

*Как узнать про все на свете?
Ну конечно, в ИНТЕРНЕТЕ!
Там музеи, книги, игры,
Музыка, живые тигры!
Можно все, друзья, найти
В этой сказочной сети!*



internet



Территория безопасности

Подготовила:
социальный педагог
Лютова В.Н.

История интернета



**ENIAC - первый компьютер "нулевого поколения".
Был создан в Америке в 1946 году.**



nternet

История интернета



**Тим Бернерс-Ли создатель
Всемирной паутины WWW (1989 г.)**



nternet

История интернета

С 22 января 2010 года прямой доступ в Интернет получил экипаж Международной космической станции



nternet

Опасности в Интернете



- **Вредоносные программы**
- **Кибермошенничество**
- **Социальные сети**
- **Кибербуллинг**
- **Контентные риски**



n



Опасности в Интернете

Вредоносные программы

Вредоносные программы – это разнообразное программное обеспечение, умышленно созданное для нанесения вреда электронным устройствам или похищения информационных ресурсов, данных. Это вирусы, «троянские кони», «черви», «боты», программы слежки. Вредоносные программы, попадая на компьютер, способствуют снижению скорости при обмене данными, а также используют ваш компьютер как базу для распространения своих вредоносных данных. Они могут использовать ваш e-mail или профиль социальной сети как разносчика спама. Такие опасные файлы могут попадать на ваши компьютеры:

- посредством посещения сомнительных веб-сайтов и скачанных с них файлов;
- из электронной почты через полученный спам;
- при помощи электронных носителей.



Опасности в Интернете

Кибермошенничество

- Фишинг;
- Вишинг;
- Смишинг.



Опасности в Интернете

Фишинг – это преступная тактика, используемая интернет-мошенниками с целью обогащения, за счет кражи персональной информации жертвы.

Для фишинга характерны:

- неожиданные сообщения в мессенджерах, смс, соцсетях и электронной почте от имени авторитетной организации (например, банка, платежной системы, онлайн-магазина и т.д.) с побуждением, будь то угроза или просьба, перейти по фишинговой ссылке, либо ввести информацию в прикрепленную к письму форму;
- зловредные баннеры и всплывающие окна, ведущие на фишинговые страницы.



Опасности в Интернете

Помимо классического фишинга существуют и другие способы выманивания денежных средств у доверчивых интернет-пользователей. Среди таковых:

Вишинг – вид телефонного мошенничества, когда злоумышленники звонят и под видом сотрудника банка, финансовой организации и проч. выманивают у жертв реквизиты банковской карты или побуждают совершить какие-либо действия с банковским счетом.

Смишинг – вид фишинга через смс.

Множество объявлений в социальных сетях, использующих призывы к благотворительности и давящие на жалость.



Опасности в Интернете

Кибербуллинг представляет собой появление сообщений в социальных сетях, содержащих угрозы, оскорбления, запугивание или травлю. Есть случаи, когда чью-то страницу могут взломать, разместив на ней негативный контент, унижающий и оскорбляющий человека.

Кибербуллинг опасен тем, что агрессор может сохранять анонимность, вовлекать в травлю других людей. Это значит, что шансы поймать агрессора снижаются, но у него появляется возможность оскорбить жертву, распространить недостоверные сведения о ней среди большой группы людей. Кибербуллинг может навредить психологическому и эмоциональному состоянию человека.

Порой травля в сети переходит в реальную жизнь. Особенно если агрессор и жертва учатся в одной образовательной организации, живут в одном районе.



