придирается, оказывать давление — вести себя невежливо и агрессивно
- Никогда не распоряжайся деньгами твоей семьи без разрешения старших. Спроси родителей.
- Встреча с Интернет-знакомыми в реальной жизни, бывает опасной: за псевдонимом может скрываться преступник



ОСТОРОЖНО

- Не все пишут правду
- Читаешь о себе неправду в Интернете — сообщи об этом своим родителям или опекунам
- Приглашают переписываться, играть, обмениваться – проверь, нет ли подвоха
- Незаконное копирование файлов в Интернете = воровство
- Открыл что-то угрожающее — не бойся позвать на помощь.



МОЖНО

- Используй «ник» (выдуманное имя) в переписке и переговорах
- Уважай другого пользователя
- Пользуешься Интернет - источником – делай ссылку на него
- Познакомился в сети и хочешь встретиться – посоветуйся со взрослым, которому доверяешь
- Открывай только те ссылки, в которых уверен
- Интернетом лучше всего пользоваться, когда поблизости есть кто-то из родителей или тех, кто хорошо знает, что такое Интернет, и как в нем себя вести.