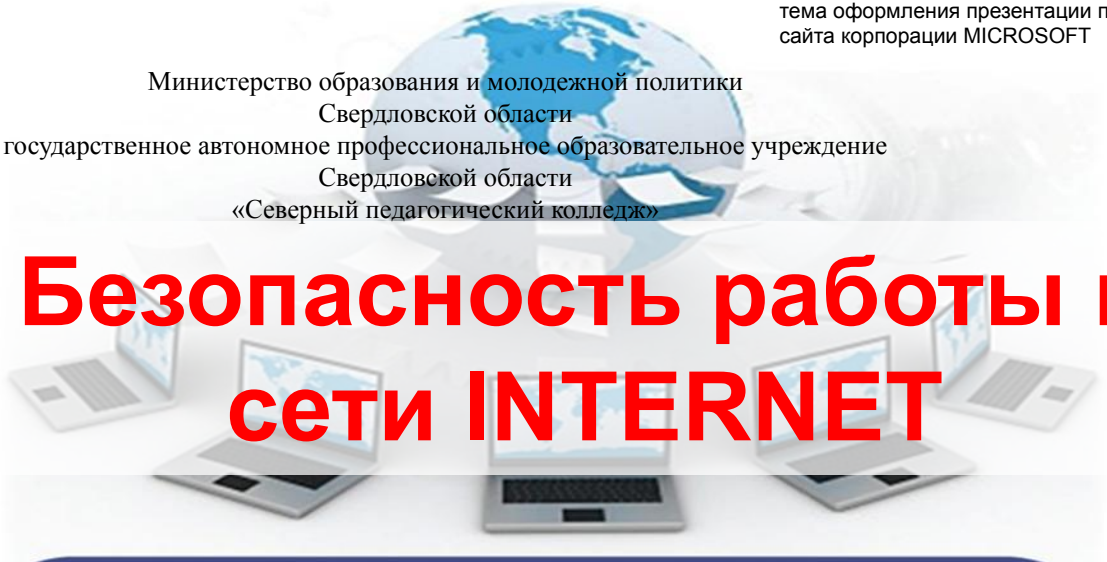
тема оформления презентации позаимствована с официального сайта корпорации MICROSOFT

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



Безопасность работы в сети INTERNET

Коллективная презентация
110 группы
февраль 2023

Что такое СПАМ и как с ним бороться?

Тутубалина Елизавета

Спам – это рассылка писем или сообщений в мессенджерах и социальных сетях без согласия пользователя. «Мусорные» сообщения раздражают потребителей и создают негативный образ компании. К спаму также относят рекламные или мошеннические звонки.

Как защититься от спама

Вот основные правила защиты от спама:

- Соблюдать режим «инкогнито» при посещении интернет-ресурсов.
- Не публиковать контакты на общедоступных сайтах.
- Читать условия обработки персональных данных перед заполнением форм обратной связи.
- Проверять чекбоксы с «галочками» в формах обратной связи, при регистрации на сайтах или в программах лояльности.
- Отзывать разрешения на обработку персональных данных у недобросовестных компаний – процесс отзыва компания описывает в политике обработки.
- Выбирать почтовые операторы с фильтрами спама – Яндекс, Gmail.
- Не отвечать на спам и не переходить по указанным в письме ссылкам.

Информация взята с этого сайта

Информация взята с этого сайта

Кто такие ХАКЕРЫ и как от них защититься?

Кинзибаева Юлия

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. 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.

Советы для защиты

- Попробуйте поискать в интернете свое имя или создать вторую учетную запись в социальной сети, чтобы понять, что из ваших данных видит посторонний человек. Если вам кажется, что личной информации слишком много, сделайте свои учетные записи приватными и проверьте, действительно ли вы знаете всех своих подписчиков.
- Избегайте простых паролей, которые можно вычислить методом подбора. Согласно опросу Tessian, 85% людей используют одни и те же кодовые слова для различных ресурсов. Разумеется, помнить разные пароли для каждого ресурса сложно, но с этим отлично справляются специальные приложения.
- Относитесь скептически как к личным, так и к рабочим письмам. Если текст вызывает подозрения, убедитесь, что адрес отправителя корректен. Спросите совета у ИТ-отдела вашей компании или подтвердите запрос устно у коллеги. Не переживайте о том, что можете кого-то побеспокоить. Безопасность важнее. Не торопитесь открывать сомнительные ссылки или вложения, тщательно проанализируйте ситуацию. Мошеннические электронные письма могут быть не такими очевидными, как раньше, но они обычно содержат множество малозаметных деталей, которые могут вас насторожить. Так что доверяйте своей интуиции.

