# Творческая работа на тему: «Безопасность в интернете»


Работу выполнила ученица 10 класса
МБОУ СОШ №1 Базарный Карабулак
Романова Ангелина.

*Безопасность в интернете – очень важная проблема нынешнего времени. И касается она всех, от детей до пенсионеров. Она становится все актуальнее в связи с массовым приходом в интернет пользователей, почти, а то и совсем, не подготовленных к угрозам, их поджидающим. Поэтому данная статья и буде посвящена такому вопросу, как безопасность в сети интернет. Ведь страдает не один пользователь, а и многие другие, объединенные в одну глобальную структуру.*

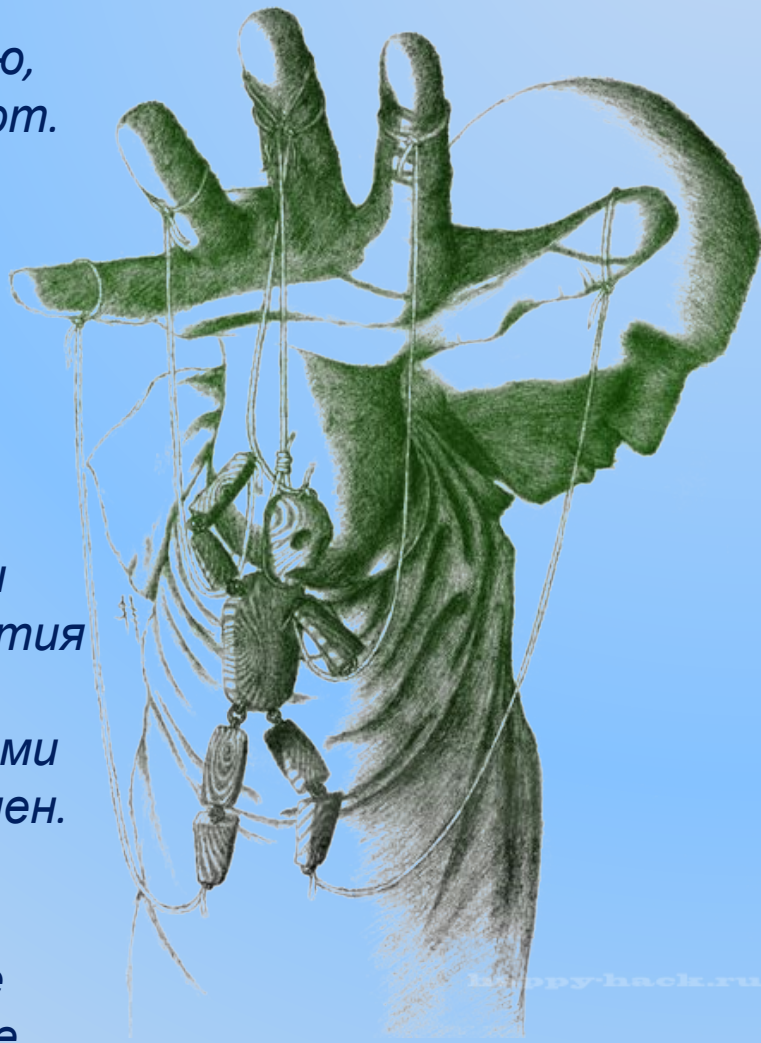
# Опасности, подстерегающие нас в сети.

*Если сказать кратко, то существуют две основные возможности того, как может ваш компьютер стать жертвой. Первое – вы сами, странствуя по различным сайтам или устанавливая программное обеспечение с непроверенных источников, а иногда и с проверенных, заражаете свой компьютер. Второе – возможна также ситуация, когда злоумышленники преднамеренно, с помощью, например, троянских программ или вирусов, делают ваше устройство источником опасности.*

*В результате всего этого компьютер, иногда даже тайно от своего владельца, начинает выполнять рассылку спама, участвует в DDoS-атаках на различные сайты, крадет пароли. Бывает и так, что провайдер вынужден принудительно отключить такое устройство от глобальной сети. Получается, что если пользователь не осведомлен о том, что представляют собой основы безопасности в сети интернет, придется ему тяжело.*

