

Безопасный Интернет



Цель урока:

Познакомить учащихся услугами Интернет, с опасностями, которые подстерегают их в сети и помочь избежать этих опасностей.



Опрос

- Как вы общаетесь со своими ?
- Какие виды общения для вас более интересны?
- Что вам больше всего нравится в сети Интернет?
- Как ваши родители воспринимают ваши занятия в Интернете? Почему?



Вопрос 1
**Какие виды услуг
Интернета вы знаете?**





- Телеконференции
- Интернет – телефония
- Файловые архивы
- Электронная почта
- WWW
- Форумы прямого общения – чат



Вопрос 2

**Какие опасности
подстерегают нас в
Интернете?**



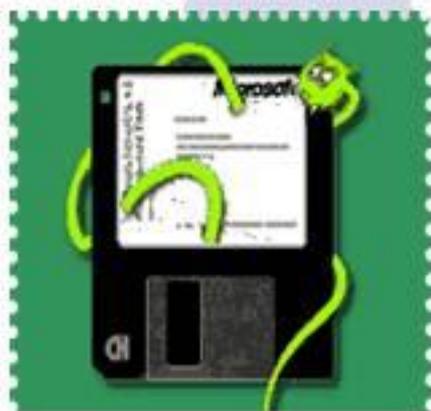
Мошенничество в Интернете



- Обман по телефону: требование выкупа
- SMS - просьба о помощи
- Телефонный номер-грабитель
- Телефонные вирусы
- Выигрыш в лотерее
- Простой код от оператора связи
- Штрафные санкции и угроза отключения номера
- Ошибочный перевод средств
- Доступ к SMS и звонкам

Классические компьютерные вирусы

К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью: последующего запуска своего кода при каких-либо действиях пользователя; дальнейшего внедрения в другие ресурсы компьютера.



Троянские программы

В данную категорию входят программы, осуществляющие несанкционированные действия: сбор информации и ее передачу злоумышленнику, ее разрушение или модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблагоприятных целях.



Сетевые черви

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

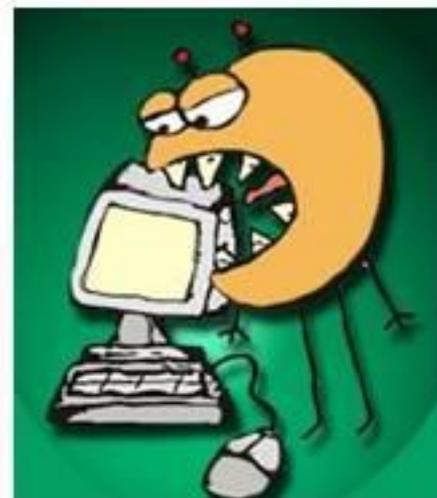
- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие компьютеры сети.



Прочие вредоносные программы

К данной категории относятся:

- утилиты автоматизации создания сетевых червей, вирусов и троянских программ
- библиотеки, разработанные для создания вредоносного ПО;
- утилиты скрытия кода зараженных файлов от антивирусной проверки



Интернет – дневники



Последние исследования показывают, что сегодня примерно половина всех веб - журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя.

Интернет-мошенничество и хищение данных с кредитной карты



Банковская карта – это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

Азартные игры



На игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков.

Сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги.

Пиратство on-line

Онлайновое пиратство – это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом – например, музыки, фильмов, игр или программ – без разрешения правообладателя.



Материалы нежелательного содержания

К материалам нежелательного содержания относятся: материалы порнографического, ненавистнического содержания, материалы суицидальной направленности, сектантские материалы, материалы с ненормативной лексикой.



Недостоверная информация



Пользователи сети должны мыслить критически, чтобы оценить точность материалов; поскольку абсолютно любой может опубликовать информацию в Интернете.



Правила поведения в Интернете



Защита от вредоносных программ



Вредоносные программы можно разделить на три группы:

- компьютерные вирусы;
- сетевые черви;
- троянские программы.

