Презентация на тему: «Безопасность в Интернете»

Фейковые страницы

Фальсификация в Интернете

Наряду с обычными блогами существуют так называемые флоги и фэйковые блоги, а также виртуальные персонажи. Они создаются для публикации рекламных сообщений под видом личных впечатлений. В европейских странах, в частности в Великобритании, подобная деятельность наказуема, так как нарушает закон о защите прав потребителей.

Поскольку технология обработки фотографий идет вперед , в интернете всё чаще встречаются фото-фейки.

Фэйковыми (поддельными) могут быть также учетные записи, страницы или сайты с содержанием, похожим на основной сайт

Фейковые сайты

Мошенники создают копию главной страницы какого-нибудь известного сайта, затем всевозможными правдами и неправдами заставляют вас на нее зайти и ввести свои логин и пароль. Это называется фишинг (от английского слова fishing – рыбная ловля). Выудив таким образом ваши конфиденциальные данные, мошенники получают возможность авторизоваться уже на настоящем сайте и от вашего имени совершать там любые действия. Если это сайт, предназначенный для совершения онлайн платежей (например, сайт банка), то вы можете потерять все свои деньги.

Влияние компьютера на психику человека!

Проблемные Вопросы

Как влияет компьютер на психику человека, и как совместить здоровый образ жизни и работу на компьютере?

АКТУАЛЬНОСТЬ ТЕМЫ

В последние годы человечество столкнулось с глобальной компьютеризацией всех видов человеческой деятельности. Персональный компьютер стал нашим спутником и дома. Без компьютера не обходятся и дети.

ГИПОТЕЗА Сейчас прожить без компьютера практически невозможно. Интернет, чаты, форумы - эти слова давно и прочно вошли в нашу жизнь. Но вместе с ними в нашу жизнь вошли и такие новые понятия как «Интернет-зависимость», «игромания». Увеличилось число людей, больных «типично компьютерными» болезнями - ухудшением зрения, искривлением позвоночника и другими неприятными заболеваниями. Но всё же компьютер приносит не одни беды, иногда он очень помогает, и в своей защите я хочу показать «обе стороны медали»..

ЗАВИСИМОСТЬ ОТ СОВРЕМЕННЫХ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Главным образом выражается в двух основных формах: интернет - зависимость (интернет - аддикция) чрезмерная увлеченность компьютерными играми. Общими чертами компьютерной зависимости является характерный ряд психологических и физических симптомов, тесно связанных между собой:Психологические симптомы:хорошее самочувствие или эйфория за компьютером; невозможность остановиться; увеличение количества времени, проводимого за компьютером; пренебрежение семьей и друзьями; ощущения пустоты, депрессии, раздражения не за компьютером; ложь членам семьи о своей деятельности; проблемы с работой или учебой.Физические симптомы: синдром карпального канала сухость в глазах; головные боли по типу мигрени; боли в спине; нерегулярное питание, пропуск приемов пищи; пренебрежение личной гигиеной; расстройства сна, изменение режима сна.

ТЕРМИН «ИНТЕРНЕТ – ЗАВИСИМОСТЬ»

предложил доктор Айвен Голдберг в 1996 году для описания патологической, непреодолимой тяги к использованию Интернет. Он исходил из предположения о том, что у человека может развиваться психологическая зависимость не только от внешних факторов, но и от собственных действий и эмоций. Впервые научный подход к изучению феномена «интернет-зависисости» продемонстрировала Кимберли Янг в 1996 году, разместившая на одном из сайтов интернета оригинальный тест для выявления интернет-зависимых лиц. Согласно исследованиям Кимберли Янг опасными сигналами (предвестниками интернет зависимости) являются:навязчивое стремление постоянно проверять электронную почту; предвкушение следующего сеанса он-лайн; увеличение времени, проводимого он-лайн; увеличение количества денег, расходуемых он-лайн.

ЗАВИСИМОСТЬ ОТ КОМПЬЮТЕРНЫХ ИГР

игровые аддикты испытывают устойчивую потребность в игре. Аддикты постоянно находятся в состоянии сниженного настроения в реальном мире, что подтверждается высокой тревожностью и депрессией. Что происходит с ними во время игры более менее объективно выявить сложно, так как любое отвлечение от игры – это выход из виртуальной реальности. В процессе игры их настроение существенно улучшается, присутствуют положительные эмоции. Положительные эмоции, сопровождающиеся подъемом настроения, Но после игры, т. е. после выхода из виртуального мира настроение снова ухудшается, быстро возвращаясь на исходный уровень, оставаясь на нем до следующего «вхождения» в виртуальный мир.Большинство аддиктов – люди, имеющие ряд семейных проблем, проблемы на работе, учебе. Поэтому для игрового аддикта реальный мир скучен, неинтересен и полон опасностей. Вследствие этого человек пытается жить в другом мире – виртуальном, где все дозволено, где он устанавливает правила игры. Логично предположить, что выход из виртуальной реальности болезненен для аддикта – он вновь сталкивается с ненавистной для него реальностью, что и вызывает снижение настроения и активности, ощущение ухудшения самочувствия.

