**Безопасный Интернет Детям**

**Защита детей от информации, причиняющей вред их здоровью и развитию.**

Законодательство:
• Федеральный закон РФ от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" [Подробнее...](http://www.rg.ru/2010/12/31/deti-inform-dok.html)
• Федеральный закон РФ от 21 июля 2011 г. N 252-ФЗ г. Москва "О внесении изменений в отдельные законодательные акты РФ в связи с принятием Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию"" [Подробнее...](http://www.rg.ru/2011/07/26/deti-dok.html)
• Письмо МИНОБРАУКИ России от 28.09.2011 г. №АП 1057/07 "О правилах подключения общеобразовательных учреждений к единой системе-контент фильтрации доступа к сети интернет [Подробнее...](https://edu.rtsoko.ru/rcoko/informatization/Shared%20Documents/pismo.pdf)
• Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющий вред здоровью и (или) развитию детей, а также не соответствующей задачам обучения [Подробнее...](https://edu.rtsoko.ru/rcoko/informatization/Shared%20Documents/metodrek.pdf)

Полезная информация.

В целях оказания психологической помощи и повышения осведомлённости детей и взрослых о способах решения сложных ситуаций, возникших при пользовании интернетом, в России начала свою работу

Линия помощи «Дети Онлайн» (<http://detionline.com/> ).
[Основы безопасности в Интернете](http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/etusivu.htm)

"Основы безопасности детей и молодежи в Интернете" — интерактивный курс по Интернет-безопасности.

На данном сайте представлены подготовленные совместно с Информационно-аналитическим ресурсом "Ваш личный Интернет" и Интернет-Университетом Информационных Технологий 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.

[Перейти на сайт "Основы безопасности в Интернете"](http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/etusivu.htm)

Группа в соц. сети ВКонтакте, созданная для просветительской работы по вопросам безопасности детей в Интернете - <https://vk.com/clubsecurechildreninSamara>

<http://fcprc.ru/projects/internet-safety/> - *Информационная безопасность*

[http://fcprc.ru/assets/files/projects/internet-safety/method-docs/Методическое пособие«Медиаграмотность».pdf](http://fcprc.ru/assets/files/projects/internet-safety/method-docs/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B5%20%D0%BF%D0%BE%D1%81%D0%BE%D0%B1%D0%B8%D0%B5) – *Центр защиты прав и интересов детей.*

[http://деткивсетке.рф/](http://xn--b1addbapnd5dgf.xn--p1ai/)  *- Всероссийская акция по безопасному поведению детей в сети Интернет «Сайты, которые выбирают дети».*

<https://vk.com/clubsecurechildreninsamara> - *Безопасность детей в Интернете*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«Безопасность в Интернете»

Во всероссийском открытом Уроке по кибербезопасности, подготовленном компанией «Лаборатория Касперского», который доступен на сайте урокцифры.рф. Задача Урока – напомнить о правилах защиты детей в Интернете. Лучшая защита от киберпреступлений – повышение уровня компьютерной грамотности. В доступной форме были озвучены практические советы и правила поведения в социальных сетях. Узнали, как создать надёжный пароль, как защититься от кражи аккаунтов, какие бывают уязвимости в умных устройствах, а также как отличить мошеннические сайты от настоящих.

Проводятся в рамках акции «Безопасность в интернете» Урок информационной безопасности, беседы, направленные на развитие ключевых компетенций цифровой экономики дошкольников и на формирование навыков их поведения в сети Интернет с целью обеспечения информационной безопасности.

Организаторами Урока выступают Министерство просвещения Российской Федерации, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, АНО «Цифровая экономика» и АО «Лаборатория Касперского» в партнёрстве с ключевыми российскими компаниями сферы информационных технологий. На Уроке узнают все о приватности аккаунтов: какие пароли заводить для аккаунтов, как часто их менять и какие данные о себе можно оставлять в открытом доступе.

Помимо этого, для самых юных интернет-пользователей –предусмотрен блок «Никогда не разговаривайте с неизвестными»: почему не стоит общаться с незнакомцами в интернете и какие меры безопасности предпринимать, чтобы избежать опасных контактов.

Школьникам постарше предстоит познакомиться с такой угрозой, как фишинг, и узнать, как от неё уберечься и что делать, если всё-таки попался на удочку мошенников.

