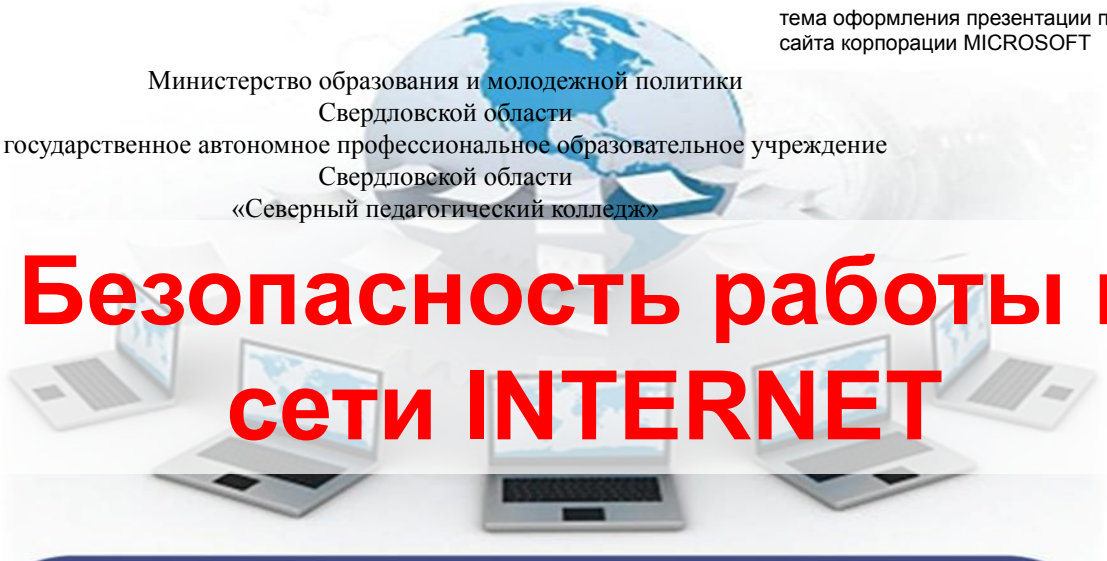
тема оформления презентации позаимствована с официального сайта корпорации MICROSOFT

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



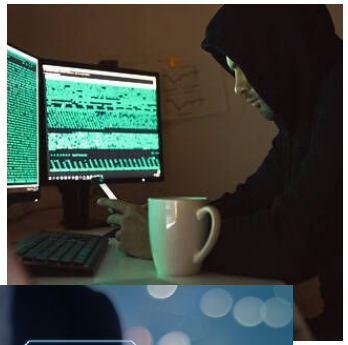
Безопасность работы в сети INTERNET

Коллективная презентация
141 группы
февраль 2023

Кто такие ХАКЕРЫ и как от них защититься?

Демина Полина

Хакер (от английского *to hack* — «рубить, обтесывать») в широком и положительном смысле — человек, превосходно разбирающийся в устройстве и функционировании вычислительных систем, умеющий быстро найти и элегантно устранить ошибки в их работе.



Как защититься от хакеров:

1. Не переходить по сомнительным ссылкам;
2. Не использовать неизвестные флэш-накопители;
3. Не скачивать фальшивый антивирус ПО;
4. Не использовать один пароль для разных сайтов при отсутствии двухфакторной аутентификации;
5. Не отвечать на фишинговые письма;
6. Не использовать публичные Wi-Fi сети и др.

Материал заимствован с этого сайта

Материал заимствован с этого сайта

Что такое СПАМ и как с ним бороться?

Будахин Даниил

Спам — массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желания её получить. Распространителей спама называют спамерами.

1. Обучайте свой **спам**-фильтр ...
2. Никогда не отвечайте на **спам** ...
3. Заведите отдельный ящик для личных писем ...
4. Подключите стороннюю защиту от **спама** ...
5. Не публикуйте личный адрес в общедоступных местах

Материал взаимствован с этих сайтов:

https://www.reg.ru/blog/kak-borotsya-so-spamom-v-ehlektronnoj-pochte-5-proverennyh-metodov/

https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B0%D0%BC

Почему нужно избегать знакомств в интернете?