Как запретить выполнение вредоносных программ

- Не открывать сообщение, если оно пришло от неизвестного отправителя.
- Никогда не открывайте сразу присланные файлы - вложения, в том числе полученные от друзей, коллег или от имени известных фирм.
- Обращайте внимание на расширение файла. Будьте очень осторожны при получении сообщений с файлами - вложениями.
- Подозрительные сообщения лучше немедленно удалять.



Безопасное использование телеконференций

Когда вы помещаете сообщение в группе новостей, в нем всегда содержится ваш обратный адрес. Это потенциально опасно, поскольку существуют специальные программы, которые способны автоматически сканировать подобные объявления, выуживая из них почтовые адреса



Безопасное использование электронной почты

- Во - первых, как правило, по электронной почте чаще всего рассылают документы и изображения, но не программы.
- Во - вторых, в случае необходимости получения программы по почте, можно договориться с отправителем, чтобы он предварительно упаковал ее с помощью какого-либо архиватора, например, Winzip или WinRar.

Общие рекомендации по обеспечению безопасной работы в Интернете



Антивирусные программы

Условно-бесплатные:

- **AVP** = Antiviral Toolkit Pro (www.avp.ru) – Е. Касперский
- **DrWeb** (www.drweb.com) – И. Данилов
- **Norton Antivirus** (www.symantec.com)
- **McAfee** (www.mcafee.ru)
- **NOD32** (www.eset.com)



Есть бесплатные пробные версии!

Бесплатные:

- **Avast Home** (www.avast.com)
- **Antivir Personal** (free-av.com)
- **AVG Free** (free.grisoft.com)



Обновление – это полезно и безопасно



- **Настройте свой компьютер против вредоносных программ**
- **Проверяйте новые файлы**
- **Будьте бдительны и осторожны**
- **Резервное копирование – гарантия безопасности**





Не выдавай личные данные никому в сети Интернет! Ты не знаешь, кто поджидает тебя на другой стороне провода!



ТВОЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

В Европе свыше 13 миллионов детей, как ты, регулярно пользуются Интернетом. Если ты ищешь информацию по своему домашнему заданию или только хочешь повеселиться, то Интернет – замечательное место, но ты должен знать об опасностях и следовать советам:

НЕ НАЖИМАЙ НЕИЗВЕСТНЫЕ ССЫЛКИ

Когда ты общаешься в чатах и интернет-пейджерах или получаешь письмо, никогда не нажимай непосредственно на ссылку. **ЕСЛИ ОНА ПРИШЛА ОТ НЕЗНАКОМОГО ЧЕЛОВЕКА, ЛУЧШЕ НЕ ОБРАЩАТЬ НА НЕЕ ВНИМАНИЯ.**



НЕ СКАЧИВАЙ ФАЙЛЫ ИЗ НЕИЗВЕСТНЫХ ИСТОЧНИКОВ

Без сомнения, ты часто получаешь сообщения, предлагающие тебе скачать фото, песню или видео. **ИНОГДА ТАКИЕ ФАЙЛЫ МОГУТ ОТПРАВЛЯТЬСЯ НЕ ЧЕЛОВЕКОМ ИЗ ТВОИХ КОНТАКТОВ, А ВИРУСОМ, КОТОРЫЙ ЗАРАЗИЛ ЕГО КОМПЬЮТЕР И ПЫТАЕТСЯ РАСПРОСТРАНИТЬСЯ СРЕДИ ДРУГИХ ПОЛЬЗОВАТЕЛЕЙ.**



Именно по этой причине ты должен всегда спрашивать своего знакомого, действительно ли он отправил тебе сообщение или файл. Если он этого не делал, сообщи ему, что его компьютер заражен. Пусть он сообщит своим знакомым, которые получили от него подобное сообщение или файл, чтобы они не открывали их и

НЕ ОТКРЫВАЙ ПОДОЗРИТЕЛЬНЫЕ ФАЙЛЫ



Если твое решение безопасности говорит тебе, что файл содержит или может содержать угрозу, не открывай файл. **ПРОСТО УДАЛИ ЕГО.**

НЕ ОБЩАЙСЯ С НЕЗНАКОМЦАМИ

В чатах или системах обмена мгновенными сообщениями **ТЫ НИКОГДА НЕ МОЖЕШЬ БЫТЬ УВЕРЕН В ТОМ, КТО С ТОБОЙ ОБЩАЕТСЯ.** Никогда не заводи дружбу с незнакомцами, и ни под какими предлогами не соглашайтесь на встречу с ними в реальной жизни.



