МЕДИАБЕЗОПАСНОСТЬ

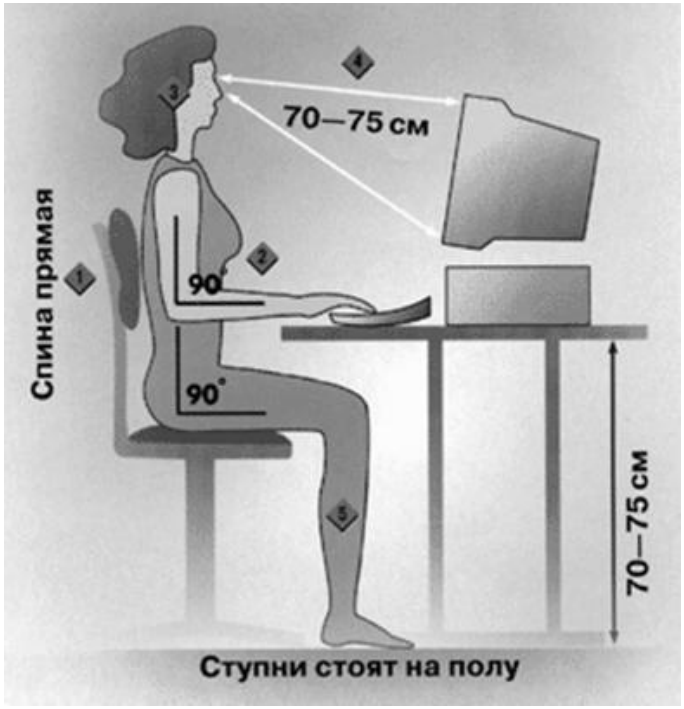
Уроки школьникам

Яркий и красочный реальный мир. Он таит множество новых открытий. Но в нем и много опасностей - электричество, огонь, неадекватные люди, транспорт.

В наше время компьютеры глубоко проникли во все сферы жизни. Трудно представить себе мир без этой умной машины. Дети родились и растут в мире, где компьютеры такая же привычная вещь как телевизор, лампочка, автомобиль.

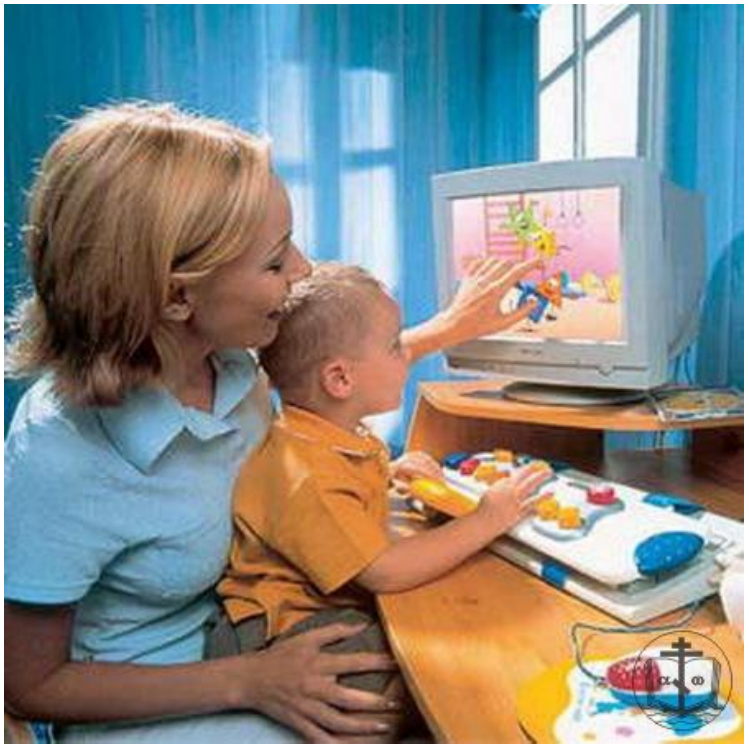
Родители приобретают ребенку компьютер и на них ложится ответственность за тот вред или пользу, которые принесет он.

