

Департамент образования администрация г. Перми
Муниципальное бюджетное учреждение
«Центр психолого-педагогической, медицинской и социальной помощи» г. Перми

РАССМОТРЕНО

утверждено на заседании
НМС МБУ «ЦПМСП» г.
Перми
Протокол № 4 от 29.12.2022г.

СОГЛАСОВАНО

О.В. Полторак,
начальник управления
воспитания и социализации
департамента образования
администрации города Перми



УТВЕРЖДАЮ

О.А. Митина
и.о. директора МБУ
«ЦПМСП» г. Перми



ПРОГРАММА
киберурока «Безопасность в сети Интернет»
(для учащихся 11 класса)

г. Пермь, 2022

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ УЧАЩИХСЯ 11 КЛАССОВ

71. КИБЕРУРОК

«Безопасность в Интернете» (для 11 классов)

Цель урока: способствовать формированию у обучающихся навыков безопасного и ответственного поведения в современной информационно-телекоммуникационной среде.

Задачи:

образовательные:

- сформировать правила безопасной работы учащихся в Интернете;
- учить ориентироваться в современном информационном пространстве;
- заложить основы правовых знаний работы в Интернете.

развивающие:

- формировать информационную культуру учащихся;
- развивать умение самостоятельно находить нужную информацию пользуясь web-ресурсами;
- развивать критическое мышление.

воспитательные:

- воспитывать ответственность и дисциплинированность учащихся при работе в сети.

Оборудование: компьютерный класс, ПК, мультимедийный проектор.

Ход урока

I. Оргмомент

II. Активизация внимания

Учитель.

Сегодня у нас очень важная тема, те проблемы, о которых мы будем говорить, касаются абсолютно каждого из вас. Посмотрев, на рисунки и попробуйте определить тему нашего урока.

Интернет вошел в нашу жизнь. Интернет наш помощник – помогает нам работать, путешествовать, отдыхать, общаться с друзьями. Интернет наш учитель – помогает получать новые знания, своевременную информацию.

Но путешествие в Интернет похоже на поход неопытного человека в лес. В лесу можно заблудиться, попасть в болото, собрать ядовитые грибы или ягоды, попасть в лапы диких зверей. Но, если человек знает лес, знает, кто в нем обитает, знает растения, которые в нем растут, то поход в лес ничего кроме пользы и удовольствия не принесет.

Так и в Интернете много полезного, нужного и интересного, но на каждой web – странице вас могут поджидать информация, опасная для вашего кошелька, физического или психического здоровья и даже жизни.

Задача нашего урока оценить эти опасности и выработать стратегию

поведения в каждом конкретном случае.

III. Новый материал

Группа 1

Вирусы

5. Что делают вирусы на нашем компьютере? (виды вирусов, пути распространения, деструктивные действия)

6. Антивирусные программы (назначение, возможности, советы по безопасности)

Группа 2:

Мошенники в Интернете

11. Сайты – двойники

12. Интернет – шантаж

13. Предложение работы на дому и не только

14. «Лохотрон» на проверке безопасности

15. Инвестиционные проекты и финансовые пирамиды

Демонстрируется видеоролик «Безопасность и развлечения в Интернете»

Группа 3:

Информация в интернете

1. Безопасное общение. Что такое «скам»?

2. Интернет – зависимость

3. Какие сайты не следует посещать никогда

Демонстрируется видеоролик «Безопасность в Интернете»

Группа 4

Этика и право в Интернете

7. Этические нормы Интернета

8. «Крэкерские» сайты и «ломанные» программы

9. Защита интеллектуальной собственности в России

Просмотр видеоролика «Я и Интернет»

(<http://kvestsetevichok.ru/index.php/2015-09-17-14-45-01/videourok>)

Правила безопасного поведения в сети Интернет

Просмотр видеоролика, подготовленный пресс-службой Совета Федерации Федерального Собрания Российской Федерации, о проведении 30 октября во всех школах страны Единого урока безопасности в сети Интернет (<http://kvestsetevichok.ru/index.php/rolik-soveta-federatsii>).

IV. Закрепление материала

Учитель.

Давайте проверим, насколько хорошо вы усвоили сегодняшний урок, выполнив тест на компьютере. (Индивидуальная работа учащихся на ПК)

V. Итог урока

VI. Домашнее задание (по выбору учащихся)

5. Запишите в тетрадь основные правила безопасного поведения в сети Интернет

6. Придумать сказку для учащихся младших классов об осторожности в Интернете

VII. Рефлексия

Киберурок "Безопасный интернет"

Аннотация

Данный урок разработан для учащихся 9-11 классов. При разработке и проведении урока были использованы методические материалы по проведению всероссийского урока безопасности школьников в сети Интернет, размещённые на сайте <http://www.сетевичок.рф>

Разработка может быть полезна учителям-предметникам и классным руководителям при проведении уроков, посвящённых проблеме безопасности в Интернете.

Цель проведения занятия – повышение информационной грамотности учащихся, обеспечение ответственного и безопасного поведения в современной информационно- телекоммуникационной среде.

Содержание

9. Введение.
10. Проблемы современной жизни в киберпространстве.
11. Наиболее злободневные вопросы.
12. Основные выводы для обеспечения безопасного и полезного пребывания в сети Интернет.

Введение

Современное общество и виртуальная реальность тесно связаны друг с другом. Подростки проводят большую часть времени в Интернет и не мыслят себя без него. Массу преимуществ и колоссальные возможности даёт возможность пользоваться Интернетом, но как и в реальной жизни, жизнь в киберпространстве сопряжена с целым рядом рисков.

