Детские безопасные сайты

[**www.saferunet.ru**](http://www.saferunet.ru/) - Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. А конкретнее – он занимаемся Интернет-угрозами и эффективным противодействием им в отношении пользователей. Центр был создан в 2008 году под названием «Национальный узел Интернет-безопасности в России».

[**www.friendlyrunet.ru**](http://www.friendlyrunet.ru/) - Фонд «Дружественный Рунет». Главной целью Фонда является содействие развитию сети Интернет как благоприятной среды, дружественной ко всем пользователям. Фонд поддерживает проекты, связанные с безопасным использованием интернета, содействует российским пользователям, общественным организациям, коммерческим компаниям и государственным ведомствам в противодействии обороту противоправного контента, а также в противодействии иным антиобщественным действиям в Сети. Фонд «Дружественный Рунет» реализует в России комплексную стратегию в области безопасного использования интернета. Основными проектами Фонда являются: Горячая линия по приему сообщений о противоправном контенте, специализированная линия помощи для детей «Дети онлайн» и просветительские проекты.

[**www.fid.su/projects/saferinternet/year/hotline/**](http://www.fid.su/projects/saferinternet/year/hotline/)  - Линия помощи «Дети онлайн». Оказание психологической и практической помощи детям и подросткам, которые столкнулись с опасностью или негативной ситуацией во время пользования интернетом или мобильной связью. Линия помощи "Дети онлайн" является первым и единственным такого рода проектом в России и реализуется в рамках Года Безопасного Интернета в России.

[**www.microsoft.com**](http://www.microsoft.com/)  - Компания **[Microsoft](http://www.microsoft.com/%22%20%5Ct%20%22_blank)** разместила на своем интернет ресурсе много полезной информации по безопасности детей в интернете. Заметки и советы, приведенные ниже, помогут вам обеспечить безопасность детей независимо от того, с какой целью они используют интернет: для поиска информации, разработки школьных проектов, игр или беседы с друзьями. Просмотрев эти видеоролики, вы сможете расширить свои знания по основным вопросам безопасности, касающимся вас как домашнего пользователя. Если вы только приступаете к изучению вопросов, связанных с защитой вашего компьютера и безопасностью информации в сети, вы можете начать с ознакомления с основами:

[**Безопасность дома**](http://www.microsoft.com/rus/protect/default.mspx)

[**Учебные видеоматериалы**](http://www.microsoft.com/rus/protect/videos/default.mspx)

[**Интернет-урок для учителей на тему «Безопасность детей в Интернете»**](http://vision.rambler.ru/users/ramblervision/1/137/) Впервые в России в сети Интернет более 25000 преподавателей со всей территории страны стали первыми участниками двух интерактивных уроков из серии уроков проекта «Всероссийский урок информатики on-line»

[**www.onlandia.org.ua/rus/html/etusivu.htm**](http://www.onlandia.org.ua/rus/html/etusivu.htm)  - ON-ляндия – безопасная веб-страна. На данном сайте представлены материалы для детей, их родителей и учителей — интерактивные сценарии, короткие тесты, готовые планы уроков, — благодаря которым дети смогут освоить основы безопасной работы в Интернете. На сайте предлагается понятная, применимая на практике информация по интернет-безопасности, изучив которую даже начинающие пользователи смогут эффективно использовать ресурсы сети и защитить себя от нежелательного контента.

[**www.webkinz.com/ru\_ru**](http://www.webkinz.com/ru_ru)  - Webkinz - глобальная социальная сеть для детей, которая полностью безопасна и предлагает возможность социальной адаптации к взрослой жизни. Участниками сообщества могут стать обладатели одноименных мягких игрушек, которые несут на себе секретный код для доступа на сайт.

[**www.icensor.ru**](http://www.icensor.ru/) - Интернет-фильтр для детей. Интернет цензор. Программа «Интернет Цензор» предназначена для предотвращения посещения сайтов, противоречащих законодательству РФ, а также любых сайтов деструктивной направленности лицами моложе 18 лет. «Интернет Цензор» обеспечивает родителям полный контроль за деятельностью в сети их детей. «Интернет Цензор» распространяется бесплатно, очень прост в использовании и хорошо защищен от удаления его ребенком.

[**www.tirnet.ru**](http://www.tirnet.ru/) - Детский Интернет адаптирован для детей младшего возраста и их родителей, а также для подростков; он дает возможность не только играть, но и обучаться программированию в инновационной компьютерной среде Скретч; создавать компьютерные игры, ориентированные на самых маленьких пользователей; активно занимается проблемой качества компьютерных игр и сайтов для детей.

[**www.ms-education.ru**](http://www.ms-education.ru/)  и [**www.apkpro.ru**](http://www.apkpro.ru/)   - электронный курс программы "Здоровье и безопасность детей в мире компьютерных технологий и Интернет". Программа представляет собой 72-х часовой курс, состоящий из 6 модулей. Каждый модуль программы дает подробное описание и рекомендации по обеспечению безопасной работы детей с компьютером и Интернетом, а также снабжен обширным списком дополнительной литературы и веб-ссылок. Кроме того, программа содержит объемное приложение, в которое включены диагностические тесты, описания упражнений, а также различные тексты, рекомендованные для использования в процессе ее освоения. Особенностью программы является еще и то, что каждый ее модуль может быть использован как отдельно, так и в комплексе с другими программами повышения квалификации.