Старшеклассники, помимо кибербуллинга, узнают, в чём опасность личных встреч с интернет-друзьями, которых никогда не видел в реальной жизни, и почему не стоит слишком активно делиться в сети информацией о своей личной жизни.



Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всём мире. Но с другой стороны, миллионы компьютеров получили доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. И ни когда-то, а прямо сейчас.

В связи с глобальным процессом активного формирования и использования информационных ресурсов особое значение приобретает информационная безопасность детей. Для преодоления негативного воздействия Интернета на детей необходимо их ознакомить с потенциальными опасностями в сети Интернет.

В связи с этим  был проведен урок, на котором рассматривались:

-  правила ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет;

– как критически относиться к сообщениям в СМИ (в т.ч. электронных), как отличить достоверные сведения от недостоверных, как избежать вредной и опасной для них информации;

-  как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет;

– как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывать в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

Обучающиеся просмотрели и обсудили видеоролик «Защита персональных данных детей», ознакомились с пособием  по медиа-информационной грамотности.

На родительском собрании родители были ознакомлены с пособием «Ребенок в медио-пространстве (право ребенка на безопасность)», какие угрозы Интернета встречаются наиболее часто, правила безопасности при работе в Интернете, как защититься от хамства и оскорблений в Интернете, как защититься от негативного использования персональной информации в социальных сетях, как защитить детей от Интернет-зависимости.

**Всероссийская Акция «Безопасность детей в Интернете»**

Цель акции: обеспечение информационной безопасности несовершеннолетних обучающихся путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникативной среде.

В в рамках Всероссийской Акции «Безопасность  детей в Интернете» были проведены следующие мероприятия:

- урок «Интернет-безопасность для детей»;

- конкурс рисунков «Интернет среди нас»;

- круглый стол «Основы безопасности в сети Интернет».

Обучающиеся узнали о видах информации способной причинить вред здоровью, а также о негативных последствиях распространения такой информации в сетях Интернет и мобильной (сотовой) связи, познакомились с правилами ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связью.

Презентация на тему: «Киберугрозы современности:  главные правила их распознавания и предотвращения» позволила рассмотреть проблемы информационной безопасности.

Демонстрация видео роликов с ситуациями по данной тематике предостерегали обучающихся от различных действий: «Профилактика формирования у учащихся интернет-зависимости и игровой зависимости», «Предупреждение совершения правонарушений с использованием информационно-телекоммукативных технологий».

Дискуссия, во время проведения круглого стола, позволила ответить на ряд вопросов: Для чего нужен интернет? Какие виды мошенничества существуют в сети интернет и как от них защититься? Виртуальный собеседник предлагает встретиться, как следует поступить? Как обезопасить себя при пользовании службами мгновенных сообщений?

На классные родительские собрания, подготовлены видеоуроки «Информация в интернете бывает грязной», «Интернет - зависимость».

**Материалы к Уроку Безопасности:**

[**Информационный буклет «Безопасный интернет детям»**](http://www.school4ndm.ru/doc/liflets_k_deti_06.pdf)

[**Памятка для родителей "Ребёнок в Медиа-пространстве"**](http://www.bgmocsha.ru/prilozhenie_k_pismu_85-03.pdf)

[**Видеоролик "Единый урок по безопасности в сети**](http://xn--b1afankxqj2c.xn--p1ai/edinyi-urok-po-bezopasnosti)[**http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/oppilaille.htm**](http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/oppilaille.htm)

 [**Фотоальбом "Урок безопасности"**](http://www.novopavlovka.edusite.ru/index.html)

[**Презентация «Киберугрозы современности:**](http://www.novopavlovka.edusite.ru/DswMedia/problemainformbezopasnosti.ppt) [**главные правила их распознавания и предотвращения»**](http://www.novopavlovka.edusite.ru/DswMedia/problemainformbezopasnosti.ppt)

