МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №74»

Исследовательская работа

Тема: Безопасность в Интернете

Выполнила:
Голованова Валерия,
Ученица 9 Г класса
МАОУ СОШ №74
"Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/".

Ижевск
2015

Все школьники являются пользователями Интернета, отчасти даже очень активными. Но информации как обеспечивать безопасность в Интернете очень мало.

Цель исследования

Классифицировать основные Интернет-опасности и освоить правила защиты от них.

Задачи исследования

- Проанализировать информацию об опасностях в сети Интернет;
- Что делать если ты столкнулся с Интернет-угрозой?
- Какие меры должны принимать родители для защиты детей от Интернет–угроз?
- Как повысить культуру поведения в сети;
- Провести анкетирование учащихся по проблеме отношения каждого из них к безопасности в сети интернету.

План работы

1. Какие бывают угрозы в Интернете?
2. Что такое "ник"?
3. Кем на самом деле может быть собеседник в сети?
4. Чем опасны незнакомцы в сети?
5. Какие существуют правила поведения в сети?
6. Как избежать неприятностей в Интернете?
7. Что такое Интернет-фильтр?
8. Какие существуют методы защиты ребенка от Интернет-угроз?

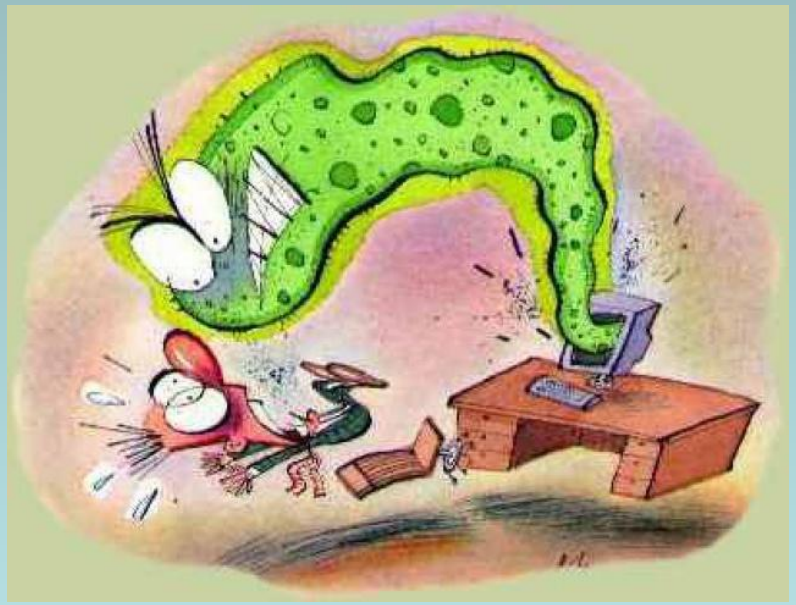
Угрозы в Интернете

- Если говорить об угрозах информационно-технического характера, можно выделить такие элементы как кража информации, вредоносное ПО, хакерские атаки, СПАМ, халатность сотрудников, аппаратные и программные сбои, финансовое мошенничество, кража оборудования.

Согласно статистике применительно к этим угрозам, можно привести следующие данные (по результатам исследований, проведённых в России компанией InfoWath)

Вирус

- Вирус Под компьютерным вирусом принято понимать программы или элементы программ, несанкционированно проникшие в компьютер с целью нанесения вреда, отличительной особенностью которых является способность самотиражирования.



Шпионские программы

- Шпионская программа (Spyware) - это программный продукт, установленный или проникший на компьютер без согласия его владельца, с целью получения практически полного доступа к компьютеру, сбора и отслеживания личной или конфиденциальной информации. Эти программы, как правило, проникают на компьютер при помощи сетевых червей, троянских программ или под видом рекламы

  Одной из разновидностей шпионских программ являются
- Фишинг (Phishing) - это почтовая рассылка имеющая своей целью получение конфиденциальной финансовой информации. Такое письмо, как правило, содержит ссылку на сайт, являющейся точной копией интернет-банка или другого финансового учреждения.
- Фарминг – это замаскированная форма фишинга, заключающаяся в том, что при попытке зайти на официальный сайт интернет банка или коммерческой организации, пользователь автоматически перенаправляется на ложный сайт, который очень трудно отличить от официального сайта. основной целью злоумышленников, использующих Фарминг, является завладение личной финансовой информацией пользователя. Отличие заключается только в том, что вместо электронной почты мошенники используют более изощренные методы направления пользователя на фальшивый сайт.