НЕ РАСТРОСТРАНЯЙ В ИНТЕРНЕТЕ ЛИЧНУЮ ИНФОРМАЦИЮ

Никогда не отправляй свою личную информацию (твои данные, фотографии, адрес и пр.) по электронной почте и через системы обмена мгновенными сообщениями, а также никогда не публикуй такого рода информацию в блогах и форумах. Кроме того, будь внимательным при создании профилей в таких сервисах, как Facebook или MySpace.

Ты никогда не должен размещать такую конфиденциальную информацию, как твой возраст и твой адрес проживания. Также рекомендуем тебе не использовать свое настоящее имя, а пользоваться псевдонимом или ником.



ОСТЕРЕГАЙТЕСЬ ЗАМАНЧИВЫХ ПРЕДЛОЖЕНИЙ РАБОТЫ

Как правило, никто ничего не дает просто так. Если ты получил фантастическое предложение работы от неизвестных пользователей, **то НЕ ОБРАЩАЙ НА НЕГО ВНИМАНИЯ.**





Безопасный интернет!

Памятка родителям для защиты ребенка от нежелательной информации в сети

Объясните своему ребенку, что:

- при общении использовать только имя или псевдоним (ник);
- номер телефона, свой адрес, место учебы нельзя никому сообщать;
- не пересылать свои фотографии;
- без контроля взрослых не встречаться с людьми, знакомство с которыми завязалось в Сети.

Обязательно расскажите о правах собственности, о том, что любой материал, выставленный в Сети, может быть авторским. Неправомерное использование такого материала может быть уголовно наказуемым.

Поясните, что в сети, несмотря на кажущуюся безнаказанность за какие-то проступки, там действуют те же правила, что и в реальной жизни: хорошо - плохо, правильно - не правильно.

Используйте современные программы, которые предоставляют возможность фильтрации содержимого сайтов, контролировать места посещения и деятельность там.

Научите детей следовать нормам морали, быть воспитанными даже в виртуальном общении.



Внимательно относитесь к вашим детям!

Помните:

Если Вы или Ваши близкие стали жертвами мошенников или Вы подозреваете, что в отношении Вас планируются противоправные действия – незамедлительно обратитесь в ближайший отдел полиции либо напишите заявление на официальном сайте МВД России

www.mvd.ru

[памятка управление «К»](#)



Интернет - ресурсы (картинки):

- <http://goo.gl/1EPiq0>
- <http://goo.gl/g0uycA>
- <https://goo.gl/W4B6uK>
- <http://goo.gl/cvc5dy>
- <http://goo.gl/J9zkAZ>
- <http://goo.gl/TROMwC>
- <http://goo.gl/wdcAFd>
- <http://goo.gl/h3VrNE>
- <http://goo.gl/0wsyul>
- <http://goo.gl/doro3U>
- <http://goo.gl/FN0Ynw>
- <http://goo.gl/OKgBkx>
- <https://goo.gl/sbXWbM>
- <http://goo.gl/THgwsV>
- <http://goo.gl/WwMjxc>
- <http://goo.gl/Xae0l4>
- <http://goo.gl/OFknKp>
- <http://qps.ru/c6teA>
- <http://qps.ru/qg7iT>
- <http://qps.ru/XLOzr>
- <http://qps.ru/7GjMd>
- <http://qps.ru/WABMC>
- <http://qps.ru/j9eL3>
- <http://qps.ru/ODxhu>
- <http://qps.ru/yDLa0>
- <http://qps.ru/Pxdcb>