Красноперов Вадим

Потому что в интернете попадаются мошенники, который могут принести вам физический и моральный вред.
Мошенники в интернете — это особый тип людей, способный втереться в доверие к женщинам, очаровывать с целью завладеть их деньгами, имуществом. Им свойственно обычно глубокое знание психологии, умение построить общение так, что жертвы сами, добровольно отдают им материальные ценности. Мошенники умело подбирают «ключик» к сердцу девушки, «сигналя» ей, что она любима, прекрасна, желанна, влюбляют ее в себя.

Материал заимствован с этого сайта

Чем опасна интернет- зависимость?

Киселёв Дмитрий

За последнее десятилетие интернет стал неотъемлемой частью жизни для большинства населения. Сегодня любой современный человек хоть раз в день, для общения, работы или просто поиска нужной информации посещает сети всемирной паутины. Безусловно, интернет имеет огромное значение в современном мире и приносит большую пользу человечеству: как неиссякаемый источник информации, доступный способ приобретения навыков и знаний, как незаменимый помощник в работе и бизнесе, как средство проведения и планирования досуга, как место для знакомств и способ поддержания связи. Интернет облегчает выбор и покупку необходимых товаров и услуг, а также позволяет сэкономить на их приобретении

Интернет-зависимость – это расстройство в психике, сопровождающееся большим количеством поведенческих проблем и в общем заключающееся в неспособности человека вовремя выйти из сети, а также в постоянном присутствии навязчивого желания туда войти.

материал заимствован с этого сайта

Чем опасны азартные игры в Internet?

Бакиров.М

Самая главная опасность, которую представляют компьютерные игры – это **возникновение игровой зависимости**. Это настоящее отклонение психики, требующее помощи квалифицированного врача и поддержки родных и близких.

Втягивание в игру происходит быстро, порой за считанные недели. Стоит этим людям начать выигрывать, как им кажется, что удача будет сопутствовать им постоянно. На процессе игры они начинают тратить все больше сил в надежде получить за это награду в виде денежного приза, но проигрыш гарантирован, а выигрыш вероятен. Проигрыш рождает чувство вины и досады, злости и попытку во что бы то ни стало добиться желаемого успеха, а, следовательно, разжигает азарт. Объединяет проблемных игроков и то, что они любят только выигрывать, но не умеют проигрывать.

Материал взят из интернет источников

https://mahnovichi.schools.by

Компьютерные вирусы и методы защиты от вредоносных программ.

Почанин Дмитрий

Компьютерный вирус – это программа, внедряемая в различные объекты или ресурсы компьютерных систем и сетей и способная производить определенные действия без ведома пользователя.

Защита компьютера от вирусов

- Не открывайте сообщения электронной почты от незнакомых отправителей или незнакомые вложения.
- Используйте блокирование всплывающих окон.
- При использовании Microsoft Edge, убедитесь, что SmartScreen включен.
- Обратите внимание на уведомления Windows SmartScreen.
- Регулярно обновляйте Windows.
- Используйте параметры конфиденциальности.

материал взаимствован из интернета

Антивирусная защита

Давыдова Алёна

Что является средством антивирусной защиты?
Средство **антивирусной защиты** - программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации **средств защиты** информации, а также …

Антивирус – это средство выявления и удаления компьютерных вирусов и других вредоносных программ. Для того, чтобы определять новые компьютерные вирусы и вредоносные программы, которые появляются каждый день, антивирусы используют базы данных.