Что такое "ник"?

- **Никнейм** (*никнэйм, ник*; англ. *nickname* — первоначально «кличка», «прозвище»); также **сетевое имя** — псевдоним, используемый пользователем в Интернете, обычно в местах общения (в чате, форуме, блоге). Чаще всего слово является производным от собственного имени или фамилии (напр. мищЪ — Мищенко, *asash* — Саша), имени мифических персонажей или героев

Чем опасны незнакомцы в сети?

- Знакомство через интернет давно стало нормальным явлением. Однако момент, когда ваш собеседник перестаёт быть двоичным кодом и превращается в живого человека, всегда таит в себе элемент риска. Как не нарваться на маньяка, который ищет свою жертву во всемирной паутине?
- **Поведение маньяка**
- Если фото удачные, принцев набежит много, вам придётся долго их сортировать. Загвоздка этого трудоёмкого процесса в том, что абсолютное большинство маньяков – прирождённые психологи и приятные собеседники. Они сделают всё, чтобы вы обратили на них внимание. Поэтому перед тем как соглашаться на свидание, узнайте о своём собеседнике как можно больше.
- Начните с фотографий. Насторожить должно одно фото в анкете (попросите прислать ещё), желательно фото, сделанные прямо сейчас – например, с любимой собакой, о которой он только что вам рассказывал, а лучше – рядом с экраном компьютера, на котором высвечивается ваше сообщение. Если потенциальный принц отказывается выполнить такое простое желание, или вы поняли, что с вами переписывается кто-то другой, прощайтесь с ним – это не ваш принц.
- Предположим, ваш виртуальный собеседник выполнил ваши требования. Не торопитесь идти на свидание, узнайте о нём как можно больше: имя, фамилию, отчество, дату рождения (не бойтесь воспользоваться поисковиками, там может всплыть самая неожиданная информация). Обзаведитесь и мобильным, и домашним, и, по возможности, рабочим телефонами потенциального жениха. Позвоните ему, убедитесь, что все номера действующие и принадлежат именно этому человеку.

Какие существуют правила поведения в сети?

- **Интернет может показаться зоной где всё позволено.**
- Но это далеко не так.
- Кроме поиска информации, люди ещё и общаются в Интернете. Для новичков очень важно понять некоторые правила поведения в Интернете, что называется - Нетикет.Прячась за вымышленными именами и пользуясь анонимностью некоторые пользователи позволяют себе хамить другим людям,глубоко веря в свою безнаказанность.Чаще всего эти пользователи не ведут себя так в реальной жизни.
- Правила Нетикета существуют для всех кто их соблюдает и для тех кто не соблюдает.Создавались эти правила для комфортного времяпровождения в сети,как и в реальной жизни пользователям удобнее общаться на приличном языке с воспитанными людьми,а не с озлобленными,комплексующими хамами.И если Вы не будете соблюдать эти простые правила с Вами просто не будут общаться.Придётся придумывать новые ники,подбирать новые аватары,заново регистрироваться на сайтах.Короче как в жизни-как Вы к людям так и они к Вам.
- Книга Netiquette,выпущенная в 1994 году описывает десять основных правил нетикета, следование которым существенно облегчит жизнь как Вам, так и окружающим. Вот они:

Как уменьшить опасность Интернета?

