Федеральное государственное автономное образовательное учреждение
дополнительного профессионального образования «Академия повышения
квалификации и профессиональной
переподготовки работников образования»
(ФГАОУ АПК и ППРО)

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по организации и проведению в общеобразовательных организациях Российской Федерации тематического урока, посвященного Интернет безопасности детей

Разработчики:
Болотина Т.В., зав. кафедрой методики преподавания истории, социально-политического образования и права ФГАОУ АПК и ППРО, к.п.н.
Павлова С.А., старший преподаватель кафедры методики преподавания истории, социально-политического образования и права ФГАОУ АПК и ППРО.
Прутченков А.С., профессор кафедры методики преподавания истории, социально-политического образования и права ФГАОУ АПК и ППРО, д.п.н.

Москва
2015 г.

Аннотация

Данные методические рекомендации ориентированы на оказание методической помощи педагогам начального, основного общего, полного (среднего) общего образования по организации и проведению тематического урока, посвященного Интернет безопасности детей. В методических рекомендациях предлагаются концептуальные, содержательные, методические и технологические подходы к проведению урока в соответствии с возрастными особенностями детей.

Материалы методических рекомендаций также могут быть использованы для проведения по данной тематике: классного часа, урока-экскурсии или иного внеклассного занятия во внеурочной деятельности школьного педагога или в форме занятия в системе дополнительного образования.

Проблема обеспечения информационной безопасности детей в сети Интернет становится все более актуальной в связи с постоянным ростом несовершеннолетних пользователей. Число пользователей Интернета в России стремительно растет и молодеет, доля детской аудитории среди них очень велика. Для многих российских школьников Интернет становится информационной средой, без которой они не представляют себе жизнь. Вместе с тем, в Интернете содержатся огромные массивы информации, которая является запрещенной для детей, так как может нанести вред их физическому и психическому здоровью, духовному и нравственному развитию.

Согласно российскому законодательству информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию.[1]

Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет. Формирование навыков информационной безопасности должно осуществляться на уроках информатики, обществознания, права, ОБЖ и т.д. и во внеурочной деятельности. Этому вопросу должно быть уделено достаточное внимание в программе по воспитанию и социализации обучающихся, которая является частью

[1] Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

основной образовательной программы в соответствии с Федеральным государственным образовательным стандартом[2]. Знания об Интернет угрозах, умения различать и предотвращать их последствия, защитить от них себя и своих близких - способствуют социализации детей.

Достичь действенных результатов в обеспечении информационной грамотности и, как следствие, - безопасности детей невозможно без привлечения родителей. Часто родители не понимают и недооценивают угрозы, которым подвергается их ребенок, находясь в сети Интернет. С родителями необходимо вести постоянную разъяснительную работу, т.к. без понимания родителями данной проблемы невозможно ее устранить силами только образовательной организации, и тем более отдельного педагога. На родительских собраниях, лекториях, встречах со специалистами нужно знакомить их с видами существующих интернет угроз, рекомендациями по обеспечению безопасности ребенка в сети Интернет дома (в зоне ответственности родителей).

Поэтому эффективное обеспечение безопасности детей при работе в сети Интернет является задачей, которую могут и должны решать вместе школа и семья, причем школа инициирует и организует это сотрудничество, просвещая родителей и обучая своих учеников.

Цель данных рекомендаций – обеспечение методический поддержки педагогов, организующих и проводящих занятия по интернет безопасности детей путем привития им навыков ответственного и безопасного поведения в среде Интернет.

Пояснительная записка

30 октября 2014 во всех школах страны состоялся первый Единый урок безопасности в сети Интернет. Инициатором проведения урока стала временная комиссии Совета Федерации по развитию информационного общества. Данные методические рекомендации ориентированы на продолжение этой образовательной акции в 2015 году.

Материалы данных рекомендаций подготовлены в соответствии с категориями информационной продукции, которые зафиксированы Федеральным законом «О защите детей от информации, причиняющей вред их здоровью и развитию»:

[2] Федеральный государственный образовательный стандарт среднего (полного) образования. Приказ № 413 от 17 мая 2012 г., зарегистрирован Минюстом России 7.06.2012, рег. № 24480

- первый раздел «Детям 6+», что соответствует обучающимся начальной школы (1 - 4 классы);
- второй раздел «Подросткам 12+» - основная школа (5 - 7 и 8 - 9 классы);
- третий раздел «Молодежь 16+» - старшая школа (10 - 11 классы).