[**www.nedopusti.ru**](http://www.nedopusti.ru/)  - социальный проект по защите прав детей «Не допусти» - социальный проект по защите детей от похищений, сексуальной эксплуатации и жестокого обращения реализуется с августа 2009 года. Организаторы проекта: Общественная палата РФ, РОЦИТ (Региональная Общественная Организация «Центр Интернет-технологий»), Межрегиональная правозащитная общественная организация «Сопротивление».

[**http://psyparents.ru**](http://psyparents.ru/)  - Сайт «Детская психология для родителей» создан по заказу Департамента образования города Москвы и является интернет-проектом Московского городского психолого-педагогического университета. Цель проекта — психолого-педагогическое просвещение родителей по возрастным проблемам обучения, воспитания и развития детей, а также профилактике нарушений личностного развития.

[**www.za-partoi.ru**](http://www.za-partoi.ru/)  - Журнал "Здоровье школьников" Ежемесячный журнал «Здоровье школьника» - проект Издательского дома МЦФЭР, который осуществляет выпуск 25 профессиональных журналов федерального значения тиражом 250 тысяч экземпляров ежемесячно и до 100 наименований книг ежегодно общим тиражом около 300 тысяч экземпляров. «Здоровье школьника» - новый журнал о психологии взросления и физическом развитии детей, о возможностях современной медицины, о взаимоотношениях родителей, детей и учителей, о досуге и здоровом образе жизни. Журнал ориентирован на широкий круг читателей, и в первую очередь, на родителей детей школьного возраста.

[**www.newseducation.ru**](http://www.newseducation.ru/)  - "Большая перемена" сайт для школьников и их родителей

[**www.tvidi.ru**](http://www.tvidi.ru/)  - «Твиди» - детский портал-соцсеть: игры, общение, дневники, фотографии и видеоматериалы.

[**www.mirbibigona.ru**](http://www.mirbibigona.ru/) - «Страна друзей»:детская соцсеть: общение, музыка, фотоальбомы, игры, новости.

[**www.smeshariki.ru**](http://www.smeshariki.ru/) - «Смешарики»: развлекательная соцсеть: игры, музыка, мультфильмы.

[**www.solnet.ee**](http://www.solnet.ee/)  - «Солнышко»: детский портал. Развивающие, обучающие игры для самых маленьких и еще много интересного и для родителей.

[**www.1001skazka.com**](http://www.1001skazka.com/)  - «1001 сказка». На сайте можно скачать аудиофайлы — сказки, аудиокниги

[**www.vkids.km.ruNachalka.info**](http://www.vkids.km.runachalka.info/)   - учись, играй, развивайся!

[**www.nachalka.info**](http://www.nachalka.info/)  - это сайт для детей, учащихся в начальной школе, а также их родителей и учителей. Здесь можно учиться и играть, развлекаться и закреплять материал школьной программы! Наш сайт создан для того, что бы сделать обучение по школьной программе интереснее и увлекательнее. Множество упражнений по математике, русскому языку, литературному чтению, окружающему миру не только развлекут ребенка, но и помогут закрепить навыки, требуемые в рамках федерального государственного образовательного стандарта.

[**www.membrana.ru**](http://www.membrana.ru/)  – «Люди. Идеи Технологии». Информационно-образовательный интернет-журнал о новых технологиях.

[**www.teremoc.ru**](http://www.teremoc.ru/)  - Детский сайт «ТЕРЕМОК» с развивающими играми, загадками, ребусами, мультфильмами.

[**www.murzilka.org**](http://www.murzilka.org/)  - Сайт журнала «Мурзилка» со стихами, раскрасками, конкурсами и другой полезной информацией.

[**www.ladushki.ru**](http://www.ladushki.ru/)   - Сайт для малышей и малышек. Мультфильмы, азбука, счет, рисунки.

[**www.girl-and-boy.ru/index/about\_girl\_and\_boy/0-14**](http://www.girl-and-boy.ru/index/about_girl_and_boy/0-14)  - Это сайт для подростков! Вся их жизнь как на ладони. Можно найти ответы на любые интересующие тебя вопросы, поделиться радостью и горестью, узнать много нового, о чём раньше даже и думать не мог. Познакомься с замечательными людьми. Общайся и заводи новых друзей. Этот мир создан для тебя!

[**www.pioner0001.narod.ru**](http://www.pioner0001.narod.ru/)  - Пионерские странички о дружбе, друзьях и товарищах.

[**www.e-parta.ru**](http://www.e-parta.ru/)  - Блог школьного «Всезнайки» - это ленты новостей по всем школьным предметам, виртуальные экскурсии, психологические и юридические советы по проблемам в школе и на улице, учебные видео-фильмы, обзоры лучших ресурсов Всемирной паутины.