ПРАВИЛЬНАЯ ПОСАДКА



Важно не только научить детей правильной посадке, выполнять упражнения для глаз, объяснить электробезопасность, пожарную безопасность, но и помочь понять существование невидимой, виртуальной опасности.

РОДИТЕЛИ И ДЕТИ

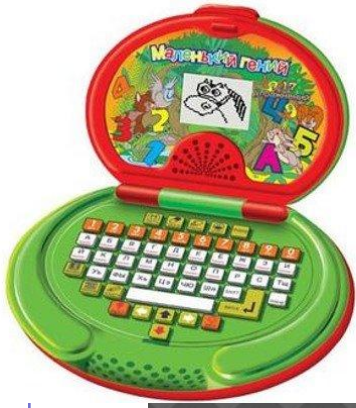


Только 11% участников опроса учат своих детей базовым правилам онлайн-безопасности и столько же ограничивают время пребывания детей в Интернете.

Ведущий детский психолог Центра психологии "Я+Семья" Валерия КУКСА:

«Многие родители допускают воспитательную ошибку, считая, что достаточно научить ребенка правилам безопасного поведения в реальной жизни - и в Сети ему тоже ничего не грозит.

Здесь кроется главный подвох - ведь в онлайне дети ощущают себя по-другому - там властвует свобода, анонимность и вседозволенность. Именно поэтому необходимой частью современного воспитания является обязательное обучение правилам онлайн-безопасности.».



КОМПЬЮТЕР В СЕТИ

По рекомендации экспертов, дети должны выучить 5 основных правил онлайн-поведения:

5 ОСНОВНЫХ ПРАВИЛ

1. Осознать важность защиты своей и чужой личной информации и не распространять конфиденциальную информацию в сети.

5 ОСНОВНЫХ ПРАВИЛ

2. Вести себя в Интернете так же, как в реальной жизни, в частности, следовать этическим нормам и правилам.

3. Не слишком доверять незнакомым людям в Сети, знать, что они могут выдавать себя за других.

5 ОСНОВНЫХ ПРАВИЛ

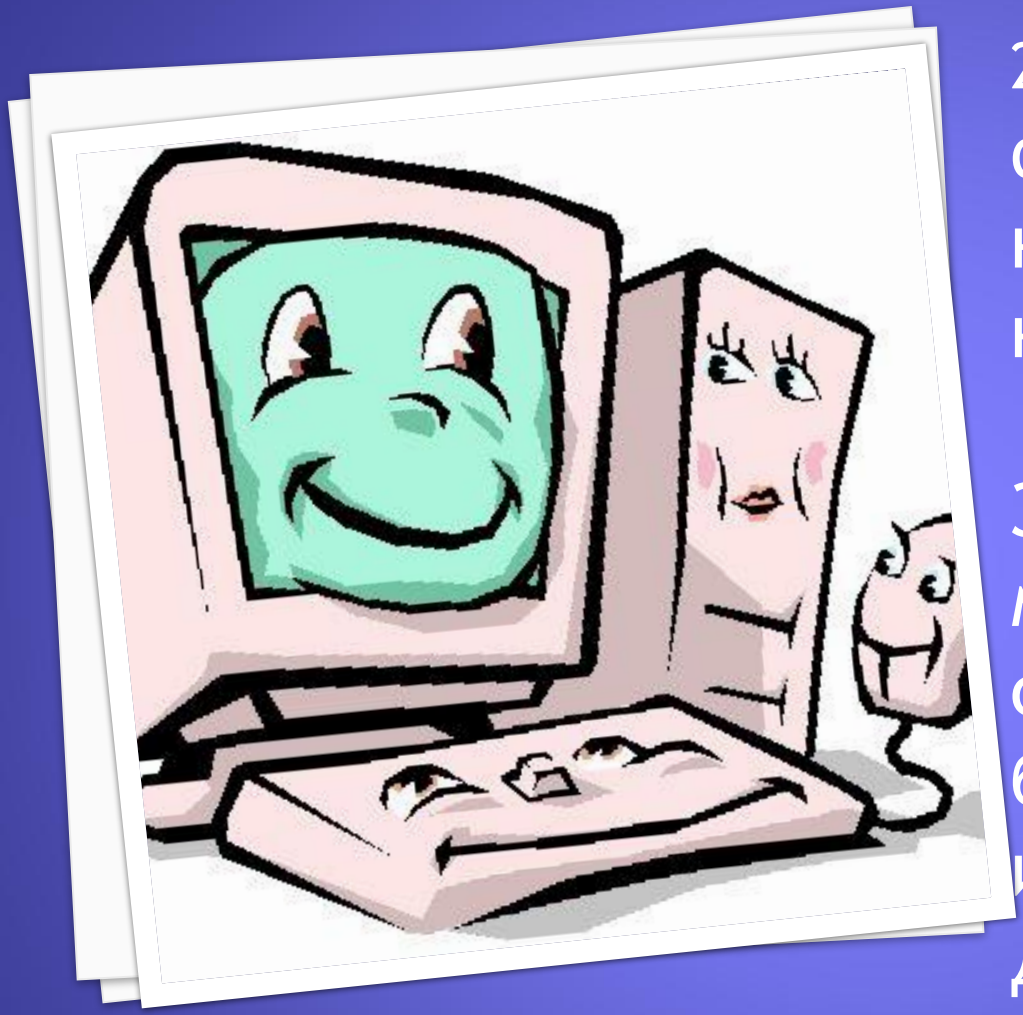
4. Помнить, что виртуальные покупки стоят реальных денег.

