

Практическое занятие **«Безопасность нам нужна, безопасность нам важна»**

Цель: создать постер по теме о безопасном Интернете.

Задачи:

- повысить навыки работы в группах;
- уметь искать необходимую информацию в Интернете;
- анализировать, обрабатывать и систематизировать полученную информацию.

Форма проведения:

Практическое занятие.

Участники: актив школьной библиотеки, зав. библиотекой .

Оборудование: лист ватмана, рисунки, фломастеры, цветная бумага, ножницы, клей.

Место проведения: читальный зал школьной библиотеки.

Ход занятия

1. Организационный момент. Эмоциональная настройка.

-Цель нашего сегодняшнего занятия - разработать памятки, касающиеся безопасности в интернете, в виде постера. Продукт нашей работы должен помочь учащимся нашей школы в усвоении правил пользования Интернетом.

2. Мозговой штурм.

-Начиная любое дело, мы должны задать себе ряд вопросов: Что? Для кого? Где? Когда? Как? Посмотрите на темы, предложенные вам, и попробуйте ответить на эти вопросы.
-Что такое ПОСТЕР? Узнаем из Интернета.

Каждый участник выдвигает свою тему.

(Темы-задания: правила общения в интернете; защита от вирусов Интернета; обучение в Интернете (полезные сайты); сохранение здоровья при работе за компьютером. Польза – вред; можно-нельзя-осторожно)

Обсуждение результатов «мозгового штурма», определение основной концепции общего мероприятия.

(Группа в течение 2-3-х минут представляет свои наработки)

Подведение итогов мозгового штурма.

3. Сказка о золотых правилах безопасности в Интернет

В некотором царстве, Интернет - государстве жил-был Смайл-царевич- Тьютор-Королевич, который правил славным городом СоцОБРАЗом. И была у него невеста– прекрасная Смайл-царевна-Он-лайн-Королевна, день и ночь проводившая в виртуальных забавах. Сколько раз предупреждал её царевич об опасностях, подстерегающих в сети, но не слушалась его невеста. Не покладая рук трудился Смайл-царевич, возводя город СоцОБРАЗ, заботился об охране своих границ и обучая жителей города основам безопасности жизнедеятельности в Интернет-государстве. И не заметил он, как Интернет- паутина всё-таки затянула Смайл-царевну в свои коварные сети. Погоревал – да делать нечего: надо спасти невесту. Собрал он рать королевскую- СоцОбразову – дружину дистанционную и организовал "Регату" премудрую. Стали думать головы мудрые, как вызволить царевну из плена виртуального. И придумали они «Семь золотых правил безопасного поведения в Интернет», сложили их в котомку Смайл-царевичу, и отправился он невесту искать. Вышел на поисковую строку, кликнул по ссылкам поганым, а они тут как тут: порно-сообщества Змея-искусителя-Горыныча, стрелялки-убивалки Соловья-разбойника, товары заморские купцов шоповских, сети знакомств-зазывалок русалочьих... Как же найти-отыскать Смайл-царевну? Крепко задумался Тьютор-королевич, надел щит антивирусный,

взял в руки меч-кладенец кодовый, сел на коня богатырского и ступил в трясину непролазную. Долго бродил он, отбиваясь от реклам шоповских зазывающих и спамов завлекающих. И остановился на распутье игрища молодецкого трёхуровневого, стал читать надпись на камне, мохом заросшим: на первый уровень попадешь – времени счёт потеряешь, до второго уровня доберешься – от родных-близких отвернешься, а на третий пойдешь - имя своё забудешь. И понял Смайл-царевич, что здесь надо искать невесту. Взмахнул он своим мечом праведным и взломал код игрища страшного! Выскользнула из сетей разомкнувшихся Смайл - царевна, осенила себя паролем честным и бросилась в объятия своего суженого. Обнял он свою невесту горемычную и протянул котомочку волшебную со словами поучительными: «Вот тебе оберег от козней виртуальных, свято соблюдай наказания безопасные!» Всегда помни своё Интернет-королевское имя (E-mail, логин, пароли) и не кланяйся всем подряд (не регистрируйся везде без надобности)! Не поддавайся ярким реклам-указателям и не ходи тропками путанными на подозрительные сайты: утопнуть в трясине можно! Если пришло письмо о крупном выигрыше – это «Лохотрон-грамота»: просто так выиграть невозможно, а если хочешь зарабатывать пиастры, нужно участвовать в полезных обучающих проектах – в «Регате...», например!