КОМПЬЮТЕРНЫЕ ИГРЫ, КАК БОЛЕУТОЛЯЮЩЕЕ СРЕДСТВО

Компьютерные игры, использующие технологию VR (виртуальная реальность), можно назначать детям с тяжелыми ожогами как дополнительное болеутоляющее средство, сообщает BBC News. Австралийские медики из госпиталя Аделаиды считают, что погружение в мир монстров и пришельцев помогает побороть боль у таких пациентов. Семи обожженным в возрасте от 5 до 18 лет предлагалось играть в VR-игры во время длительной процедуры смены повязок. При этом дети, которым давались и традиционные обезболивающие, гораздо легче переносили перевязку. В качестве "игрового" обезболивания использовались закрепленные на голове два миниатюрных компьютерных экрана и специальный сенсор, который позволял детям двигаться внутри виртуального мира и отстреливать монстров. Медики объясняют подобный эффект тем, что дети, переключаясь на переживания внутри игры, перестают концентрироваться на собственных болевых ощущениях. Исследователи считают, что можно подобрать игры, которые будут максимально эффективны в той или иной возрастной группе.

Компьютер-друг человека

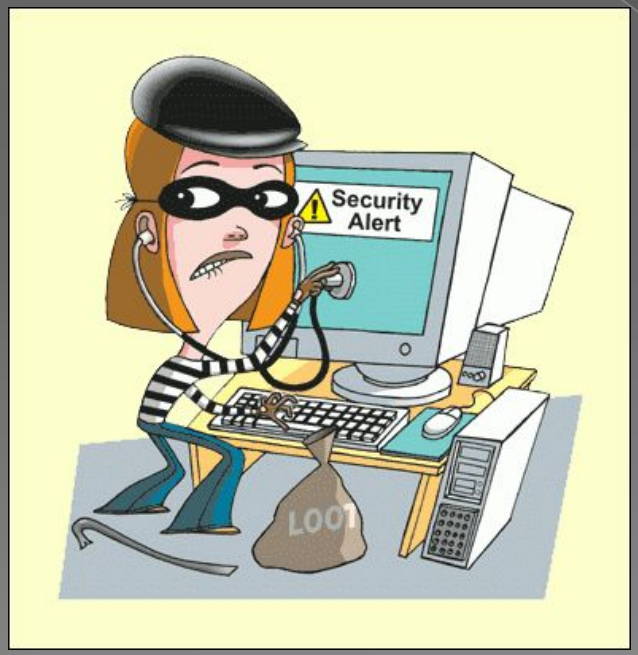
Компьютер может стать, как врагом воспитания и развития личности, так и лучшим помощником в этих процессах. Главное - уметь правильно пользоваться этим интеллектуально-психологическим инструментом XXI века. Поэтому нужно обратить внимание на обилие программ для школьников, которые предлагает сегодня индустрия програм -много обеспечения. А среди них много весьма полезных продуктов. Это, многочисленные и разнообразные словари и справочники, разнообразные электронные библиотеки, весьма полезными будут обучающие программы. Помимо общеобразовательных предметов, рынок программного обеспечения предлагает спектр программ, обучающих иностранным языкам, клавиатурные тренажеры. Как видите, компьютер может оказать немалую помощь. Главное - помнить и соблюдать простые правила работы за компьютером, и мы снизим отрицательный риск к минимуму: не проводить за компьютером более двух - трех часов в день, не исправлять самостоятельно неисправности, сидеть прямо и на расстоянии вытянутой руки от монитора, а после работы за компьютером делать простую зарядку для глаз.

Сигналы опасности

Сигналы опасности при работе за компьютером:

- навязчивое желание постоянно проверять электронную почту;
- предвкушение очередного сеанса он-лайн;
- увеличение времени, проводимого он-лайн;
- увеличение количества денег, расходуемых он-лайн.

«Способ противодействия интернет угрозам»



Уивинг

- ***Уивинг*** - одно из наиболее распространенных преступлений этого вида, связанное с кражей услуг, происходит в процессе "запутывания следов". Злоумышленник проходит через многочисленные системы и многочисленные телекоммуникационные сети - Интернет, системы сотовой и наземной телефонной связи, чтобы скрыть свое подлинное имя и местонахождение. При такой ситуации причиной проникновения в данный компьютер является намерение использовать его как средство для атаки на другие системы.
- Повреждение системы. Данная группа объединяет преступления, совершаемые с целью разрушить или изменить данные, являющиеся важными для владельца или многих пользователей системы - объекта несанкционированного доступа.
- Объектом подобных атак могут стать компьютеры, соединенные с Интернетом. Маршрутизаторы - компьютеры, определяющие путь, по которому пакеты информации перемещаются по Интернету - аналогичны телефонным коммутаторам и поэтому являются объектами для опытных хакеров, которые хотят нарушить или даже изменить маршрут "трафика" в сети.
- Использование вирусов. Применение данного средства повреждения компьютерных систем доступно в настоящее время не только профессиональным программистам, но и людям, обладающим лишь поверхностными познаниями в этой сфере. Во многом это обусловлено доступностью самих вредоносных программ и наличием простой технологии их создания.
- Особую опасность представляют злоупотребления, связанные с распространением вирусов через Интернет.