Проблема безопасного интернета становится всё более актуальной проблемой, так как год от года возрастает количество киберпреступлений.

Проблемы современной жизни в киберпространстве

Какие опасности могут подстерегать пользователей Интернета?

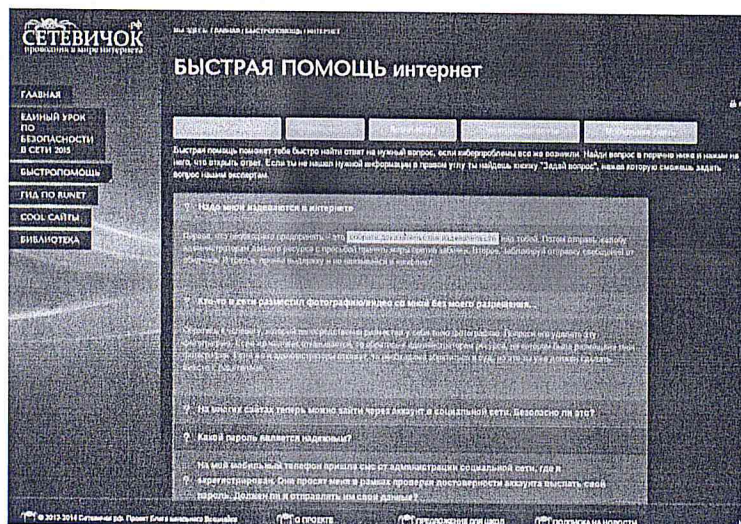
В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Для этого они могут использовать вирусное программное обеспечение (или

«вирусы»), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и на почтовых сервисах, смс-мошенничество.

Мошенникам удаётся достичь своих целей, так как они манипулируют такими человеческими качествами как доверчивость, невнимательность и неосведомлённость. Осведомлён – значит вооружён! Надо знать о возможных действиях мошенников, быть готовым не поддаваться провокации с их стороны и в случае атаки дать отпор, действовать грамотно.

Наиболее злободневные вопросы

Множество вопросов возникает у пользователей сети Интернет, когда они сталкиваются с проблемами. И есть много ресурсов, посвящённых безопасности в сети. Наиболее частовозникающие вопросы по разрешению проблем, возникающих у подростков, разработчики сайта «Сетевичок» собрали в раздел «Быстропомощь» (<http://xn--b1afankxqj2c.xn--p1ai/vopros/elektronnaya-all>)



На этом ресурсе отдельно рассматриваются общие вопросы безопасности, вопросы, посвящённые Интернету, компьютеру, электронной почте и мобильной связи.

Здесь же можно задать свой вопрос, если ответ на страницах сайта не найден. Для этого существует форма обратной связи, и все операторы находятся офлайн. Можно оставить сообщение и получить ответ на него в ближайшее время.

Памятка для пользователей

Как уберечь компьютер от заражения вирусом

- Используйте антивирусное программное обеспечение с обновленными базами вирусных сигнатур.
- Не открывайте вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства связи, не удостоверившись, что файл или ссылка не содержит вирус.
- Внимательно проверяйте доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).
- Обращайте внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.
- Не подключайте к своему компьютеру непроверенные съемные носители.
- Не поддавайтесь на провокации злоумышленников, например, требования перевести деньги или отправить смс, чтобы снять блокировку компьютера.

Как защитить свои личные данные

- Используйте сложные пароли (они состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).
- Никому не сообщайте свой пароль.
- Для восстановления пароля используйте привязанный к аккаунту мобильный номер, а не секретный вопрос или электронную почту.
- Не передавайте учетные данные — логины и пароли — по незащищенным каналам связи (не защищены, как правило, открытые и общедоступные wi-fi сети).
- Внимательно проверяйте доменные имена сайтов, на которых вводите учетные данные.
- Не вводите пароли от важных учётных записей, когда подключены к общественной Wi-Fi-сети.

Как не попасться на удочку смс-мошенников

- Не отправляйте смс на незнакомые телефонные номера, за отправку таких смс могут взимать плату.
- Переводите деньги только на известные телефонные номера.
- Не вводите телефонный номер на незнакомых сайтах.

Как избежать мошенничества при платежах

- Помните, что банки и платежные сервисы никогда не просят сообщать — ни по почте, ни по телефону — пароль, пин-код или код из смс.
- Никому не сообщайте пароли, пин-коды и коды из смс от своего кошелька или банковской карты.
- Храните банковскую карту в надежном месте.
- Не держите записанные пароли и коды рядом с картой.
- Заведите отдельную карту для покупок в интернете.
- Используйте для покупок в интернете только личный компьютер.
- Регулярно обновляйте антивирусную защиту компьютера.
- Старайтесь делать покупки в известных и проверенных интернет-магазинах.
- Перед подтверждением оплаты убедитесь, что в адресной строке браузера указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.
- Подключите в банке услугу уведомлений по смс, чтобы оперативно получать сведения о совершенных транзакциях.
- Сохраняйте документы об оплате услуг и доставке товаров, полученные по электронной почте.
- Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.

Основные выводы для обеспечения безопасного и полезного пребывания в сети Интернет

Пользователи должны научиться грамотно пользоваться Интернетом и электронными устройствами:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет;

- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
- избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
- распознавать признаки злоупотребления их доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
- критически относиться к информационной продукции;
- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

Будь внимателен! Стань грамотным потребителем цифровой эпохи!