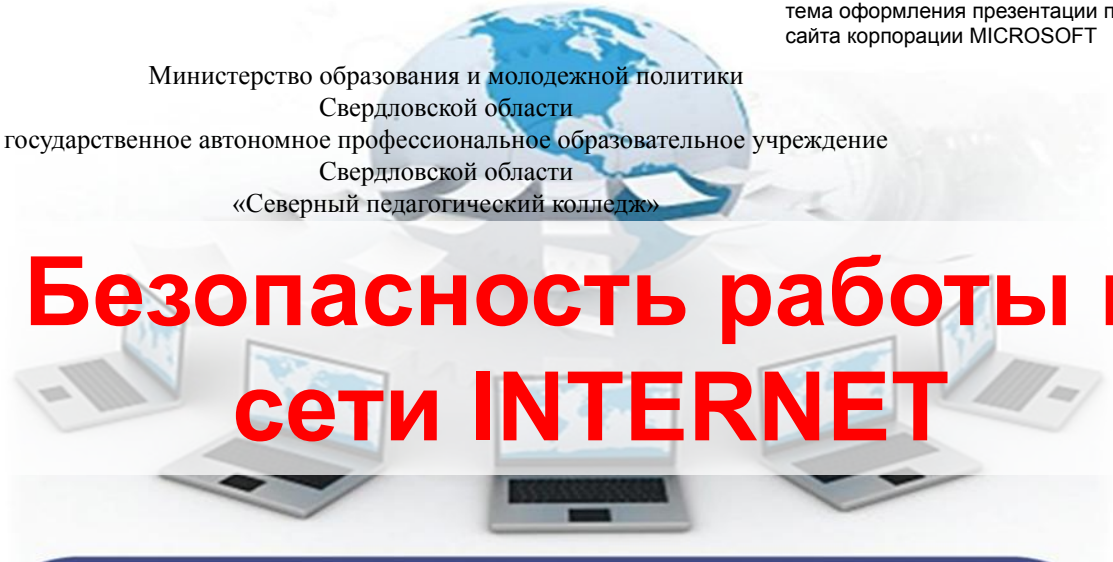
тема оформления презентации позаимствована с официального сайта корпорации MICROSOFT

Министерство образования и молодежной политики
Свердловской области
государственное автономное профессиональное образовательное учреждение
Свердловской области
«Северный педагогический колледж»



Безопасность работы в сети INTERNET

Коллективная презентация
144 группы
март 2023

Возможные опасности сети INTERNET

Климова Виктория

Как программное обеспечение может представлять угрозу информационной безопасности в сети Интернет?К таким угрозам мы можем отнести:

- Вредоносное программное обеспечение(вирусы),интернет-мошенничество
- атаки на отказ обслуживание
- кражи денежных средств
- кражи персональных данных
- несанкционированный доступ к информационным ресурсам и систем
- распространение заведомо недостоверной информации

Что такое СПАМ и как с ним бороться?

Волошко Ольга

Спам- это массовая рассылка незапрашиваемых получателем электронных сообщений коммерческого и некоммерческого содержания.

Как бороться со СПАМом?

-настроить безопасность браузера и почтовой программы (подключить антифишинг, защиту от спама и другие встроенные средства защиты)

-использовать дополнительные расширения браузеров, например AddBlock (позволяет блокировать СПАМ и рекламные блоки)

-использовать антивирус и файерволл

-проверять надежность поставщика услуг, использовать информационные сервисы “who is”

Кто такие ХАКЕРЫ и как от них защититься?

Кузьминых Анастасия

Хакер — человек, превосходно разбирающийся в устройстве и функционировании вычислительных систем, умеющий быстро найти и элегантно устранить ошибки в их работе. Однако сейчас этим словом также обозначают киберпреступника, который с помощью высоких технических знаний и навыков взламывает информационные системы ради удовольствия, с корыстными или иными целями.

Чтобы защитить компьютер от взлома и хакеров, нельзя делать этого:

1) Переход по сомнительным ссылкам

2) Использование неизвестных флэш-накопителей

3) Скачивание фальшивого антивирусного ПО

4) Отключение функций управления учетными записями пользователей

5) Использование одного пароля для разных сайтов при отсутствии двухфакторной аутентификации

6) Использование слабых паролей

7) Использование публичных Wi-Fi сетей

Что такое фишинг?

Шестакова Татьяна

Фишинг- вид интернет- мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей- логинами и паролями. Это достигается путем проведения массовых рассылок электронным писем от имени популярных брендов,а также личных сообщений внутри различных сервисов, например,от имени банков, или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Почему нужно избегать знакомств в интернете?