Опасности в Интернете

ПОСЛЕДСТВИЯ КИБЕРБУЛЛИНГА



58%

*взрослых были
вынуждены вмешаться,
чтобы помочь ребенку*



13%

*виртуальных конфликтов
переросли в реальные*



7%

*пострадавших получили
настолько тяжелую
психологическую травму,
что длительное время
переживали случившееся*



26%

*родителей узнали
об инцидентах
кибербуллинга намного
позже того, как они
случились*



Опасности в Интернете



Вероятность встреч с незнакомыми людьми и **груминг** – еще одна опасность использования социальных сетей. Добавляя в друзья совершенно незнакомых людей и общаясь с ними, дети подвергают себя опасности. Нередки случаи, когда, представляясь сверстником в онлайн-чате, злоумышленник настаивает на личной встрече, которая может обернуться насилием или даже похищением.



n



Опасности в Интернете

Контентные риски

Это присутствие в интернете материалов противозаконного, неэтичного и иного вредоносного характера. Такие материалы могут быть представлены текстами, изображениями, звуковыми и видеофайлами, ссылками и баннерами на посторонние сайты. Не совершеннолетний гражданин может столкнуться с порнографическим контентом, призывами к использованию и приобретению наркотиков, призывами к участию в экстремистских действиях. Такой контент может нанести психологический вред сознанию детей и подростков, изменить их ценностные ориентации.



n



Правила безопасности в интернете

ОСТОРОЖНО:

ВИРУСЫ И ДРУГИЕ ЧЕРЕЗ ТРОЙНЬЕ ВРЕДОНОСНЫЕ ПРОГРАММЫ

В Интернет ты заходишь через компьютер. Это может быть школьный или библиотечный компьютер, твой личный или тот, которым пользуется вся семья.

Любому компьютеру могут повредить вирусы, их еще иногда называют вредоносными программами. Они могут уничтожить важную информацию или украсть деньги через Интернет.

- ▶ Для защиты компьютера на нём установлены специальные защитные программы и фильтры. Не меняй ничего в их настройках!
- ▶ Не сохраняй подозрительные файлы и не открывай их.
- ▶ Если антивирусная защита компьютера не рекомендует, не заходи на сайт, который считается «подозрительным».
- ▶ Никому не сообщай свой логин с паролем и не выкладывай их в Интернете – относись к ним так же бережно, как к ключам от квартиры.



ВИРТУАЛЬНЫЕ МОШЕННИКИ И ДРУГИЕ ПРЕСТУПНИКИ ИНТЕРНЕТА

Ты знаешь, что вне дома и школы есть вероятность столкнуться с людьми, которые могут причинить тебе вред или ограбить. В Интернете также есть злоумышленники – ты должен помнить об этом и вести себя так же осторожно, как и на улице или в незнакомых местах.

- ▶ Не сообщай свой адрес или телефон незнакомым людям и никогда не выкладывай в Интернете. Никогда не высылай свои фотографии без родительского разрешения. Помни, что преступники могут использовать эту информацию против тебя или твоих родных.
- ▶ Если ты хочешь поучаствовать в каком-нибудь конкурсе, где нужно указывать свои данные, посоветуйся с родителями.
- ▶ Никогда не соглашайся прийти в гости к человеку, с которым ты познакомился в Интернете. Если назначается встреча, она должна проходить в людном месте и желательно с присутствием родителей. Помни, что под маской твоего ровесника может скрываться взрослый человек с преступными намерениями.



ГРУБИЯНЫ И ХУЛИГАНЫ В ИНТЕРНЕТЕ: КАК СЕБЯ ВЕСТИ?

Кроме преступников в Интернете есть просто злые и невоспитанные люди. Ради собственного развлечения они могут обидеть тебя, прислать неприятную картинку или устроить травлю. Ты можешь столкнуться с такими людьми на самых разных сайтах, форумах и чатах.

- ▶ Помни: ты не виноват, если получил оскорбительное сообщение. Не нужно реагировать на грубых людей – просто прекрати общение.
- ▶ Если тебе угрожают по Интернету, не стесняйся сообщить об этом родителям. Помни, что цель угроз – испугать тебя и обидеть. Но подобные люди боятся ответственности.
- ▶ Коллективное преследование – это крайнее проявление жестокости. Жертву забрасывают оскорблениями и угрозами, его фотографию искажают и все данные публикуют. Никогда не участвуй в травле и не общайся с людьми, которые обижают других.
- ▶ Всегда советуйся с родителями во всех указанных случаях.