Чтобы не забыть тропинку назад и вернуться вовремя, бери с собой Клубок волшебный (заводи себе будильник, садясь за компьютер)! Если хочешь дружить с другими царствами-государствами, изучай полезные социальные сервисы Web 2.0: они помогут тебе построить «Мой королевский мир», свой царский блог, форум для глашатаев важных – друзей званых. Не забывай обновлять антивирусную программу – иначе вирус Серый Волк съест весь твой компьютер! Не скачивай нелегальные программные продукты – иначе пираты потопят твой корабль в бурных волнах Интернет! Залилась сочувственными слезами дева красная, дала своему наречённому слово честное, что не будет пропадать в забавах виртуальных, а станет трудиться на благо народа города своего СоцОБРАЗа, сама начнёт обучаться и помогать будет людям заблудшему и погрязшему в трясине сетевой. И зажили они дружно и счастливо с мечтою расширить границы образовательные.

4. Подбор основных изречений для оформления постера, определение места расположения картинок, рисунков и правил.

МАТЕРИАЛ для работы по созданию постера

Это важно знать!

- ✓ Когда ты регистрируешься на сайтах, не указывай личную информацию (номер мобильного телефона, адрес места жительства и другие данные).
- ✓ Используй веб-камеру только при общении с друзьями. Проследи, чтобы посторонние люди не имели возможности видеть ваш разговор. Научись самостоятельно включать и выключать веб-камеру.
- ✓ Ты должен знать, что если ты публикуешь фото или видео в интернете — каждый может посмотреть их.
- ✓ Не публикуй фотографии, на которых изображены другие люди. Делай это только с их согласия.
- ✓ Публикуй только такую информацию, о публикации которой не пожалеешь.
- ✓ Нежелательные письма от незнакомых людей называются «Спам». Если ты получил такое письмо, не отвечай на него. Если ты ответишь на подобное письмо, отправитель будет знать, что ты пользуешься своим электронным почтовым ящиком, и будет продолжать посылать тебе спам.
- ✓ Если тебе пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
- ✓ Не добавляй незнакомых людей в свой контакт-лист в ICQ.
- ✓ Если тебе приходят письма с неприятным или оскорбляющим тебя содержанием, если кто-то ведет себя в твоём отношении неподобающим образом, сообщи об этом взрослым.

- ✓ Если человек, с которым ты познакомился в интернете, предлагает тебе встретиться в реальной жизни, то предупреди его, что придешь навстречу со взрослым. Если твой виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к твоей заботе о собственной безопасности.
- ✓ Если у тебя возникли вопросы или проблемы при работе в онлайн-среде, обязательно расскажи об этом кому-нибудь, кому ты доверяешь. Твои родители или другие взрослые могут помочь или дать хороший совет о том, что тебе делать. Любую проблему можно решить! Ты можешь обратиться на линию помощи «Дети онлайн» по телефону: 8–800–25–000–15 (по России звонок бесплатный) или по e-mail: helpline@detionline.com. Специалисты посоветуют тебе, как поступить.