Цели подготовки методических рекомендаций:

- оказать методическую помощь педагогам-практикам в организации и проведения урока, посвященного интернет безопасности детей;

- помочь учителю в осмыслении роли интернета в современном образовании, обозначении проблемно-тематического поля и важнейших содержательных и сюжетных линий урока;

- помочь педагогам в отборе и систематизации необходимой информации к уроку, добываемой из различных источников;

- предложить школьным педагогам несколько вариантов проведения данного урока в соответствии с уровневой системой общего образования и возрастными особенностями детей в рамках того или иного уровня общего образования по соответствующим сюжетам;

- предложить учителю интересные подходы к методической, содержательной и технологической составляющей урока.

Цель проведения занятий - обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи:

1) информирование обучающихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;

2) информирование обучающихся о способах незаконного распространения такой информации в информационно-телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);

3) ознакомление обучающихся с международными принципами и нормами, с нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности несовершеннолетних;

4) обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде, то есть намеренное и регулярное причинение вреда: запугивание, унижение, травля, физический и психологический террор - одним человеком или группой людей другому человеку с использованием электронных форм контакта) и буллицид (доведение до самоубийства путем психологического насилия);

5) предупреждение совершения обучающимися правонарушений с использованием информационно-телекоммуникационных технологий.

Ожидаемый результат от использования данных методических рекомендаций:

- учитель получит возможность подготовить и провести урок, выделяя в нём содержательные блоки в зависимости от возрастных и психологических особенностей школьников, используя современные методические и технологические подходы;

- родители получают практические материалы, знакомство с которыми поможет им более грамотно организовать общение с детьми при обсуждении проблем, связанных с интернетом.

Основной ожидаемый результат - в **ходе уроков Интернет - безопасности обучающиеся должны научиться** делать более безопасным и полезным свое время пребывания в сети Интернет и иных информационно-телекоммуникационных сетях, а именно:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;

- 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 неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;

- распознавать манипулятивные техники, используемые при подаче рекламной и иной информации; критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;

- анализировать степень достоверности информации и подлинность ее источников; применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

Методические рекомендации

Формы работы с учащимися при проведении урока интернет безопасности могут быть самыми разнообразными, главное, чтобы они были увлекательными и эффективными, способствовали формированию навыков информационной безопасности, соответствовали возрасту учеников.

Первый раздел: начальная школа - 1 - 4 классы.

В рамках урока «Интернет-безопасность» в начальных классах целесообразно ознакомить обучающихся:

- с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи;

- как критически относиться к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, как отличить достоверные сведения от недостоверных, как избежать вредной и опасной для них информации, как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет;

- как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывания в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

Рекомендуется продемонстрировать возможности детских поисковых систем http://kids.quintura.ru, http://agakids.ru и детского браузера http://www.gogul.tv, а также познакомить с детскими социальными сетями:

- http://cyberpapa.ru/,
- http://interneshka.net/,
- http://kinderonline.ru/detskiy_portal.html,
- http://1dnevnik.ru/,
- http://www.detkino.ru.

Для отбора содержания урока могут быть использованы материалы сайта www.detionline.com (видеоматериалы, материалы электронного

журнала «Дети в информационном обществе», материалы Линии помощи), а также материалы других сайтов, содержащих информацию по безопасному использованию сети Интернет. Большое значение для эффективности урока Интернет-безопасности имеет не только содержание, но и форма его проведения.

Целесообразно использовать для 1-4 классов – урок-путешествие, урок-викторину, урок- соревнование, урок-игру, беседу.

Полезные ссылки:

1) http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/loputon_metsa.html – о правилах безопасного поведения в сети Интернет с элементами интерактива;

2) http://www.nachalka.com/node/948 - учебное видео «Как обнаружить ложь и остаться правдивым в Интернете»;

3) http://content-filtering.ru/aboutus/ - информационно-аналитический ресурс «Ваш личный Интернет».

В качестве примера приводим урок-сказку.

Сказка о золотых правилах безопасности в Интернет

Источники: 1. Методические рекомендации: Методика организации недели «Безопасность Интернет»./Авторы составители: Селиванова О. В., Иванова И. Ю., Примакова Е. А., Кривопалова И. В. - Тамбов, ИПКРО 2012.с. 35-37

2. Блог педагога-психолога Краснощековой Т.Н. - http://krasatatiana.blogspot.ru/2009/10/blog-post.html

В некотором царстве, Интернет - государстве жил-был Смайл-царевич-Тьютор-Королевич, который правил славным городом СоцОБРАЗом.