материалы взяты

Что такое фишинг?

Игнатьева Виктория

Фи́шинг (англ. *phishing* от *fishing* «рыбная ловля, выуживание») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных 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 свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Материал взят

Почему нужно избегать знакомств в интернете?

Сатеева Ксения

1. Человек, с которым Вы общаетесь продолжительное время, может выдавать себя за совершенно другого. Он может разместить свои данные под чужими фотографиями с целью привлечь к себе внимание. А на встречу придет человек совершенно другой внешности. Для того чтобы этого избежать, необходимо попросить собеседника сделать селфи или поговорить с Вами по видеосвязи. Чем больше вы будете знать информации, тем меньше будет разочарований потом.
2. Человек может оказаться Интернет-мошенником. Нужно себе отдавать отчет, что человек про себя может рассказать что угодно. Нельзя слепо верить совершенно незнакомому Вам человеку.

Материал взят с сайта.

Изображение взято с сайта.

Чем опасна интернет- зависимость?

Загумённова Иришка

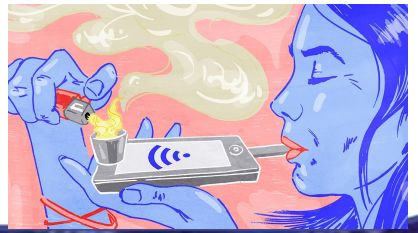
Интернет-зависимость – это *расстройство в психике, сопровождающееся большим количеством поведенческих проблем и в общем заключающееся в неспособности человека вовремя выйти из сети, а также в постоянном присутствии навязчивого желания туда войти.*

Чем опасна интернет-зависимость?

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.

Однако нарушение мыслительных процессов и ухудшение памяти - не единственные негативные влияние интернета на человека. Окунаясь с головой в сети всемирной паутины, человек постепенно утрачивает навыки реального общения, что приводит к некой асоциальности. Зачем встречаться с друзьями, когда можно поболтать с ними по Skype, зачем с кем-то договариваться в живую или созваниваться, если можно просто отправить письмо по e-mail, зачем искать и покупать товар в обычных магазинах, когда можно приобрести что угодно, не выходя из дома… То есть описанные ранее как преимущества, все эти удобства при длительном и безальтернативном их использовании превращаются в проблему.

Ссылка источника изображения



Чем опасны азартные игры в Internet?

Барышникова Анна

Азартные игры в сети повсеместно становятся зависимостью. Например, карточные игры на деньги. Известно, что далеко не все люди обладают сильной силой воли и могут вовремя сказать себе «Стоп!». Человек во чтобы то ни стало, хочет одержать победу, и на деле всё приводит к большим финансовым потерям. Вплоть до полного разорения.

Ещё один огромный минус азартных игр в сети интернет – 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.

Информация взята с сайта

Изображение взято с сайта

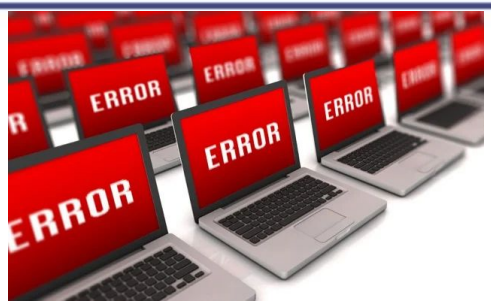
Антивирусная защита

Гузнякова Виктория

Для обеспечения своего функционирования вирусу достаточно лишь нескольких вполне обычных операций, используемых большинством обычных программ. Поэтому принципиально не может существовать универсальный метод, защищающий операционную систему от распространения любого вируса. Тем не менее, можно существенно затруднить задачу создания вируса, применяя специальные методы, как в самой ОС, так и используя дополнительные резидентные и нерезидентные средства защиты. Аппаратные средства защиты – это специальные платы, вставляемые в компьютер. Вместе с соответствующей резидентной программой такая плата аппаратно блокирует пути инфекции. Загрузка с дискеты происходит только по паролю, подозрительные действия с дискетами и винчестером блокируются и на экран выдаются предупреждающие сообщения.