Материал взаимствован с этого сайта

Признаки “заражения” компьютера

Левченко
Александр

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.

https://support.kaspersky.ru/common/beforeinstall/790

Защита авторских прав

Черныгин
Андрей

Пресечение действий, нарушающих авторских права или создающих угрозу нарушения. В частности, такое требование может быть направлено на запрет распространения контрафактных экземпляров произведения.

https://sumip.ru/biblioteka/avtorskoye-pravo/zashhita-avtorskix-prav/

Защита авторских прав осуществляется способами, предусмотренными гражданским законодательством. Способ защиты – это требования, которые автор может предъявить к нарушителю исключительного права или личных неимущественных прав.

Признание права, если нарушитель оспаривает существование авторских прав или их принадлежность определенному лицу. Признание исключительного права позволяет установить правообладателя произведения, признание права авторства направлено на разрешение конфликта по поводу личных неимущественных прав. Довольно часто с требованием о признании авторства обращаются соавторы произведения.

Какие данные относятся к персональным?

Мозылев Андрей

К персональным данным, согласно закону, относят:

- фамилия, имя, отчество;
- место, дата рождения;
- место постоянной или временной регистрации;
- фотография или видеозапись человека, позволяющие идентифицировать человека;
- сведения о заработной плате;
- индивидуальные личные данные (раса, национальность, политические или религиозные взгляды, философские убеждения; состояние здоровья);
- номер телефона, адрес электронной почты, иные идентификаторы в соц. сетях или мессенджерах;
- паспортные данные, СНИЛС, ИНН
- биометрические данные.

Персональные данные — это любая информация, прямо или косвенно относящаяся к физическому лицу, и позволяющая его определить.

Материал взаимствован с этого сайта.

Как защитить персональные данные при общении в социальных сетях?

Прохорова Татьяна

5 рекомендаций по защите персональных данных в социальных сетях:

1.Не следует запускать сомнительные программы, присланные от незнакомого человека, или даже от знакомого (т.к. его страница может быть взломана и находиться в руках злоумышленников).

2. Старайтесь не открывать сомнительные письма от любых адресатов людей, а уж тем более не переходите по ссылкам, которые могут содержаться в этих письмах, так как это могут быть вредоносные ссылки. Например, вы переходите по ссылке, и ваш компьютер автоматически скачивает программу, которая закреплена там злоумышленниками.

3. Проверяйте все скачанные файлы антивирусом, так как в них могут быть помещены специальные вредоносные программы. Например, программа, которая отправляет информацию с вашего компьютера на абсолютно любой другой, в основном на компьютер злоумышленника.

4. При вводе пароля внимательно проверяйте точно ли это настоящая главная страница социальной сети (существуют сайты, которые созданы для того чтобы получать информацию, вводимую пользователем в строки «пароль» и «логин»), например, главная страница «Вконтакте» - https://vk.com. Если, выделяя ссылку, мы увидим лишнюю букву, или хоть какие-то изменения, такие как - https://vkontakte.com, то будьте уверены - этот сайт создан злоумышленниками.

5. При пользовании чужим компьютером следуют помнить, что вся введённая вами информация (пароли, переписки и т.д.) может дублироваться в специальных текстовых документах, не говоря уже о том, что не нужно ставить галочку *запомнить пароли*, а тем более не нужно забывать выходить с социальных сетей, в которых вы авторизовались.

Выполнение всех 5 пунктов позволит улучшить *защиту персональных данных* в социальных сетях.

Материал заимствован с этого сайта

Каким образом злоумышленники могут получить доступ к вашему компьютеру?

Жаркевич Алексей

Первый приём. Социальная инженерия.
Это метод управления действиями человека без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным.
Второй приём. Фишинг (“рыбалка”).
Основан на создании подделок популярных сайтов. Так вместо официальной страницы банка, вы можете оказаться на его поддельной копии со всеми вытекающими последствиями.
Третий приём. Блокирование операционной системы.
Основан на блокировании операционной системы и требования некоторых сведений или суммы денег за её разблокировку.

Материалы были взяты
с данного сайта

Что такое кибератака и как от нее уберечься?