5. Обращаться за советом к родителям в любой неоднозначной или непонятной ситуации.

7 СОВЕТОВ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ДЛЯ УЧАЩИХСЯ

1. Соблюдайте основные меры компьютерной безопасности. Перед тем, как отправиться в путешествие по Интернету, необходимо выполнить три важных действия для усиления компьютерной защиты.

- Активизация брандмауэра
- Обновление антивирусных программ
- Обновление программного обеспечения



2. Не открывайте файлы, полученные от неизвестных корреспондентов

Электронная почта и мгновенные сообщения позволяют быстро обменяться информацией с друзьями, родственниками и одноклассниками.

Но если не проявить необходимой осторожности, электронная почта и мгновенные сообщения могут распространить вирусы и черви. Основная масса вредоносных программ попадает в компьютер через электронную почту теми, кто нечаянно попытался открыть зараженный файл. Не дайте себя одурачить! Ни в коем случае нельзя открывать файл, вложенный в письмо электронной почты или мгновенное сообщение, если его отправитель неизвестен и вы не ожидаете получения файла.

3. Бороться со спамом и сетевыми мошенниками Нужно также освоить способы борьбы со спамом. Мошенничество представляет собой еще одну угрозу конфиденциальности ваших данных. У вас могут украсть номер кредитной карты, пароли, учетную информацию или другие личные данные.

4. Защита от программ-шпионов.
Получить эту вредоносную программу можно при скачивании музыки или программ обмена файлами; загрузки бесплатных игр с подозрительных сайтов или других программ.

5. Принимайте необходимые меры предосторожности, пользуясь беспроводной связью.

6. Пароль защищает ваш компьютер и блокирует возможность его использования
Пароли являются первой линией защиты от злоумышленников, шутников или беспечного соседа по комнате.

7. Делайте резервные копии результатов работы (а также игр и других развлекательных программ)
Образ студента, оставшегося без своей курсовой работы из-за того, что он забыл сделать резервную копию, стал уже почти штампом. Тем не менее многие до сих пор не находят времени на копирование.

ПЯТЬ СОВЕТОВ ПО БЕЗОПАСНОСТИ ПРИ РАБОТЕ НА КОМПЬЮТЕРЕ ОБЩЕГО ПОЛЬЗОВАНИЯ

1. НЕ СОХРАНЯЙТЕ СВОИ УЧЕТНЫЕ ДАННЫЕ ДЛЯ ВХОДА В СИСТЕМУ.

После завершения работы на веб-узле обязательно пользуйтесь функцией выхода из системы. Просто закрыть окно обозревателя или ввести другой адрес недостаточно.