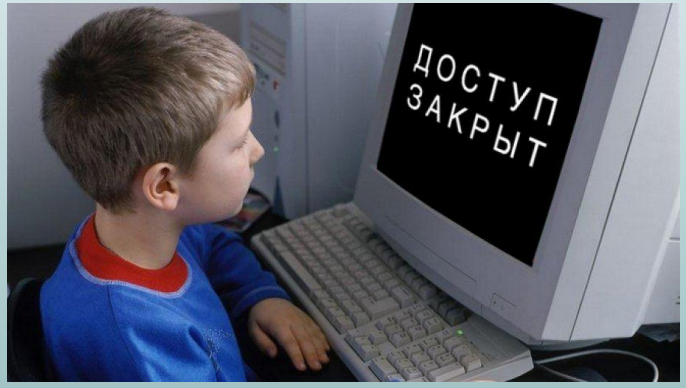
- **Как уменьшить опасность Интернета**?
- **Никогда не сохраняй на компьютере**, даже личном, пароли для входа на различные сайты. Существуют шпионские программы, которые, проникая в компьютер, «воруют» все «запомненные» пароли.
- **Не используй** одинаковые пароли и логины на разных сайтах.
- **Не используй** в качестве пароля данные, которые так или иначе фигурируют в «открытой форме» — дату рождения, имя, фамилию и т.п.
- **Не храни пароли** в текстовых файлах на компьютере **–** эти данные могут быть украдены шпионской программой. Лучше действуй по старинке – внеси их в обыкновенный блокнот!
- Если это не принципиально важно, используй **никнейм**, а не реальные имя и фамилию.
- **Заведи несколько почтовых ящиков** на разных серверах. Это нужно при регистрации на различных сайтах, требующих «привязки» к электронному адресу. Если «сложить все яйца в одну корзину», то взлом одного аккаунта может повлечь взлом всех остальных!
- **Увидев на чужой страничке** или стороннем сайте свои фото или данные, размещенные без твоего согласия, сделай «моментальный снимок» экрана – если начнется разбирательство, то у тебя будут доказательства!
- **Не открывай сообщения**, попавшие в папку «Спам» — удаляй их без прочтения! Если ты это сделаешь, то не только рискуешь подвергнуться вирусной атаке, но и даешь сигнал почтовому серверу не считать в дальнейшем сообщения с данного адреса спамом.
- **Регулярно обновляй антивирусную программу.** Вставив в компьютер флешку (даже свою), прежде чем открывать, проверь ее на наличие вирусов.
- Соблюдая эти несложные рекомендации, можно сделать Интернет гораздо безопаснее!

Что такое Интернет-фильтр?

- Интернет-фильтры – это программные инструменты, которые могут помочь отслеживать веб-содержимое, просматриваемое на определенном компьютере или в сети. В случае с настройками семейной безопасности Интернет-фильтры также могут помочь родителям управлять тем, с кем могут общаться дети и как долго они могут использовать компьютер.

Какие существуют методы защиты ребенка от Интернет-угроз?

- Во-первых:
- – расскажите о возможных интернет-угрозах и последствиях, чтобы на примере показать, как это важно,
- – работайте в интернет вместе,
- – поговорите о том, почему нельзя сообщать посторонним личные данные (адреса, телефоны),
- – разъясните детям, почему необходимо пользоваться антивирусными программами,
- – согласуйте с ребенком правила пользования интернетом (что можно и что нельзя).
- Во-вторых:
- – уделяйте внимание компьютерной грамотности своего ребенка, объясните ему элементарные правила безопасности, которыми пользуетесь сами (не запускать подозрительные файлы, не переходить по ссылкам в спам-сообщениях). Для более надежной защиты установите на компьютер ребенка антивирусную программу с со специальной функцией – например, Родительский контроль в продуктах Kaspersky Internet Security). Этот инструмент позволит ограничивать нецензурную лексику, общение с подозрительными лицами в соцсетях, блокировать доступ к нежелательным сайтам.



Выводы:

Защитите свой компьютер Защитите свой компьютер Регулярно обновляйте операционную систему. Регулярно обновляйте операционную систему. Используйте антивирусную программу. Используйте антивирусную программу. Применяйте брандмауэр. Применяйте брандмауэр.