Интернет-этикет

- ✓ Когда общаешься в онлайн, относись к другим людям так, как ты хотел бы, чтобы относились к тебе. Избегай сквернословия и не говори вещей, которые заставят кого-то плохо себя чувствовать.
- ✓ Научись "сетевому этикету", когда находишься в онлайн. Что считается делать и говорить хорошо, а что нет? Например, если ты печатаешь сообщение **ЗАГЛАВНЫМИ БУКВАМИ**, твой собеседник может подумать, что ты кричишь на него.
- ✓ Если кто-то говорит что-то грубое или что-то неприятное - не отвечай. Уйди из чата или форума незамедлительно.
- ✓ **«Подозрительные» сайты**
- ✓ Если веб-сайт выглядит подозрительно или имеет страницу с предупреждением для лиц моложе 18 лет, покинь его немедленно. Некоторые сайты не предназначены для детей.
- ✓ Не заходи на неприличные сайты и не делись ссылками на такие сайты. Если ты видишь, что что-то тебя беспокоит, обсуди это с родителями или с кем-то, кому ты доверяешь.
- ✓ Знай, как уйти с веб-сайта, если поиск по интернету приведет тебя на неприятный или неприличный веб-сайт. Нажми control-alt-delete, если сайт не позволяет тебе выйти, или выключи монитор компьютера и сообщи об этом взрослому.
- ✓ Проверь с родителями, настроен ли поисковик, которым ты пользуешься, так, чтобы он блокировал материалы, предназначенные для взрослых.
- ✓ Попроси родителей установить программное обеспечение для фильтрации информации из интернета, которое блокировало бы "неправильные" сайты.
- ✓ Попроси родителей помочь тебе найти безопасные и забавные сайты и сделай на них "закладки" для последующего использования.
- ✓ **Будь начеку!**
- ✓ Если ты видишь или знаешь, что твоего друга запугивают в онлайн, поддержи его и сообщи об этом взрослому. Ведь ты бы захотел, чтобы он сделал то же самое для тебя.
- ✓ Не посылай сообщения или изображения, которые могут повредить или огорчить кого-нибудь. Даже если не ты это начал, тебя будут считать участником круга запугивания.
- ✓ Всегда будь начеку, если кто-то, особенно незнакомец, хочет поговорить с тобой о взрослых отношениях. Помни, что в сети никогда нельзя быть уверенным в истинной сущности человека и его намерениях. Обращение к ребенку или подростку с сексуальными намерениями всегда является серьезным поводом для беспокойства. Ты должен рассказать об этом взрослому, которому доверяешь, для того чтобы вы могли сообщить о неприятной ситуации в правоохранительные органы.

5. Практическая работа.

Вырезание из цветной бумаги облачков, наклеивание рисунков, смайлов и правил на лист ватмана. Оформление названия постера.

6. Рефлексия

Итог нашего сегодняшнего занятия мы подведем с помощью вопросов-ответов.

1. Выберите высказывание, которое в данный момент наиболее вам ближе:

- Интернет ни капельки не сближает людей. Интернет - как скопление одиночества: вроде мы вместе, но каждый одинок, это иллюзия жизни, иллюзия дружбы, иллюзия любви...
- Интернет - это идеальное место для общения с людьми.
- Интернет - парадокс - он сближает людей, находящихся далеко, но отдаляет с теми, которые находится рядом.

2. В Интернете чаще всего Я...

- ищу необходимую учебную информацию
- общаюсь с друзьями
- отслеживаю музыкальные и киноновинки