Аман Анастасия

Кибератаки — это попытки получить несанкционированный доступ к компьютерным системам и украсть, изменить или уничтожить данные.

Чтобы уберечь себя от кибератак, нужно делать следующее:

- С подозрением относитесь к сообщениям от незнакомых отправителей, особенно к тем, которые содержат ссылки или вложения.
- Не нажимайте на подозрительные ссылки или подозрительные электронные письма и вложения.
- Регулярно перезагружайте мобильные устройства, что может помочь повредить компоненты вредоносных программ.
- Используйте шифрование и защищайте паролем ваши устройства.
- По возможности сохраняйте физический контроль над своим устройством.
- Отключите геолокацию и закройте камеру на устройствах.

Материал заимствован с этого сайта

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

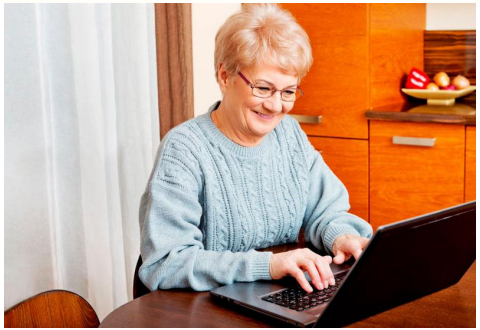
Вершков Данила

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

Материал заимствован с этого сайта

Правила пользования интернетом для пожилых людей

Литовских
денис



По мере развития интернет-сервисов в сети появляются новые виды мошенничеств, причем нацелены они, в первую очередь, на неподготовленных к цифровому миру пожилых людей.
По словам эксперта, чтобы защитить близкого пожилого человека, нужно объяснить ему простые правила и описать наиболее распространенные угрозы, потому что сам он не всегда сможет сориентироваться в цифровом пространстве. В частности, в первую очередь, надо помочь пожилым людям придумать уникальные и длинные пароли и объяснить, что делиться ими нельзя.

Материал заимствован с этого сайта

Советы по безопасности при работе в Интернете

Жмурин
Тимофей

Безопасность при работе в сети

Защитить компьютер от большинства угроз интернета можно соблюдая простые правила безопасности. Среди перечисленных ниже советов есть как конкретные рекомендации, так и общие правила. Следовать каждому конкретному совету — ваш выбор, но каждый из них поможет сделать вашу работу в интернете безопаснее.

- **Используйте последнюю версию вашей операционной системы и следите за ее обновлениями**
- **Следите за обновлениями браузера и его компонентов**
- **Установите антивирус**
- **Включите и настройте файрволл (брандмауэр)**
- **Пользуйтесь учетной записью с ограниченными правами**
- **Используйте сложные пароли**
- **Используйте легальное ПО**
- **Делайте резервные копии ценных данных**

Материал заимствован с этого сайта

Опасные сообщества сети INTERNET

Москаленко
Ульяна

1. Суицидальные группы и группы смерти «Синий кит»
2. Вербовка детей в запрещенные организации и группы
3. Новое детское увлечение АУЕ*
4. «Колумбайн» или скулшутинг
5. Кибербуллинг или травля ребенка сверстниками

Материал заимствован с этого сайта

Правила осуществления интернет- платежей

Никалюкина В.

Услуга оплаты через интернет осуществляется в соответствии с Правилами международных платежных систем Visa, MasterCard и Платежная система «Мир» на принципах соблюдения конфиденциальности и безопасности совершения платежа, для чего используются самые современные методы проверки, шифрования и передачи данных по закрытым каналам связи.

- Подключите интернет-банк и СМС-оповещение. Это позволит вам отслеживать операции в режиме реального времени.
- Не используйте подозрительные сайты. Адрес защищенного сайта должен начинаться с https://. Также рядом с адресной строкой должна быть иконка в виде закрытого замка. Эти знаки покажут, что вы имеете дело с ответственным продавцом и ваши данные будут передаваться в зашифрованном виде.
- Откройте отдельную карту для интернет-платежей и не храните на ней значительных денежных остатков.
- Не сообщайте данные своей банковской карты другим людям: ни банковским служащим, ни работникам интернет-магазинов.
- Совершайте покупки с устройств, на которых установлена антивирусная защита.
- Если интернет-магазин по каким-либо причинам вызывает у вас подозрение, используйте платежные системы Apple Pay, PayPal или другие.