Михель Екатерина

Обманщики и подозрительные типы. В Интернете каждый может представить себя кем угодно. Простой уставший работяга вешает в Интернете фото модели и придумывает себе красивую легенду о своих машинах и яхтах, и все, он уже звезда, толпы красавиц мечтают с ним встретиться, засыпая его письмами. У него может быть обычная серая жизнь, а ваши письма придают ей новый смысл. Ничего ужасного нет в том, что он хочет вашего тепла и внимания, если Вам тоже это нравится.

Интернет-мошенники. Хуже, если ваш визави по переписке окажется и вовсе мошенником. За красивыми комплиментами для доверчивых женщин могут скрываться корысть и расчет. Нужно себе отдавать отчет, что человек про себя может рассказать что угодно. Нельзя слепо верить совершенно незнакомому вам человеку

Всегда нужно помнить о своей безопасности и не стоит раскрывать все карты: сообщать свои координаты, адрес проживания и д. т. Чтобы не столкнуться с подобными проблемами не стесняйтесь задавать интересующие вас вопросы в переписке, чтобы узнать побольше о потенциальном кавалере. Поинтересуйтесь, есть ли у него аккаунты в социальных сетях: в Контакте и Одноклассниках. По личной страничке человека, зарегистрированного в любой из социальных сетей, можно сделать много выводов: с кем он дружит, чем он живет, какие мысли его посещают, понять его интересы и желания. Чем больше вы соберете информации до вашей первой встречи, тем лучше!

Материал заимствован с этого сайта:
https://vk.com/@club_zol-podvodnye-kamni-internet-znakomstv-chego-sleduet-opasatsya

Чем опасна интернет- зависимость?

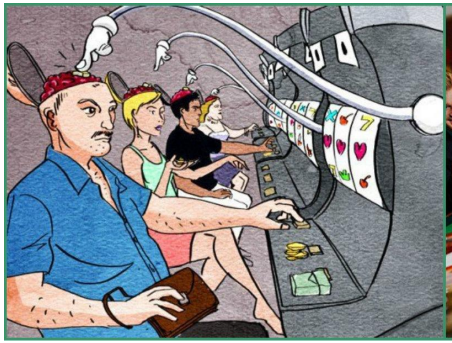
Свиридова Екатерина

Психологи бьют тревогу и сравнивают феномен интернет-зависимости не иначе как с пристрастием к алкоголю и наркотикам. Поводы для беспокойства действительно имеются. Проводимые исследования на тему интернет-зависимости показывают, что при длительном и неконтролируемом нахождении в сети происходят изменения в состоянии сознания и в функционировании головного мозга. Постепенно это приводит к потере способности обучаться и глубоко мыслить.

Чем опасны азартные игры в Internet?

Орыщенко Лиза

1) необходимость введения информации о банковских картах, ведь при переводе денег приходится вводить свои данные. Любой хакер, взломавший интернет- сайт азартных игр, может получить доступ к информации пользователя.
2) подростков, страдающих зависимостью от азартных игр в интернет сети, значительно ухудшается моральное и психическое состояние здоровья. Обычно это проявляется в излишней замкнутости, или наоборот- агрессивности, раздражительности.
3) Обычно подростки стараются убегать от реального мира в виртуальный, и никак наоборот. Поэтому когда они неоднократно терпят поражение, постепенно пропадает уверенность в себе, упадок сил, расстройство нервной системы.
4) Как правило, когда подростки играют в бесплатные азартные игры в сети интернет, куда больше шансов выиграть. Это вселяет им уверенность, что в платных играх им так же будет везти.



Компьютерные вирусы и методы защиты от вредоносных программ.

Ходырева Дарья

Компьютерный вирус — это **небольшая программа, которая распространяется с одного компьютера на другой и мешает работе компьютера**. Компьютерный вирус может повредить или удалить данные на компьютере, распространить его на другие компьютеры с помощью почтовой программы или даже удалить все данные на жестком диске.

Методы защиты от вредоносных программ:

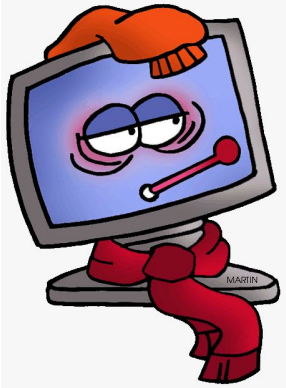
- Используй современные операционные системы;
- Постоянно скачивай обновления своей ОС;
- Ограничить физический доступ к ПК;
- Используй внешние носители информации;
- Работай на своем компьютере под правами пользователя, а не администратора;
- Используй антивирусные программные продукты известных производителей.