3. Интернет нам –

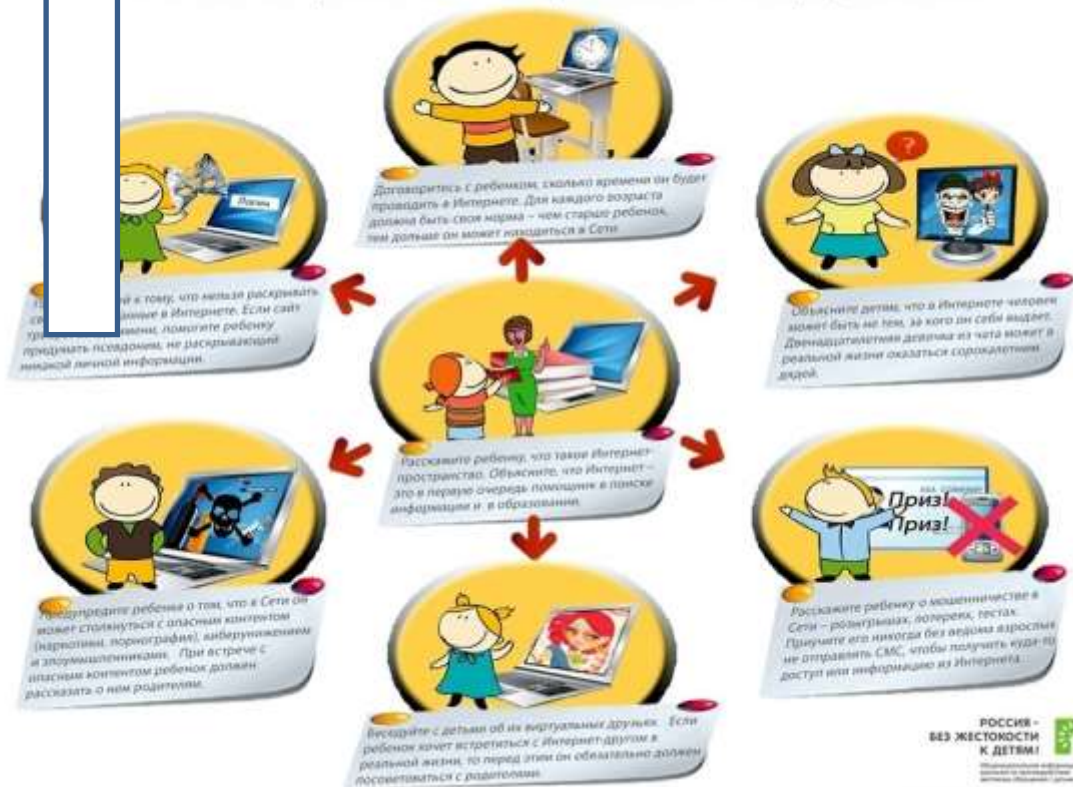
- скорее друг
- скорее враг

Вывод: хочется верить, что каждый из вас знает «плюсы» и «минусы» Интернета. Мы выбираем реальную жизнь! Мы за Безопасный Интернет!

7. **Размещение постера на стенде школы.**



Безопасность ребенка в Интернете. Памятка родителям.



▶ 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, придираться, 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



ПАМЯТКА

СОБЛЮДАЙТЕ ПРАВИЛА ПРЕДОСТОРОЖНОСТИ ПРИ РАБОТЕ В ИНТЕРНЕТЕ

- Нельзя сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей).
- Используй выдуманное имя в переписке и переговорах.
- Нельзя открывать вложенные файлы электронной почты, если не знаешь отправителя.
- Не нажимай неизвестные ссылки.
- Нельзя рассылать спам и информационную грязь.
- Не отправляй SMS на незнакомый номер.
- Не общайся с незнакомыми людьми из интернета вживую. Встреча с интернет-

знакомыми в реальной жизни бывает опасной:
за псевдонимом может скрываться преступник.

- Остерегайся заманчивых предложений.

Stream unlimited images \$2.90/month - Click here!





ВАЖНО ЗНАТЬ

- | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none">❖ Придумай сложные логин и пароль, не говори их никому.❖ Уважай другого пользователя. Общайся в интернете, будь дружелюбен с другими.❖ Чтобы не сталкиваться с неприятной информацией в Интернете, установи на свой браузер фильтр. | <ul style="list-style-type: none">❖ Используй веб-камеру только при общении с друзьями. Проследи, чтобы посторонние люди не имели возможности видеть ваш разговор. Научись самостоятельно включать и выключать веб-камеру.❖ Ты должен знать, что если ты публикуешь фото или видео в интернете — каждый может |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

❖ Не скачивайте и не открывайте неизвестный тебе или присланные незнакомцами файлы из Интернета .

❖ Открывай только те ссылки, в которых уверен.

❖ Пользуешься интернет-источником - делай ссылку на него.

❖ Установи антивирус.

❖ Используйте фильтры электронной почты для блокирование спама нежелательных сообщений

посмотреть их.

❖ Познакомился в сети и хочешь встретиться - советуйся со взрослым, которому доверяешь.

❖ Не публикуй фотографии, на которых изображены другие люди. Делай это только с их согласия.

❖ Публикуй только такую информацию, о публикации которой не пожалеешь

❖ Не заходи на неприличные сайты.

❖ Ограничь время пребывания в сети.

❖ Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.

Плюсы интернета

- оперативность получения любой информации
- общение
- участие в международных конкурсах
- возможность дополнительного образования
- обеспечение досуга
- формирование информационной компетентности

Минусы интернета

- беспорядочная недостоверная информация
- ухудшения здоровья
- вредная информация
- психологическое давление
- потеря рабочего времени

Безопасный Интернет

Интернет может быть прекрасным и полезным средством для обучения, отдыха, или общения с друзьями. Но как и реальный мир, Сеть тоже может быть опасна: в ней появились своя преступность, хулиганство, вредительство и прочие малоприятные явления.

