



Безопасность в Интернете



Выполнил: Шпилько
Елизавета,
ученик 8 класса «А»
МБНОУ «Гимназия №44»
г. Новокузнецк

"Презентация подготовлена для конкурса
"Интернешка" <http://interneshka.org/> .



Интернет -
является прекрасным
источником для новых
знаний, помогает в
учебе, занимает
досуг.

Но в то же время, Сеть таит
в себе много опасностей.
Обязательно нужно знать,
что могут возникать
различные неприятные
ситуации и то, как из них
лучшим образом выходить.
Помните, что безопасность
в Интернете, на зависит от
вас.



Как распознать интернет и игровую зависимость

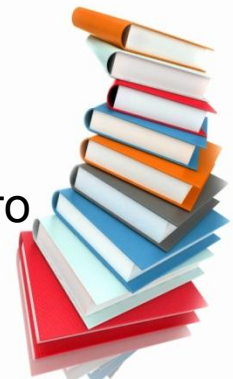
Сегодня в России все более актуальны проблемы так называемой «интернет-зависимости». Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки, в случае, если у сотрудников появляется патологическое влечение к пребыванию онлайн.

Согласно исследованиям Кимберли Янг, предвестниками интернет-зависимости являются:

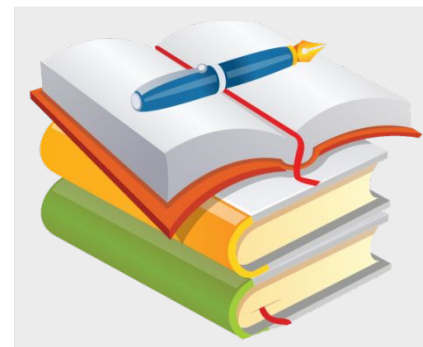
- навязчивое стремление постоянно проверять электронную почту;
- предвкушение следующего сеанса онлайн;
- увеличение времени, проводимого онлайн;
- увеличение количества денег, расходуемых онлайн.



Если Вы считаете, что Ваши близкие страдают от чрезмерной увлеченности компьютером, это наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой.



Как научиться
быть
осторожным
в Сети и не стать
жертвой
интернет -
мошенников



Кибермошенничество
— ОДИН ИЗ ВИДОВ
киберпреступления, целью
которого является обман
пользователей:

*незаконное получение
доступа либо хищение
личной информации (номера
банковских счетов,
паспортные данные, коды,
пароли и др.), с целью
причинить материальный
или иной ущерб.*



Предупреждение кибермошенничества:

1. Узнайте о самых распространенных методах мошенничества;

2. Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных;

3. Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если Вы уже совершаете онлайн-покупки самостоятельно, то соблюдайте простые правила безопасности.



Простые правила безопасности при онлайн-покупках

1. Ознакомьтесь с отзывами покупателей.
2. Проверьте реквизиты и название юридического лица – владельца магазина.
3. Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис *WhoIs*).

4. Поинтересуйтесь, выдает ли магазин кассовый чек.
5. Сравните цены в разных интернет-магазинах.
6. Позвоните в справочную магазина.
7. Обратите внимание на правила интернет-магазина.
8. Выясните, сколько точно вам придется заплатить.



Как научиться не загружать на компьютер вредоносные программы

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным.

Предупреждение столкновения с вредоносными программами:

- Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных..

- Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.

Периодически старайтесь полностью проверять свои домашние компьютеры.

- Делайте резервную копию важных данных.

- Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

Семейное соглашение о работе в Интернет

Если в вашей семье хотят посещать Интернет, вам следует выработать вместе со всеми соглашение по использованию Интернет. Не забудьте четко сформулировать **ответы на следующие вопросы:**

- Сколько времени каждый может проводить в Интернет;
- Как защитить личные данные;
- Как следить за безопасностью;
- Как вести себя вежливо;
- Как пользоваться чатами, группами новостей и службами мгновенных сообщений.

Не забудьте, что формально составленное соглашение не будет выполняться! Регулярно, по мере необходимости, вносите изменения в данное соглашение. Не забывайте, что вы должны проверять выполнение соглашения

со всеми членами семьи



Базовые правила безопасного Интернета

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.
- ✓ Встреча с Интернет-знакомыми в реальной жизни, бывает опасной: за псевдонимом может скрываться преступник.



Базовые правила безопасного Интернета для детей

ОСТОРОЖНО

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



Базовые правила безопасного Интернета

МОЖНО

- ✓ Используй «ник» 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



ССЫЛКИ:

- http://evlevavg.3dn.ru/publ/informacionnaja_bezopasnost/roditeljam/kibermoshennichestvo/3-1-0-17
- <http://pptcloud.ru/informatike/6202-bezopasnyy-internet.html>
- <http://baby-consultant.ru/2012/10/bezopasnost-detey-v-internete.html>



Спасибо за
внимание!!!

