|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Интерактивный урок по теме: кибербезопасность детей и молодежи***  **Цели урока:**  Методическая: показать актуальность данной темы. Учебная: обучение информационной безопасности в Интернете.  Воспитательная: развитие самоконтроля учащихся и воспитание внимательного отношения к информационным ресурсам.  **Задачи урока:**   * - ознакомить уч-ся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет и научить избегать их; * - формирование навыков поведения в информационном обществе с целью обеспечения информационной безопасности и освоить практические навыки работы в сети Интернет. * Отработка навыков и умений: сравнения информации, критического анализа; выделения главных мыслей и грамотного их изложение; восприятия и усвоения услышанного; * Расширение кругозора учащихся * Формирование информационной культуры   **Оснащение и методическое обеспечение урока: к**омпьютерный класс, подключенный к Internet;АРМ учителя, мультимедийный проектор, интерактивная доска, доска.  **Ход урока:**  1. Организационный момент. Постановка задачи.  2. Значение Интернет.  Преподаватель: Ребята, в Интернете можно найти информацию для реферата или курсовой, послушать любимую мелодию, купить понравившуюся книгу или обсудить горячую тему на многочисленных форумах. Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но сеть Интернет скрывает и угрозы.  3. Наиболее часто встречающиеся угрозы при работе в Интернет.  Преподаватель: Давайте разобьёмся на группы, и каждая группа подумает и назовет опасности, которые нас поджидают в Интернете (обучающиеся называют угрозы. Вся информация открывается в презентации).   1. Угроза заражения вредоносным программным обеспечением (ПО). Для распространения вредоносного ПО и проникновения в компьютеры используется почта, компакт-диски, дискеты и прочие сменные носители, или скачанные из сети Интернет файлы. Эти методы довольно часто используется хакерами для распространения троянских вирусов. 2. Доступ к нежелательному содержимому. Это насилие, наркотики, страницы, подталкивающие к самоубийствам, отказу от приема пищи, убийствам, страницы с националистической идеологией. Независимо от желания пользователя, на многих сайтах отображаются всплывающие окна, содержащие подобную информацию; 3. Контакты с незнакомыми людьми с помощью чатов или электронной почты. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. Выдавая себя за сверстника, они могут выведывать личную информацию и искать личной встречи; 4. Поиск развлечений (например, игр) в Интернете. Иногда при поиске нового игрового сайта можно попасть на карточный сервер и проиграть большую сумму денег. 5. Неконтролируемые покупки.   *Просмотр видеоролика.*  Преподаватель: А сейчас мы посетим сайт, который помогает вас защитить от ненужной информации  http://icensor.ru/  4. Составление правил поведения в сети Интернет.  Преподаватель: Очередное задание для каждой команды. Мы знаем, что для плодотворной работы в Интернете, защиты от ненужной информации, нам необходимо соблюдать правила пользования Интернет-ресурсами. Сейчас вам в группах необходимо обсудить и сформулировать не более 5 самых  важных правил безопасности поведения детей и подростков в сети Интернет. Одно правило может ссылаться сразу на несколько сайтов. (Работа проводится с использованием компьютеров, подключенных к сети Интернет). Когда ребята готовы на доске составляется сводная таблица правил поведения в сети Интернет.   |  |  | | --- | --- | | Никогда | Всегда | | Никогда не оставляй встреченным в Интернете людям свой номер телефона, домашний адрес или номер школы без разрешения родителей | Всегда будь внимательным, посещая чаты. Даже если в чате написано, что он только для детей, нельзя точно сказать, что все посетители действительно являются твоими ровесниками. В чатах могут сидеть взрослые, пытающиеся тебя обмануть | | Никогда не отправляй никому свою фотографию, не посоветовавшись с родителями | Всегда спрашивай у родителей разрешения посидеть в чате | | Никогда не договаривайся о встрече с интернет-знакомыми без сопровождения взрослых. Они не всегда являются теми, за кого себя выдают. Встречайся только в общественных местах | Всегда покидай чат, если чье-то сообщение вызовет у тебя чувство беспокойства или волнение. Не забудь обсудить это с родителями | | Никогда не открывай прикрепленные к электронному письму файлы, присланные от незнакомого человека. Файлы могут содержать вирусы или другие программы, которые могут повредить всю информацию или программное обеспечение компьютера | Всегда держи информацию о пароле при себе, никому его не говори | |  | Если ты услышишь или увидишь, что твои друзья заходят в «небезопасные зоны», напомни им о возможных опасностях и посоветуй, как им правильно поступить. | |  | Будь внимателен при загрузке бесплатных файлов и игр на компьютер, тебя могут обмануть: нажав на ссылку, ты можешь попасть в «небезопасную зону» или загрузить на свой компьютер вирус или программу — шпион. | |  | Если вы получили оскорбляющие сообщения, расскажите об этом родителям. | |  | Всегда принимайте помощь от взрослых или друзей, разбирающихся в вопросах безопасного Интернета. Мама и папа могут не знать ответов на все интересующие вас вопросы. | | Никогда не отвечай на недоброжелательные сообщения или на сообщения с предложениями, всегда рассказывай родителям, если получил таковые | Всегда помни, что если кто-то сделает тебе предложение, слишком хорошее, чтобы быть правдой, то это, скорее всего, обман. | |  | Всегда держись подальше от сайтов «только для тех, кому уже есть 18». Такие предупреждения на сайтах созданы специально для твоей же защиты. Сайты для взрослых также могут увеличить твой счет за Интернет |   Преподаватель: Вы ребята хорошо поработали и за это я хочу показать и рассказать вам сказку:  5. Золотые правила безопасности в Интернет:   * - всегда помни свои: E-mail, логин, пароли; * - не поддавайся ярким рекламам-указателям; * - не заходи на подозрительные сайты; * - если пришло письмо о крупном выигрыше – это «Лохотрон»: просто так выиграть невозможно; * - не сиди часами в Интернет, заводи себе будильник, садясь за компьютер; * - изучай полезные социальные сервисы Web 2.0; * - не забывай обновлять антивирусную программу; * - не скачивай нелицензионные программные продукты.   6.Практическая часть.  Зайдите в детский чат <http://prikol.interchat.ru/>, зарегистрируйтесь там, и пообщайтесь, используя правила безопасности, с которыми мы сегодня ознакомились.  7.  Подведение итогов  8. Домашнее задание. Найти в Интернете сайты,  защищающие вас  от «опасной» информации. |