Для того чтобы защитить себя от всего этого необходимо соблюдать правила безопасности в Интернете.



БЕЗОПАСНЫЙ ИНТЕРНЕ

- Установите правила работы в интернет
- Научите детей осторожности.
- Убедите их, что правильное и неправильное одинаково в интернете и в реальности
- Научите детей доверять интуиции.
- Скажите им, что не все, содержащееся в интернете, - правда.
- Контролируйте деятельность детей в интернете.

Безопасный интернета для детей

*Ни за что не раскрывай свои личные данные.

*Если ты вдруг хочешь встретиться с «интернет другом» в реальной жизни обязательно сообщи родителям ;

*Старайся посещать только те страницы интернета, которые тебе советуют родители;



Зачем нужен злоумышленникам доступ

к компьютеру пользователя

Зря обычный пользователь думает, что его компьютер никому не нужен. Это раньше хакеры часто писали вирусы просто ради интереса, сейчас же это делается почти всегда с коммерческой выгодой. Лет 20 тому назад злоумышленник получал удовольствие от того, что мог просто отформатировать жесткий диск. Или сделать так, что при включении компьютера вместо стандартного рабочего стола появятся какие-либо прикольные картинки. Сейчас же они делают все возможное, чтобы владелец ПК как можно дольше не знал о том, что его устройство заражено и втайне от него выполняет дополнительные функции. Для чего все это делается? Кроме того, о чем было сказано выше, хакеры стараются получить доступ к вашим электронным почтам, кошелькам, аккаунтам в социальных сетях, форумах. Случается так, например, что вы ложитесь спать с 20 000 рублей на электронном кошельке, а утром получаете СМС-сообщение о том, что денег на нем уже нет. А с почты все ваши контакты, да и не только, получают спам-письма, а то еще и трояны. Хакеры могут объединить множество зараженных компьютеров в единую мощную сеть, провести DDoS-атаку даже на мощные государственные серверы. Из самого простого, но также приносящего деньги: заблокируют работу операционной системы и потребуют деньги за устранение проблемы. И, кстати, деньги возьмут, но компьютер оставят заблокированным. Так что безопасность в сети интернет должна стать основой вашей работы в ней.

Начальная защита компьютера

Несмотря на то что Windows имеет встроенный фаерволл, рекомендуется установить более надежный, так как имеющийся - далеко не самый лучший. Выбирайте платный или бесплатный, исходя из их рейтингов. Следующий шаг – установка антишпионского и антивирусного ПО. Нужно сразу же его обновить и настроить на автоматическое обновление. Также оно должно запускаться автоматически, вместе с ОС. И постоянно, в фоновом режиме, работать. И обязательно проверяйте любую устанавливаемую программу. Как только появляются обновления для Internet Explorer и других используемых вами браузеров, тут же скачивайте их и устанавливаете. Отключайте все неиспользуемые службы на своем

устройстве, это уменьшит шансы для хакеров получить к нему доступ.
Дальнейшие уроки безопасности

Как злоумышленники проникают в компьютер?

Подробная информация Для того чтобы взломать защиту ПК, даже если она есть, хакеры применяют целый ряд способов, и пользователи зря думают, что, просто установив антивирус, они избавились от опасности, например, подцепить вредоносную программу. Поэтому, прежде чем искать информацию о том, как правильно соблюдать безопасность в сети интернет, нужно понять, а откуда берутся вирусы и трояны. Сейчас мы перечислим основные пути их проникновения и методы воровства различной информации. Первый метод называется социальной инженерией. Благодаря различным психологическим приемам, уловкам и доверчивости пользователей хакеры присылают вам вполне безобидный файл или письмо, а вы сами и запускаете троянчик в нем. Или же по просьбе якобы администрации сервиса выдаете все свои пароли и явки. Второй метод – предлагается разное бесплатное программное обеспечение, пиратские диски, где спрятано множество вирусов, троянов и тому подобной гадости. В ПО, в том числе и из самых надежных проверенных источников, постоянно появляются дыры в безопасности. Это относится и к операционным системам. Вот злоумышленники внимательно и следят за такими моментами, стараются их не упустить, а использовать в собственных целях. Зайдете на какую-нибудь страничку сто раз проверенного сайта и - раз - ваше устройство заражено. Четвертый способ получил особое распространение в последнее время. Это фишинг, когда создаются поддельные сайты. И вы вместо странички своего банка оказываетесь на его поддельной копии. О том, что может быть дальше, говорить не будем, сами догадаетесь.