Защитите себя в Интернете *Защитите себя в Интернете С осторожностью разглашайте личную информацию. С осторожностью разглашайте личную информацию. Думайте о том, с кем разговариваете. Думайте о том, с кем разговариваете.*

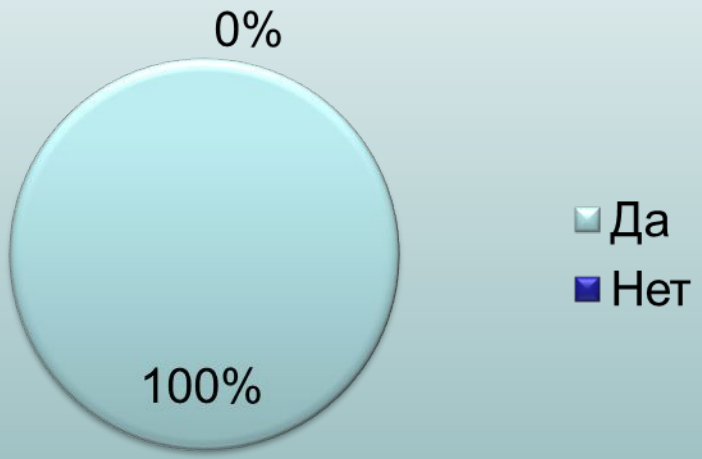
Создавайте резервные копии важных файлов.
Создавайте резервные копии важных файлов. Будьте осторожны при загрузке новых файлов. Будьте осторожны при загрузке новых файлов.

Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.
Помните, что в Интернете не вся информация надежна и не все пользователи откровенны. Соблюдайте правила Соблюдайте правила

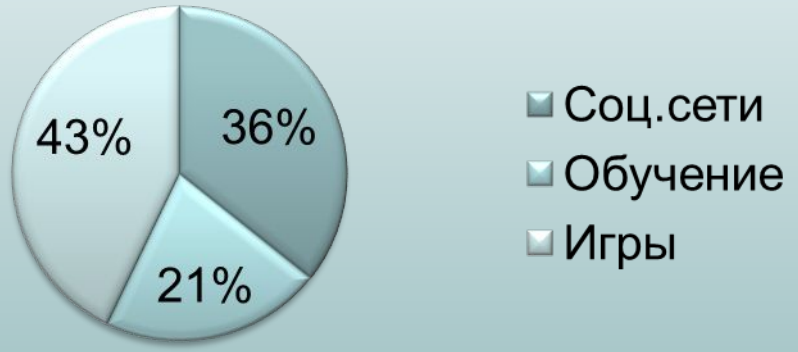
Закону необходимо подчиняться даже в Интернете.
Закону необходимо подчиняться даже в Интернете. При работе в Интернете не забывайте заботиться об остальных так же, как о себе. При работе в Интернете не забывайте заботиться об остальных так же, как о себе.