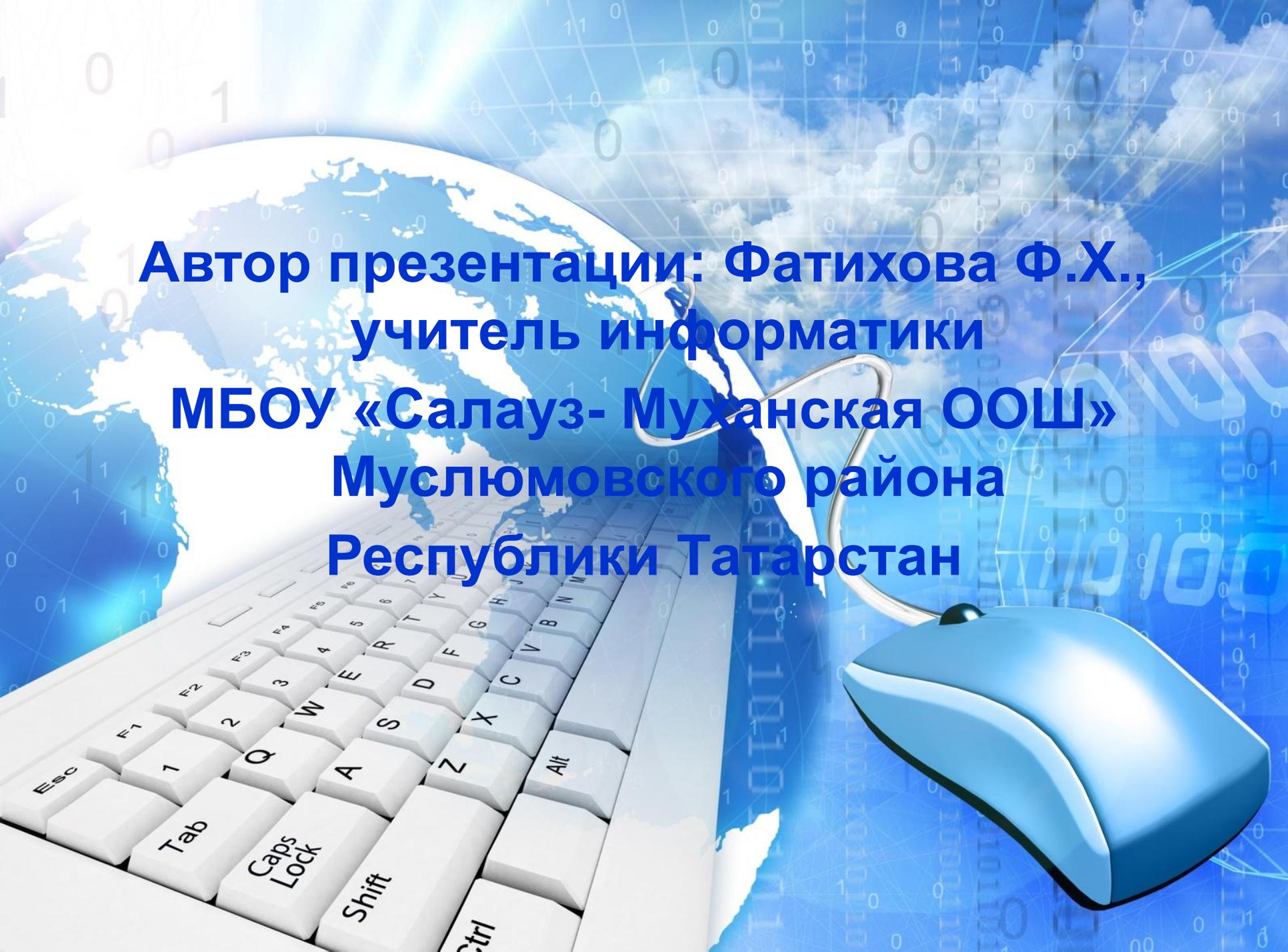


Шаблоны презентации:

http://pedsovet.su/_Id/455/76515848.jpg

<http://pedsovet.su/load/395-1-0-3791>





**Автор презентации: Фатихова Ф.Х.,
учитель информатики
МБОУ «Салауз-Муханская ООШ»
Муслюмовского района
Республики Татарстан**