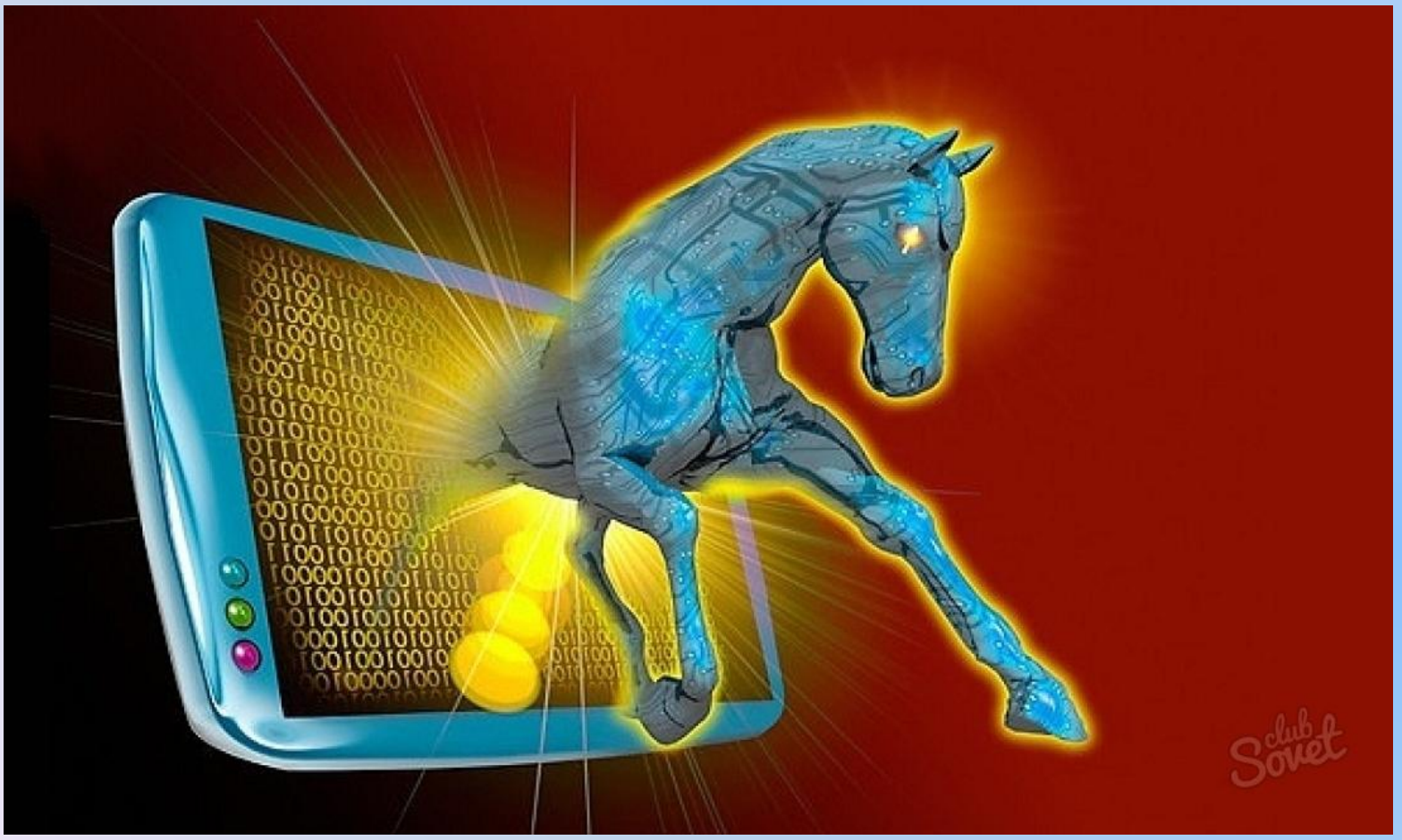
# Источники опасностей.