Признаки “заражения” компьютера

Кошкина Александра



источник

1.Снижение производительности;
2.Приложения перестают работать;
3.Появляется множество всплывающих окон и сообщений о том, что компьютер заражён;
4. Вы не можете подключиться к Интернету или он работает слишком медленно;
5. При подключении к Интернету открываются различные окна, или браузер отображает страницы, которые вы не открывали;
6. Пропали файлы;
7. Антивирус исчез, а брандмауэр заблокирован;
8. Смена языка;
9. Потеря сохраненных файлов, программ, игр из компьютера;
10. Если компьютер действует сам по себе, система отправляет письма без вашего ведома, разные сайты открываются самостоятельно, то Ваш компьютер инфицирован.

источник

Защита авторских прав

Габитова Лиза

Материал взят с этого сайта

Защита авторских прав в интернете действует по умолчанию, как и в офлайне. Если автор не разрешал использование материалов, значит, это запрещено. При этом отсутствие прямого запрета не означает согласия.

Без чёткого разрешения автора запрещено использовать созданный им контент, а именно:

- Публиковать контент, вне зависимости будет ли это в общем или закрытом доступе.
- Использовать материалы для коммерческих и иных целей.
- Менять имя автора либо присваивать авторство.
- Изменять любым образом исходный материал.

Под изменениями подразумевают любую переработку — обрезку изображений, использование фрагментов видео, переработку текстов.

Материал всят с этого сайта

Какие данные относятся к персональным?

Панфилова Наталия

Информация взята с этого источника

Персональные данные - **любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу** (далее - субъект персональных данных) (фамилия, имя, отчество, год, месяц, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование)

Источник:http://www.consultant.ru/law/podborki/chto_otnositsya_k_personalnym_dannym_fizicheskogo_lica/

Как защитить персональные данные при общении в социальных сетях?

Никифорова Мария

- не используйте для регистрации на общедоступных ресурсах почту, которая связана с важными процессами (например, рабочими и финансовыми сервисами);
- устанавливайте разные пароли для каждого ресурса, избегайте классических комбинаций типа «12345»;
- для восстановления или подтверждения пароля используйте мобильный телефон, а не электронную почту;
- делитесь личной информацией в соцсетях осторожно;
- не добавляйте в друзья незнакомых людей и не переходите по всем ссылкам подряд;
- не публикуйте в соцсетях фотографии важных документов, не пересылайте такие документы через личные сообщения;
- не скачивайте предлагаемые вам через соцсети приложения, если не уверены в том, что это официальный продукт известной вам компании.
- обязательно подключайте двухфакторную аутентификацию там, где она реализована

Текст и изображение взяты с данного интернет-ресурса:
https://nris.ru/blog/zashita-v-socialnyh-setyah/

Каким образом злоумышленники могут получить доступ к вашему компьютеру?

Карякина Валерия

Фальшивая техподдержка

Вам поступает звонок, незнакомец обращается к вам по имени и представляется агентом поддержки крупной компании.

Откройте доступ, это полиция

Некоторые злоумышленники заходят еще дальше и представляются сотрудниками полиции, которым нужна помощь в поимке киберпреступников.

Мы из торговой комиссии (на самом деле нет)

Мошенники действуют не только угрозами — некоторые заманивают жертву в ловушку, обещая ей легкие деньги.

Источник:https://www.kaspersky.ru/blog/remote-access-scams/23061/

Что такое кибератака и как от нее уберечься?

Яровая Валерия

Кибератаки — это попытки получить несанкционированный доступ к компьютерным системам и украсть, изменить или уничтожить данные. Кибератаки направлены на получение контроля над важными документами и системами или их повреждение. Их целью могут стать корпоративные или личные компьютерные сети.

Чтобы уберечь себя от кибератак, нужно делать следующее:

- Регулярно обновляйте операционные системы устройств и мобильные приложения.
- 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.
- Проверяйте URL-адреса, прежде чем переходить по ссылкам, или переходите на веб-сайты напрямую.
- 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.
- Используйте VPN.
- Отключите геолокацию и закройте камеру на устройствах.