Методы манипуляции.

Сущность методов манипуляции состоит в подмене данных, которая осуществляется, как правило, при вводе/выводе данных. Это простейший и поэтому очень часто применяемый способ.

Вариантом подмены данных является подмена кода.

Рассмотрим некоторые конкретные методы:

Манипуляция с пультом управления. Манипуляция с пультом управления относится к злоупотреблению механическими элементами управления ЭВМ. Характеристика манипуляции с вычислительной техникой заключается в том, что в результате механического воздействия на технические средства машины создаются возможности манипуляции данными.

Некоторые из таких нарушений связаны с компьютерами телефонных

"*Троянский конь*"- способ, состоящий в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

Действия такого рода часто совершаются сотрудниками, которые стремятся отомстить за несправедливое, по их мнению, отношение к себе, либо оказать воздействие на администрацию предприятия с корыстной целью.

"*Логическая бомба*" - тайное встраивание в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

Методы обеспечения защиты информации

Препятствие - метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. п.).

Управление доступом - метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы предприятия.

Управление доступом включает следующие функции защиты:

1. · идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора);
2. · аутентификацию (установления подлинности) объекта или субъекта по предъявленному им идентификатору;
3. · проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
4. · регистрацию обращений к защищаемым ресурсам;
5. · реагирование (сигнализация, отключение, задержка работ, отказ в запросе при попытках несанкционированных действий).

Маскировка - метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия.

Регламентация - метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму.

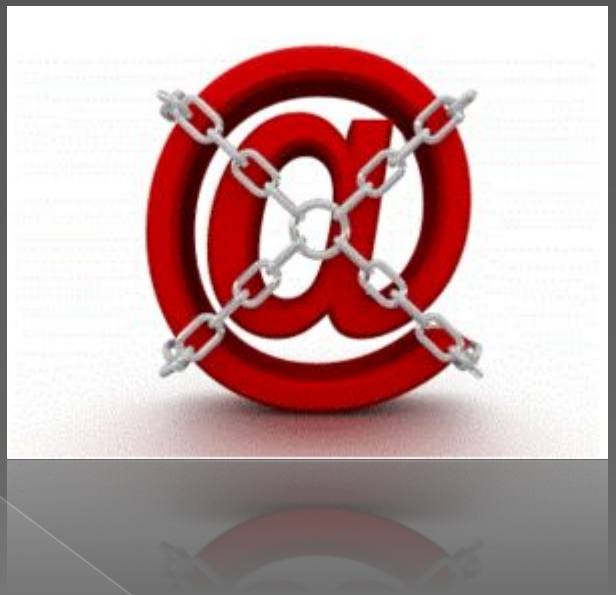
Принуждение - метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности.

Побуждение - метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.

Указанные выше методы обеспечения информационной безопасности реализуются с помощью следующих основных средств: физических, аппаратных, программных, аппаратно-программных, криптографических, организационных, законодательных и морально-этических.

Физические средства защиты предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.

Аппаратные средства защиты - это электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д.



Основные результаты тестирования современных антивирусов (в скобках - процент обнаруженных вирусов):

- Kaspersky Internet Security 2011 (100%)
- DrWeb Security Space 6.0 (99%)
- Online Solutions Security Suite 1.5 (97%)
- Outpost Security Suite Pro 2010 (97%)
- Norton Internet Security 2010 (91%)
- Avast! Internet Security 5.0 (91%)
- Comodo Internet Security 4.1 (89%)
- Avira Premium Security Suite 10.0 (88%)
- BitDefender Internet Security 2011 (86%)
- ZoneAlarm Internet Security Suite 2010 (86%)
- Eset Smart Security 4.2 (76%)
- Panda Internet Security 2011 (70%)
- G DATA Internet Security 2011 (70%)
- McAfee Internet Security 2010 (63%)
- AVG Internet Security 9.0 (59%)
- F-Secure Internet Security 2010 (57%)
- VBA32 Personal 3.12 (55%)
- Trend Micro Internet Security 2010 (50%)
- PC Tools Internet Security 2010 (49%)
- Microsoft Security Essentials 1.0 (29%)

Спасибо за внимание!!!