Признаки “заражения” компьютера

Анисимова Настя

При заражении компьютера могут появиться следующие признаки:

- На компьютере появляются неожиданные сообщения, изображения или звуковые сигналы.
- Программы без вашего участия могут запускаться или подключаться к интернету.
- Друзьям на почту или через мессенджер приходят сообщения, которые вы не отправляли.
- В вашем почтовом ящике много сообщений без адреса отправителя и темы письма.
- Компьютер работает медленно или часто зависает.
- При включении компьютера операционная система не загружается.
- Файлы и папки могут исчезнуть, или их содержимое может измениться.
- Всплывает множество системных сообщений об ошибке.
- Браузер зависает или ведет себя неожиданным образом. Например, вы не можете закрыть вкладку.



Материал взаимствован с этого сайта:
https://support.kaspersky.ru/common/beforeinstall/790

Какие данные относятся к персональным? Ильина Полина

К персональным данным относят:

- фамилия, имя, отчество;
- место, дата рождения;
- место постоянной или временной регистрации;
- фотография или видеозапись человека, позволяющие идентифицировать человека;
- сведения о детях, родственниках, семейном положении;
- сведения о заработной плате;
- оценка навыков, личностных качеств;
- индивидуальные личные данные (раса, национальность, политические или религиозные взгляды, философские убеждения; состояние здоровья);
- информация о судимостях, или их отсутствии;
- номер телефона, адрес электронной почты, иные идентификаторы в соц. сетях или мессенджерах;
- паспортные данные, СНИЛС, ИНН (хотя с ИНН вопрос спорный);
- биометрические данные.

Как защитить персональные данные при общении в социальных сетях?

Воронина Лада

Как защитить персональные данные в Сети:

1. Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.
2. Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.
3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат действительно тот, за кого себя выдает.
4. Используйте только сложные пароли, разные для разных учетных записей и сервисов

ИСТОЧНИК

Пять правил для родителей, которые заинтересованы в безопасности своих детей в интернете.

Шрайнер Ева

1. Разместите компьютер в общей комнате — таким образом, обсуждение Интернета станет повседневной привычкой, и ребенок не будет наедине с компьютером, если у него возникнут проблемы.
2. Используйте будильник, чтобы ограничить время пребывания ребенка в Сети — это важно для профилактики компьютерной зависимости.
3. Используйте технические способы защиты компьютера: функции родительского контроля в операционной системе, антивирус и спам-фильтр.
4. Создайте «Семейные Интернет-правила», которые будут способствовать онлайн-безопасности для детей.
5. Обязательно обсуждайте с детьми все вопросы, которые возникают у них в процессе использования Сети, интересуйтесь друзьями из Интернета. Учите критически относиться к информации в Интернете и не делиться личными данными онлайн

Источник: https://www.mbdou192.ru/images/Bezopasnost/pam-1.pdf

Советы по безопасности при работе в Интернете

Коротич Яна

1.Установите антивирусные программы;
2.Используйте сложные логины и пароли;
3.Проверяйте безопасность соединений;
4.Будьте внимательны к соединениям Wi-Fi;
5.Создайте тве почты, для работы и личную;
6.Не передавайте конфиденциальные сведения;
7.Ограничьте информацию о себе в интернете;
8.Не открывайте подозрительные письма;
9.Не переходите по подозрительным ссылкам;
10.Не устанавливайте подозрительные приложения;
11.Будьте аккуратны с незнакомыми людьми в сети;
12.Блокируйте подозрительных пользователей;
13.Будьте осторожны с бесплатными приложениями
14.Посторайтесь ничего не покупать в социальных сетях.

Какие правила пользования чужой техникой нужно помнить?

Лукашова Ирина

Несколько простых правил, которые следует соблюдать при работе в открытых сетях или с использованием «чужой» техники:

- При работе с публичным устройством используй пункт «чужой компьютер».
- Используй режим «приватного просмотра» в браузере.
- Всегда используй кнопку «выйти» при завершении работы с ресурсом.
- Отказывайся от сохранения пароля при работе на «чужом компьютере».
- Используй только открытые сети в надежности которых ты уверен.
- Используй безопасное соединение с почтой и сервисами (безопасное соединение обозначено замком с зелёным текстом).
- Не оставляй без присмотра устройства доступа в сеть (телефон, планшет, ноутбук).
- Используй шифрованные хранилища данных, которые помогут защитить твои личные файлы.
- Используй сложные пароли, состоящие из прописных и заглавных латинских букв и цифр, а также символов.