информация и картинка были взяты с этих сайтов

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

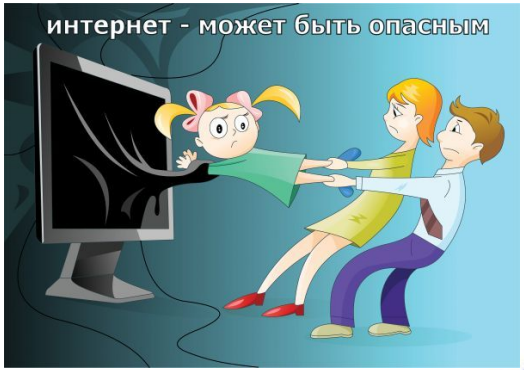
Волкова Алёна

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.

Информацию взяла

фото

ФОТО



Советы по безопасности при работе в Интернете

Сурикова Анастасия

1. Не заходите на подозрительные сайты и ссылки, полученные от незнакомых людей. Не нажимайте на всплывающую рекламу.
2. Используйте сложные пароли.
3. Не сообщайте свои данные посторонним.
4. При авторизации используйте экранную клавиатуру.
5. При использовании браузера установите специальные дополнения такие, как напри дополнение **Adblock Plus**. При использовании этого дополнения вы не увидите большую часть рекламы, том числе и вредоносную.
6. Проверяйте и контролируйте настройки антивируса и брандмауэра.
7. Не открывайте письма от неизвестных отправителей, и не загружайте прикрепленные к таким письмам файлы.
8. Помните о снижении безопасности при использовании беспроводного соединения в общественных местах.

Материал взят с этого сайта

Фото

Опасности использования сетей WI-FI

Каримова Милана

1. Подключение к общественным точкам Wi-Fi опасно для пользователей тем, что они рискуют потерять платежные данные, документы, логины, пароли и другую личную информацию.
2. Перед подключением к публичному Wi-Fi нужно тщательно изучить название точки доступа. Это связано с тем, что мошенники могут создать сеть с названием, похожим на Wi-Fi кафе или другого общественного заведения. Во время прогулок нужно отключать функцию автоматического подключения к Wi-Fi, чтобы не подключиться к сетям злоумышленников.
3. Нужно отказаться от использования банковских приложений или других важных сервисов посредством общественного Wi-Fi. При наличии необходимости лучше воспользоваться мобильным Интернетом. Отсутствие авторизации при подключении к общедоступной сети должно насторожить, так как это является нарушением и говорит о том, что она небезопасна.

Материал взят с этого сайта

Как сохранить деньги на банковском счете от злоумышленников?

Городиловой Софьи

Как обезопасить себя.

- В первую очередь перепроверяйте адрес сайта. Чаще всего официальные адреса страниц начинаются с защищенного соединения «https://». Обратите внимание на доменное имя. Фишинговые сайты, к примеру, могут оканчиваться на «.su» вместо «.ru». Само название сайта в адресе тоже порой написано немного иначе, например «ozoon.ru» вместо «ozon.ru».
- Всегда осматривайте устройство перед тем, как вставить карту: закреплен ли картоприемник, нет ли подозрительных накладок и модификаций на нем.
- Не переходить по ссылкам в сообщениях. Во-вторых, раз и навсегда запомнить: службы безопасности банков не имеют права запрашивать данные вашей карточки.
- 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.
- Помните, что самая важная информация о карте – трехзначный код CVC на оборотной стороне. Он позволяет совершать виртуальную идентификацию и покупать онлайн.
- Перепроверяйте интернет-страницы, на которых совершаете покупки. Официальные сайты защищены специальным шифрованием при вводе данных карточки.

Информация была взята с сайта:

Если Вас шантажируют или Вам угрожают через интернет...

Кутепова Илона

Если вас шантажируют: 4 советов, которые сохранят деньги и репутацию

В большинстве случаев за шантажом в интернете ничего не стоит: у мошенников нет задачи шантажировать лично вас. Вымогатели-любители не выбирают жертву специально. Некоторые могут отправлять по 15 сообщений разным жертвам с требованием заплатить. Если хоть кто-то заплатит — мошенник своего добился.

🤦 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

💳 Пожалуйтесь в банк

Если мошенник дал вам номер своей карты для перевода, вы можете пожаловаться на него в банк. Чтобы понять, какой у мошенника банк, достаточно набрать первые шесть цифр карты в сервисе переводов с карты на карту

🤐 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

Используемый источник:
https://journal.tinkoff.ru/short/ne-platite/

Источник информации