*Подхватить вредоносную программу, к сожалению, значительно легче, чем многие себе представляют. Для взлома компьютеров пользователей сети и кражи важных данных, например, паролей электронных платёжных систем, применяются следующие методы:*



*1) социальная инженерия - метод основанный на психологических приёмах, который существует и эффективно используется с самого начала развития компьютерных сетей и которому не грозит исчезновение. Список уловок, придуманных хакерами в расчёте на доверчивость пользователей, огромен. Вам могут прислать письмо от имени администрации сервиса с просьбой выслать им якобы утерянный пароль или письмо, содержащее безобидный, якобы файл, в который на самом деле спрятан троян, в расчёте на то, что из любопытства вы сами его откроете и запустите вредоносную программу.*

*2) трояны и вирусы могут быть спрятаны в различных бесплатных, доступных для скачивания из интернета программах, которых огромное множество или на пиратских дисках, имеющихся в свободной продаже.*



*3) взлом вашего компьютера может быть произведён через дыры в распространённом программном обеспечении, которых, к сожалению, довольно много и всё новые уязвимости появляются регулярно. Хакеры, в отличие от большинства пользователей, не следящих за уязвимостями и часто не скачивающих устраняющие их патчи, за обнаружением новых уязвимостей следят и используют их в своих целях. Для того, чтобы компьютер, имеющий уязвимости, был заражён, достаточно, например, всего лишь зайти на определённую страничку (ссылку на эту страничку хакер может прислать в письме, оставить на форуме и т. д.).*

*4) в последнее время получил распространение фишинг - создание поддельных сайтов, копирующих сайты известных фирм, сервисов, банков и т. д. Заманить вас на такой поддельный сайт могут разными способами, а цель - украсть данные вашего аккаунта (т. е. логин и пароль), которые вы обычно вводите на странице настоящего сайта.*

# Начальная защита компьютера пользователя.

В идеале, купив ПК, пользователь должен выполнить целый ряд операций, прежде чем броситься бороздить бесконечные просторы сети. Сейчас мы представим некоторые самые первые уроки безопасности в интернете.

- *Несмотря на то что Windows имеет встроенный файрволл, 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.*

- *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.*
- *Выходя в сеть из мест общего пользования, будьте аккуратны и осторожны. Это же касается и использования прокси-серверов. Желательно не проводить никаких банковских и других подобных операций из таких мест.*
- *Предпочитайте работать с платежными системами через их собственные приложения, а не через сайт. Это намного безопаснее.*
- *Нежелательно посещать сайты для взрослых или подобные им ресурсы. Велика вероятность подхватить троян.*
- *Следите за интернет-траффиком, даже если он безлимитный. Если он без особой причины значительно увеличился, это может быть признаком активности вируса. Если будете соблюдать эти минимальны правила безопасности в сети интернет, то избежите многих проблем. Это, конечно, далеко не все. Опасностей столько, что нельзя о них забывать ни на минуту.*

# Дети и интернет.

*В связи с развитием современных технологий все большее количество детей получает возможность выхода в интернет. И если раньше они в основном играли в игры, даже не выходя в сеть, то теперь все совсем по-другому, да вы и сами все знаете. Поэтому появилась новая задача – обеспечить безопасность детей в сети интернет. Это достаточно сложно, так как Всемирная паутина изначально развивается полностью бесконтрольно.*

*В ней есть очень много информации, доступа к которой у детей быть не должно. Ко всему прочему, их нужно научить, как не "наловить" вирусов и троянов. Кто же им поможет с этим, как не взрослые. К тому же очень важна и информационная безопасность в сети интернет, так как дети – совсем неискушенные пользователи. Они легко могут попасться на удочку опытного мошенника или злоумышленника.*

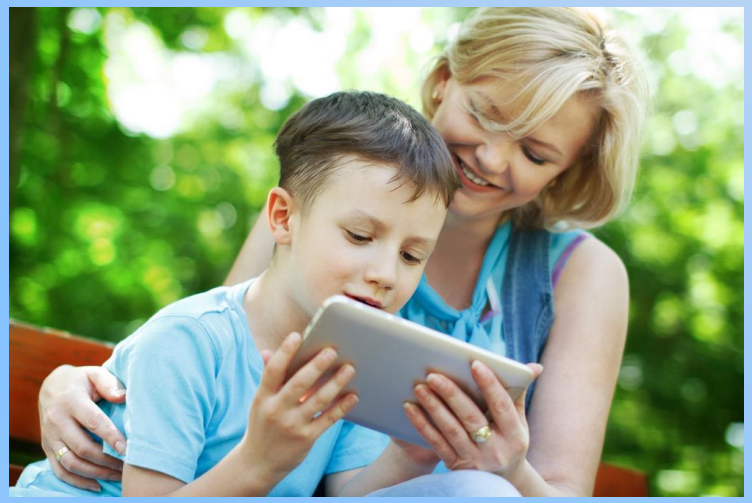
# Как научить детей правильно пользоваться интернетом.