Анкетирование

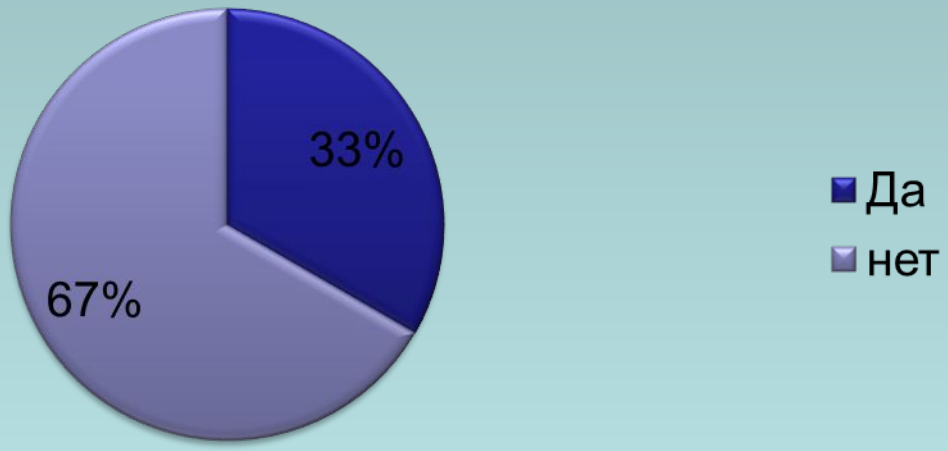
Есть ли у тебя дома интернет



Какие сайты ты посещаеш

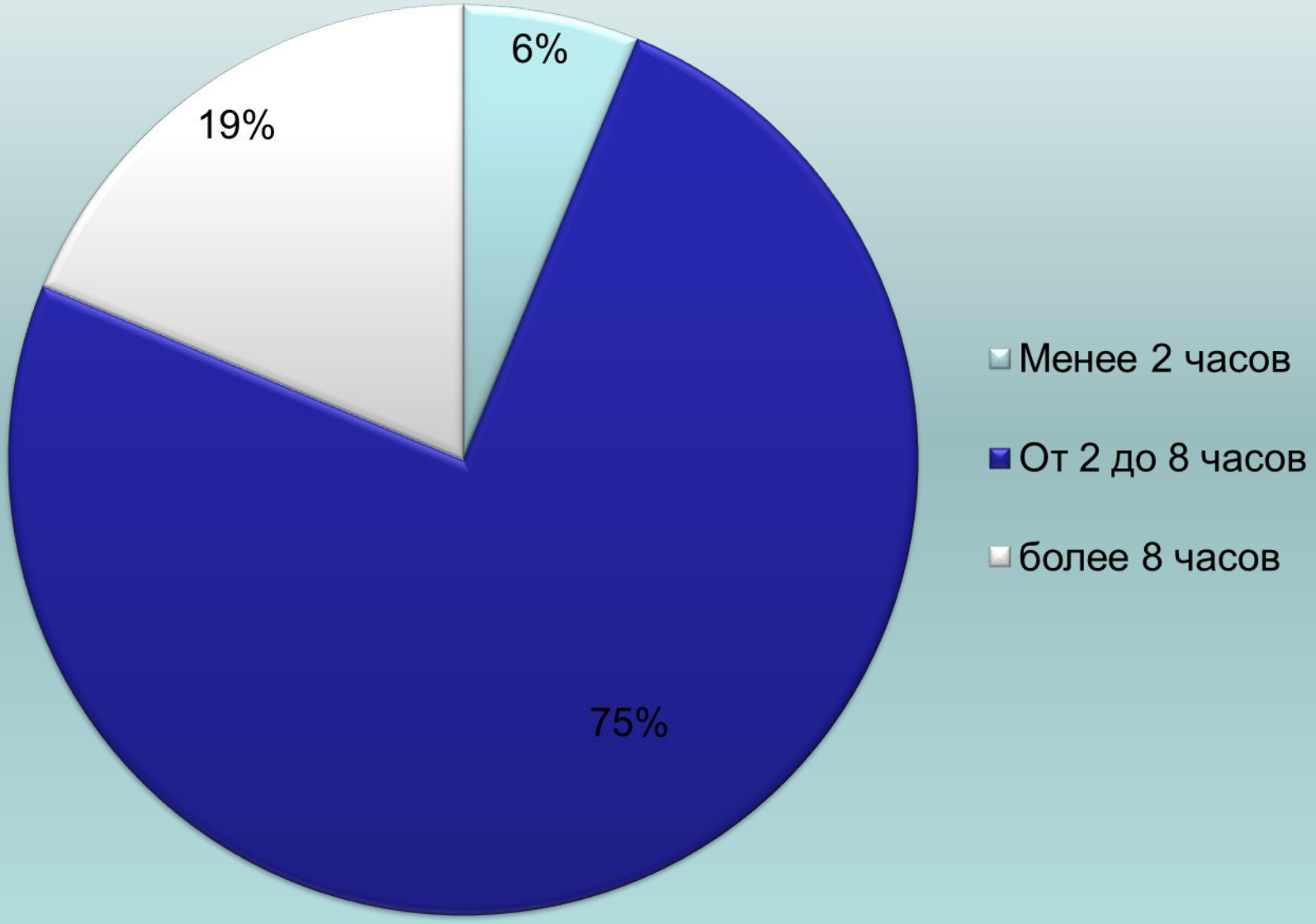


Знаешь ли ты об опасностях интернет



Если бы ты имели неограниченный доступ в Интернет, сколько времени ты бы там проводил?

Сколько времени в день ты проводиш в Интернете



Какими браузерами вы пользуйтесь