Как сохранить деньги на банковском счете от злоумышленников?

Шерстобитов Кирилл

1. Никогда не сообщайте реквизиты своей карточки посторонним людям. Никто не имеет права знать эту информацию. Даже работники банка при выдаче карты отворачиваются, когда вы устанавливаете PIN.

2. Помните, что самая важная информация о карте – трехзначный код CVC на оборотной стороне. Он позволяет совершать виртуальную идентификацию и покупать онлайн.

https://sovcombank.ru

Если Вас шантажируют или Вам угрожают через интернет...

Лямин Александр

🤐 Не общайтесь

Мошенники действуют массово в расчете на тех, кто испугается и заплатит. Даже не начинайте вести диалог с шантажистами. Лучше выкинуть листок с угрозами или переместить электронное письмо в спам

🚫 Не платите

Даже если вы согласитесь и отправите деньги мошеннику, нет гарантий, что он не исполнит угрозу — например, не опубликует ваши интимные фото. К тому же он будет знать, что вы на крючке, и обязательно попросит заплатить еще и еще

🙋 Предупредите друзей

Таким образом вы лишите мошенника рычага давления. Расскажите на странице в соцсети, что на вас сфабриковали компромат и теперь требуют деньги. Шантажисту станет неинтересно, и он пойдет искать другую жертву

👮 Подайте заявление в полицию

Можно даже не ходить в полицию, а подать заявление по телефону. Вместо поиска новых жертв мошеннику придется заметать следы

[Материал взаимтвован с этого сайта]

Что такое эксплойт и как обезопасить себя от него?

Шумайлов Данил

Эксплойт – это программа, фрагмент машинного кода или набор команд, использующих уязвимости (ошибки в алгоритме) для атаки на компьютер, чтобы его контролировать или нарушить работоспособность.

Чтобы защитить себя от эксплойтов, необходимо :

1. регулярно обновлять приложения и операционную систему,
2. организовать антивирусную защиту, в состав которой входит антивирус, брандмауэр и антишпион.

В зависимости от мишени эксплойты подразделяются :

информация взята с этого сайта

Как избавиться от навязчивой интернет-рекламы?

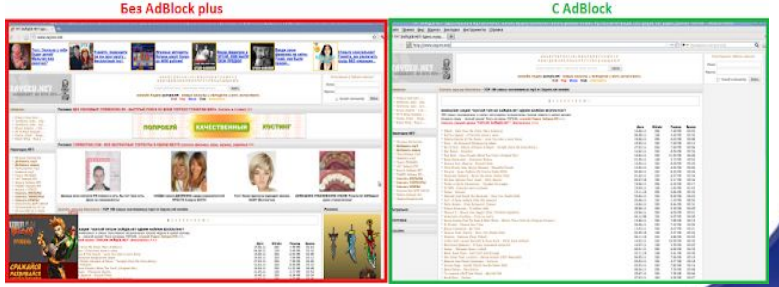
Конюхов Влад

Каждый день мы сталкиваемся с надоедливой рекламой в интернете, которая всплывает, мешает и вообще часто содержит непотребную информацию (в тему прошлого поста о том, как защитить детей от плохого интернета).
Есть простейший способ от нее избавиться - дополнение к браузеру AdBlock Plus.
Установить его очень просто:

Для Chrome
1 вариант кликните сюда (магазин Chrome) и нажмите установить
2 вариант Настройки (справа сверху кнопка) -> Инструменты -> Расширения -> Еще расширения (снизу) -> В поиске вводим "adblock plus" и нажимаем установить

Для Firefox
Ctrl+Shift+A (расширения) -> Ctrl+F (поиск расширений) -> В поиске вводим "adblock plus" и нажимаем установить

После установки расширения вся плохая реклама будет заблокирована.