*Самый первый совет заключается в том, что первые сеансы в сети ребенок должен проводить с кем-нибудь из взрослых. Желательно пользоваться такими программами, как "Родительский контроль", чтобы контролировать все действия детей в интернете.*

*Нужно ограничивать самостоятельное использование почты и чатов, ведь это может быть даже опасно. Так как там, например, педофилы могут искать себе жертв. Дадим несколько рекомендаций относительно того, как можно постараться обеспечить максимально безопасность детей в сети интернет.*

# Рекомендации.

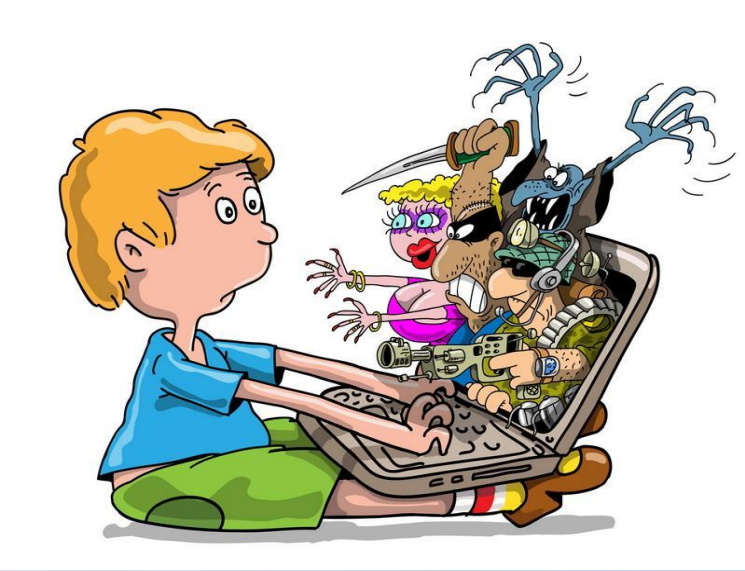
- *Сделайте так, чтобы дети делились с вами всеми своими неудачами и успехами при освоении интернета.*
- *Научите ребенка рассказывать обо всем, что вызывает у него беспокойство.*
- *Расскажите, как соблюдать конфиденциальность, помогите выбрать регистрационные данные, не разглашающие реальных, ведь информационная безопасность в сети интернет – залог того, что удастся избежать многих неприятностей.*
- *Объясните, что в виртуальном пространстве не нужно никому называть свою фамилию, домашний адрес, номер школы и т. п.*
- *Научите, что нет разницы между поступками в реальной жизни и в интернете.*
- *Посоветуйте не встречаться с друзьями из сети, так как ожидания могут быть обмануты, не верить всему тому, что им говорят/пишут.*
- *Обязательно установите специальное ПО и контролируйте своих детей.*



# Советы родителям детей 14-16 лет.

*Когда вашему ребенку 14-16 лет, маловероятно, что вы сможете больше его разбираться в компьютерах, интернете и всех подобных вещах. Хотя, конечно, о контроле и влиянии на него забывать нельзя. Тем более надо помнить о такой проблеме, как обеспечение безопасности в сети интернет. Ведь, если компьютер общий, или все устройства подключены к единой домашней сети, то и угрозы будут общими. К тому же просматривать отчеты о деятельности ребенка вы всегда сможете. Рекомендуется не конфликтовать с ребенком по этому поводу, а пробовать общаться и находить общий язык. Несмотря на возражения, постарайтесь заставить принять правила пользования интернетом, скажите, какие сайты нельзя посещать.*

*ПК, имеющий выход в сеть, должен быть установлен в общей комнате. Это будет немного сдерживать вашего ребенка. Установите ПО, блокирующее нежелательные сайты, не разрешайте без согласования с вами устанавливать любые программы. И не забывайте следить за тем, чтобы дети не стали зависимыми от интернета. Надеемся, что наши советы помогут защитить ваши компьютеры от угроз.*



# Спасибо за внимание!