Дальнейшие уроки безопасности

Теперь немного информации о том, как обеспечить безопасность работы в сети интернет. Выполнив указанное в предыдущем разделе, продолжайте не забывать о ежедневной защите. Удаляйте сразу же все письма подозрительного содержания, не

вздумайте открывать файлы из неизвестных источников.
Игнорируйте все предложения легкого заработка, никому не
высылайте свои пароли, не переходите по подозрительным
ссылкам. Используйте только сложные пароли, состоящие из
сложного набора цифр, букв и символов. Для каждого случая
назначайте свой, оригинальный

СОВЕТЫ ПО БЕЗОПАСНОЙ РАБОТЕ В ИНТЕРНЕТЕ

СЛОЖНЫЙ ПАРОЛЬ

Если ты регистрируешься на сайте, в социальной сети или в электронной почте, придумай сложный пароль, состоящий из цифр, больших и маленьких букв и знаков. Чем сложнее пароль, тем сложнее взломать твой аккаунт. Помни, что твой пароль можешь знать только ты.



СОВЕТ ВЗРОСЛЫХ

Всегда спрашивай взрослых о непонятных вещах, которые ты встречаешь в Интернете: ты не знаешь, какой пункт выбрать, на какую кнопку нажать, как закрыть программу или окно. Они расскажут тебе, как поступить - что можно делать, а что нет.



ЛИЧНАЯ ИНФОРМАЦИЯ

Никогда не рассказывай о себе незнакомым людям в Интернете: где ты живешь и учишься, не сообщай свой номер телефона. Не говори никому о том, где работают твои родители и номера их телефонов. Эта информация может быть использована во вред тебе и твоим родителям.



НЕ ОТПРАВЛЯЙ СМС

Если в Интернете ты решил скачать картинку, игру или мелодию, а тебя просят отправить смс - не делай этого! Смс на короткие номера могут стоить несколько сотен рублей. Ты потеряешь деньги, которые мог бы потратить на что-то другое.



НЕ ЗАБУДЬ ВЫЙТИ

При использовании чужих компьютеров или мобильных устройств, не забывай выходить из своего ящика электронной почты или профилей в социальных сетях. Иначе, следующий пользователь этого устройства сможет просмотреть твою личную информацию.



ОСТОРОЖНО, НЕЗНАКОМЕЦ!

Никогда не отвечай на сообщения от незнакомцев в Интернете и не отправляй им смс. Если незнакомый человек предлагает встретиться или пишет тебе оскорбительные сообщения - сразу скажи об этом взрослым! Не все люди являются теми, за кого себя выдают в Интернете!



БЕСПЛАТНЫЙ Wi-Fi

При выходе в Интернет через общественную Wi-Fi сеть, не совершай никаких покупок и оплаты, не проверяй личную электронную почту и не передавай конфиденциальную информацию. Злоумышленники могут похитить ваши пароли и данные.



ЗАЩИТИ КОМПЬЮТЕР

Попроси родителей или сам установи систему фильтрации SkyDNS на сайте www.skydns.ru. Она защитит тебя от потери денег и кражи паролей, а также будет блокировать большую часть рекламы, ускоряя загрузку страниц в Интернете.



Защитите своих детей от неблагоприятного воздействия интернета!!!

Памятка по безопасному использованию сети Интернет:

1. Родители должны знать интересы и цели детей, которые используют сеть Интернет
2. Рекомендуется допускать использование сети Интернет детьми в присутствии взрослых.
3. Необходимо исключить доступ детей к ресурсам сети Интернет, содержание которых противоречит законодательству Российской Федерации
4. Родители должны контролировать использование информации несовершеннолетними
5. Для ограничения доступа детей к «вредным» материалам можно установить на ПК антивирусную программу (например, программу «Касперский Интернет секьюрити»)