жмакать сюда)))

Правила безопасности в интернете.

Куликов Сергей

1. Установите антивирусные программы

2. Используйте сложные логины и пароли

3. **Разлогинивайтесь на чужих устройствах**

4. Проверяйте безопасность соединений

5. Будьте внимательны к соединениям Wi-Fi

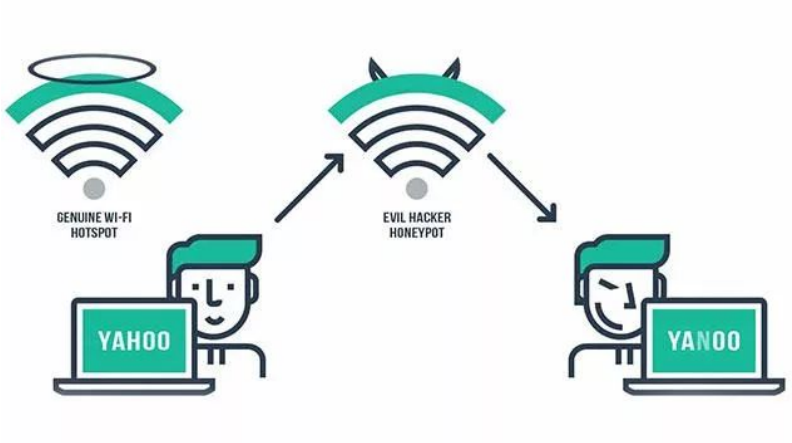
Материал заимствован с этого сайта

Опасности использования сетей WI-FI

Есаулков Дмитрий

Ответ прост: кражей данных. Пользуясь Интернетом, вы передаете много ценной информации — платежные данные, логины и пароли от всевозможных сервисов, документы и переписку. Если она попадет в руки преступника, он сможет перевести все ваши банковские накопления на свой счет, украсть ваши аккаунты и распространять через них спам или выпрашивать у ваших знакомых деньги. Добравшись до личной переписки, он способен вас шантажировать.

А если вы подключились к небезопасной сети с рабочего устройства, то коммерческая информация вашей компании также может оказаться в чужих руках. В отдельных случаях преступники могут даже незаметно заразить ваше устройство зловредом, который останется в нем и после отключения от опасного вайфая.



Материал взят с этого сайта

Дети в информационном обществе

Котов Денис

В современных условиях развития общества компьютер стал для ребенка и «другом», и «помощником», и даже «воспитателем», «учителем».

Не стоит думать, что Интернет – это безопасное место, в котором ваши дети могут чувствовать себя защищенными. Существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых школьников, представляющих для детей угрозу.

В связи с этим необходимо направить все усилия на защиту детей от информации, причиняющей вред их здоровью и развитию. Просвещение подрастающего поколения, знание ребенком элементарных правил отбора информации, а также умение ею пользоваться способствует развитию системы защиты прав детей. Зачастую дети принимают всё, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать степень достоверности информации и подлинность ее источников.

Материал взял

Что такое ПНП и как от него защититься?

Антонов Кирилл

ПНП – это **потенциально нежелательная программа**, часто устанавливаемая на компьютер при установке других программ. Как правило, ПНП выполняет роль маркетингового инструмента, часто **меняет настройки браузера** или отображает **нежелательную рекламу**. Самая распространенная форма ПНП – **рекламные программы**. Аббревиатура ПНП означает «потенциально нежелательная программа».

Как защититься от потенциально нежелательных программ:

1.**Осторожность при установке программ**.

2.**Здоровое недоверие**.

3.**Загрузка оригинальной версии**.

4.**Расширенная установка**. Всегда **отменяйте выбор установки дополнительных программ**.

Материал взят с этого сайта