 **Программно-аппаратное обеспечение, рекомендуемое для защиты от нежелательного контента в сети Интернет**

Интернет Контроль Сервер — интернет-шлюз со встроенным контент-фильтром [**Подробно...**](http://xserver.a-real.ru/)
Аппаратные шлюзыIdeco Hardware Appliance [**Подробно...**](http://ideco.ru/products/hardware.html)
Программно-аппаратный комплекс - UserGate Web Filter Appliance [**Подробно...**](http://www.school4ndm.ru/%28http%3A/usergate.ru/products/ug_hardware/ugwfa.php)
Контент-фильтр SkyDNS [**Подробно...**](https://www.skydns.ru/)
Интернет-фильтр для детей «Интернет Цензор» [**Подробно...**](http://www.icensor.ru/)
TimeBoss Родительский контроль [**Подробно...**](http://nicekit.ru/parental-control/time-boss.php)
KinderGate Родительский контроль [**Подробно...**](http://usergate.ru/products/kindergate_parental_control%20/)
Встроенная функция «Родительский контроль» Windows **Подробно...**
Детский интернет-браузер «Гогуль» [**Подробно...**](http://gogul.tv/)

**О БЕЗОПАСНОМ ИНТЕРНЕТЕ**

**Основные правила для дошкольников и школьников младших классов**

**Вы должны это знать:**

Всегда спрашивайте родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет. Прежде чем начать дружить с кем-то в Интернете, спросите у родителей как безопасно общаться. Никогда не рассказывайте о себе незнакомым людям. Где вы живете, в какой школе учитесь, номер телефона должны знать только ваши друзья и семья. Не отправляйте фотографии людям, которых вы не знаете. Не надо чтобы незнакомые люди видели фотографии Вас, Ваших друзей или Вашей семьи. Не встречайтесь без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду. Общаясь в Интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Вы можете нечаянно обидеть человека. Если вас кто-то расстроил или обидел, обязательно расскажите родителям.

**Основные правила для школьников средних классов**

**Вы должны это знать:**

При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям. Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан. Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы. Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом Если вас кто-то расстроил или обидел, расскажите все взрослому.

**Основные правила для родителей**

**Чтобы помочь учащимся, Вы должны это знать:**

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 открывайте файлы, присланные от неизвестных Вам людей. Эти файлы могут содержать вирусы или фото/видео с «агрессивным» содержанием. Помогите ребенку понять, что некоторые люди в Интернете могут говорить не правду 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 агрессивный контент в Интернете, так же расскажите куда в подобном случае они могут обратится. Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации.

**Основные правила для воспитателей, учителей и преподавателей**

**Чтобы помочь обучающимся, Вы должны это знать:**

Подготовьтесь. Изучите технику безопасности в Интернете, чтобы знать виды Интернет — угроз, уметь их распознать и предотвратить. Выясните, какими функциями обладают компьютеры подопечных, а так же какое программное обеспечение на них установлено. Прежде чем позволить ребенку работу за компьютером, расскажите ему как можно больше о виртуальном мире, его возможностях и опасностях. Не позволяйте детям самостоятельно исследовать Интернет-пространство, они могут столкнуться с агрессивным контентом. Выберите интересные ресурсы и предложите детям изучить их вместе. Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации контента, спама и антивирусы.

С более подробными советами по безопасности детей разного возраста можно ознакомиться на сайте Корпорации Microsoft   [**сайт Корпорации Microsoft**](http://www.microsoft.com/ru-ru/security/family-safety/childsafety-internet.aspx)

Материал использован с сайта [**www.kindergate.ru**](http://www.kindergate.ru/)

**Памятка для обучающихся об информационной безопасности детей**

НЕЛЬЗЯ

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

Открывать вложенные файлы электронной почты, когда не знаешь отправителя;

Грубить, придираться, оказывать давление — вести себя невежливо и агрессивно;

Не распоряжайся деньгами твоей семьи без разрешения старших – всегда спрашивай родителей;

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

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;

Всегда рассказывай взрослым о проблемах в сети – они всегда помогут;

Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

МОЖНО

Уважай других пользователей;

Пользуешься Интернет-источником – делай ссылку на него;

Открывай только те ссылки, в которых уверен;

Общаться за помощью взрослым – родители, опекуны и администрация сайтов всегда помогут;

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 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:

Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;

Постоянно устанавливай почти (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;

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

Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;

Ограничь физический доступ к компьютеру для посторонних лиц;

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

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:

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 закачки вируса на твое устройство;

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;

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 нефиатные 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 свою 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 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:

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 скринов;

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

О портале

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!