Многие программы (особенно программы для обмена мгновенными сообщениями) имеют функцию автоматического входа в систему, сохраняющую имя пользователя и пароль. Отключите эту функцию, чтобы никто, кроме вас, не смог войти в систему.

2. НЕ ОСТАВЛЯЙТЕ БЕЗ ПРИСМОТРА КОМПЬЮТЕР С ВАЖНЫМИ СВЕДЕНИЯМИ НА ЭКРАНЕ.

Закончив работу на компьютере общего пользования, воспользуйтесь функцией выхода из системы во всех программах и закройте все окна, в которых могут отображаться конфиденциальные данные.

3. ЗАМЕТАЙТЕ СВОИ СЛЕДЫ

В таких веб-обозревателях, как Internet Explorer, сохраняются сведения о паролях пользователя и всех посещенных им веб-страницах, даже если он закрыл их и вышел из системы. Отключайте функцию сохранения паролей

- Перед открытием веб-страниц в обозревателе Internet Explorer отключите функцию сохранения паролей.
- Завершив работу на компьютере общего пользования, удалите все временные файлы и очистите журнал пользования Интернетом.

4. ОПАСАЙТЕСЬ ПОДГЛЯДЫВАНИЯ ЧЕРЕЗ ПЛЕЧО.

Работая на компьютере общего пользования, следите за мошенниками, которые собирают информацию о вас, подглядывая через плечо или подсматривая, как вы вводите секретные пароли.

5. НЕ ВВОДИТЕ ВАЖНЫЕ СВЕДЕНИЯ НА КОМПЬЮТЕРЕ ОБЩЕГО ПОЛЬЗОВАНИЯ.

Эти меры обеспечат некоторую защиту от обычных хакеров, которые могут воспользоваться компьютером после вас.

Однако профессиональный мошенник может установить на компьютере общего пользования специализированное программное обеспечение, которое будет записывать каждое нажатие клавиши, а затем отправлять ему эту информацию по электронной почте.

5. НЕ ВВОДИТЕ ВАЖНЫЕ СВЕДЕНИЯ НА КОМПЬЮТЕРЕ ОБЩЕГО ПОЛЬЗОВАНИЯ.

В таком случае мошенники все еще имеют доступ к информации, даже если вы не сохранили ее или стерли следы.

Чтобы действительно быть в безопасности, не вводите номер кредитной карты, а также любые другие финансовые или иные важные сведения на компьютере общего пользования.

ВНИМАНИЕ!

Необходимо обращаться за советом к родителям или учителю в любой неоднозначной или непонятной ситуации.

ИСТОЧНИКИ ИНФОРМАЦИИ

- http://znz11.ucoz.ru/news/komp_juterni_geniji/2011-04-10-7
- http://missia.od.ua/articles/in-form/681-rebenok-i-kompjuternye-igry.html
- http://infomed.by/article/207
- http://www.microsoft.com/rus/protect/athome/privacy/publiccomputer.mspx
- http://www.123rf.com/stock-photo/blonde_girl_children.html

ТАКЖЕ МОЖНО ИСПОЛЬЗОВАТЬ

- Ролик «Интернет опасен для детей»

http://www.youtube.com/watch?v=B5gbk6TVbWs&feature=related

- Ролик «Правила безопасного поведения детей в интернете»

http://www.youtube.com/watch?v=-JhpUVtNEHk&feature=related

- http://zavertjaev.ucoz.ru/news/bezopasnost_detej_v_seti_internet_pravila_povedenija_i_roditelskij_kontrol/2010-11-02-4

ТАКЖЕ МОЖНО ИСПОЛЬЗОВАТЬ

http://genpas.net/view_post.php?id=63

http://genpas.net/view_post.php?id=77

http://www.adme.ru/generalnyj-direktor/pravila-bezopasnosti-v-internete-oni-71402

МАОУ СОШ № 50 ГОРОДА ТОМСКА

Презентацию по материалам из Интернета подготовила

Гришкова Татьяна Павловна