**www.teenclub.ru - «Teen**club» - портал для подростков. Все в одном месте: рефераты, сочинения, гороскопы, анекдоты, новости, образование, любовь, игровые новинки, здоровье, мода, стиль, знакомства, объявления, форумы, чат, раскрутка сайтов, дизайн и многое другое.

[**www.web-landia.ru**](http://www.web-landia.ru/)  - Страна лучших сайтов для детей.

         [**http://www.nachalka.com/node/950**](http://www.nachalka.com/node/950) Видео «Развлечение и безопасность в Интернете».

         [**http://i-deti.org/**](http://i-deti.org/) портал «Безопасный инет для детей», ресурсы, рекомендации, комиксы.

         [**http://сетевичок.рф/**](http://xn--b1afankxqj2c.xn--p1ai/)сайт для детей — обучение и онлайн-консультирование по вопросам кибербезопасности, сетевой безопасности.

         [**http://www.igra-internet.ru/**](http://www.igra-internet.ru/) — онлайн интернет-игра «Изучи Интернет – управляй им».

         [**http://www.safe-internet.ru/**](http://www.safe-internet.ru/)— сайт Ростелеком «Безопасность детей в Интернете, библиотека с материалами, памятками, рекомендациями по возрастам.

         [**http://www.fid.su/projects/deti-v-internete**](http://www.fid.su/projects/deti-v-internete)сайт Фонда Развития Интернет.

         [**http://content-filtering.ru/**](http://content-filtering.ru/)сайт «Ваш личный интернет», советы, рекомендации для детей и родителей по безопасной работе в Интернет.

         [**http://www.ligainternet.ru/**](http://www.ligainternet.ru/)Лиги безопасного Интернета.

         [**http://ppt4web.ru/informatika/bezopasnyjj-internet.html**](http://ppt4web.ru/informatika/bezopasnyjj-internet.html)презентации о безопасном Интернете.

         [**http://www.microsoft.com/ru-ru/security/default.aspx**](http://www.microsoft.com/ru-ru/security/default.aspx)сайт Центра безопасности Майкрософт.

         [**http://www.saferunet.org/children/**](http://www.saferunet.org/children/)Центр безопасности Интернета в России.

         [**https://edu.tatar.ru/upload/images/files/909\_029 Orangepdf**](http://s-intern-osn-kuyby.edusite.ru/images/909_029-orange7.pdf)Безопасно и просто: родительский контроль. — Буклет

         Урок в 9–10 классах. Профилактика Интернет-зависимости «Будущее начинается сегодня» [**http://festival.1september.ru/articles/612789/**](https://docviewer.yandex.ru/r.xml?sk=0c02c71819619c959a25742d60574947&url=http%3A%2F%2Ffestival.1september.ru%2Farticles%2F612789%2F) Материал разработан для учащихся 9-11 классов, но может модифицироваться и для учащихся среднего звена школы.

         Материалы (буклет, презентация и текст) для бесед профилактике игровой и интернет-зависимости у детей и подростков на сайте Министерства образования и науки Республики Татарстан: [**http://mon.tatarstan.ru/prof\_internet\_zavisimosti.htm**](https://docviewer.yandex.ru/r.xml?sk=0c02c71819619c959a25742d60574947&url=http%3A%2F%2Fmon.tatarstan.ru%2Fprof_internet_zavisimosti.htm)

         [**http://www.nachalka.com/node/950**](http://www.nachalka.com/node/950)Видео «Развлечение и безопасность в Интернете»

         [**http://i-deti.org/**](http://i-deti.org/)портал «Безопасный инет для детей», ресурсы, рекомендации, комиксы

         [**http://сетевичок.рф/**](http://xn--b1afankxqj2c.xn--p1ai/)сайт для детей — обучение и онлайн-консультирование по вопросам кибербезопасности сетевой безопасности

         [**http://www.igra-internet.ru/**](http://www.igra-internet.ru/)— онлайн интернет-игра «Изучи Интернет – управляй им»

         [**http://www.safe-internet.ru/**](http://www.safe-internet.ru/)— сайт Ростелеком «Безопасность детей в Интернете, библиотека с материалами, памятками, рекомендациями по возрастам

ИНФОРМАЦИОННАЯ ПАМЯТКА ПО БЕЗОПАСНОСТИ В СЕТИ ДЛЯ ОБУЧАЮЩИХСЯ

18.03.2019

**ИНФОРМАЦИОННАЯ ПАМЯТКА ПО БЕЗОПАСНОСТИ В СЕТИ**

**ДЛЯ ОБУЧАЮЩИХСЯ**

С каждым годом молодежи в интернете становиться 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;

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.

**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 высшей 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 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 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.

**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:**

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 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.

**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 нефиатные деньги (не равны государственным валютам).

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

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 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:**

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 или виртуальное издевательство**

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; 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.

**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 саму 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:**

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 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:**

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**

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:**

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.

**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 установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.

**О портале**

[Сетевичок.рф](http://xn--b1afankxqj2c.xn--p1ai/)- 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