И была у него невеста– прекрасная Смайл-царевна-Он-лайн-Королевна, день и ночь проводившая в виртуальных забавах.

Сколько раз предупреждал еѐ царевич об опасностях, подстерегающих в сети, но не слушалась его невеста.

Не покладая рук трудился Смайл-царевич, возводя город СоцОБРАЗ, заботился об охране своих границ и обучая жителей города основам безопасности в Интернет-государстве.

И не заметил он, как Интернет- паутина всѐ-таки затянула Смайл-царевну в свои коварные сети.

Погоревал – да делать нечего: надо спасать невесту.

Собрал он рать королевскую- СоцОбразову – дружину дистанционную и организовал "Регату" премудрую.

Стали думать головы мудрые, как вызволить царевну из плена виртуального.

И придумали они «Семь золотых правил безопасного поведения в Интернет», сложили их в котомку Смайл-царевичу, и отправился он невесту искать.

Вышел на поисковую строку, кликнул по ссылкам поганым, а они тут как тут: сообщества Змея-искусителя-Горыныча, стрелялки Соловья-разбойника, товары заморские купцов шоповских, сети знакомств-зазывалок …

Как же найти-отыскать Смайл-царевну?

Крепко задумался Тьютор-королевич, надел щит антивирусный, взял в руки меч-кладенец кодовый, сел на коня богатырского и ступил в трясину непролазную.

Долго бродил он, отбиваясь от реклам зазывающих и спамов завлекающих.

И остановился на распутье игрища молодецкого трѐхуровневого, стал читать надпись на камне, мохом заросшим: на первый уровень попадѐшь – времени счѐт потеряешь, до второго уровня доберѐшься – от родных-близких отвернѐшься, а на третий пойдѐшь - имя своѐ забудешь.

И понял Смайл-царевич, что здесь надо искать невесту.

Взмахнул он своим мечом праведным и взломал код игрища страшного!

Выскользнула из сетей, разомкнувшихся Смайл - царевна, осенила себя паролем честным и бросилась в объятия своего суженого.

Обнял он свою невесту горемычную и протянул котомочку волшебную со словами поучительными: «Вот тебе оберег от козней виртуальных, свято соблюдай наказы безопасные!»

1. Всегда помни своѐ Интернет-королевское имя (E-mail, логин, пароли) и не кланяйся всем подряд (не регистрируйся везде без надобности)!

2. Не поддавайся ярким рекламам-указателям и не ходи тропками, путанными на подозрительные сайты: утопнуть в трясине можно!

3. Если пришло письмо о крупном выигрыше – это «обманная грамота»: просто так выиграть невозможно, а если хочешь зарабатывать пиастры, нужно участвовать в полезных обучающих проектах – в «Регате…», например,!

4. Чтобы не забыть тропинку назад и вернуться вовремя, бери с собой Клубок волшебный (заводи себе будильник, садясь за компьютер)!

5. Если хочешь дружить с другими царствами-государствами, изучай полезные сервисы: они помогут тебе построить «Мой королевский мир», свой царский блог, форум для глашатаев важных – друзей званных

6. Не забывай обновлять антивирусную программу – иначе вирус Серый Волк съест весь твой компьютер!

7. Не скачивай нелицензионные программные продукты – иначе пираты потопят твой корабль в бурных волнах Интернет!

Залилась совестливыми слезами дева красная, дала своему наречѐнному слово честное, что не будет пропадать в забавах виртуальных, а станет трудиться на благо народа города своего СоцОБРАЗа, сама начнѐт обучаться и помогать будет люду заблудшему и погрязшему в трясине сетевой.

И зажили они дружно и счастливо с мечтою расширить границы образовательные.

Второй раздел: основная школа (5 - 7 и 8 - 9 классы)

В ходе урока «Интернет-безопасность» в среднем звене целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве:

- Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (Закон определяет информационную безопасность детей как состояние защищѐнности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.);

- № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», (направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации,

способной развить в ребѐнке порочные наклонности, сформировать у ребѐнка искажѐнную картину мира и неправильные жизненные установки.)

Важно ознакомить обучающихся с адресами помощи в случае интернет- угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Возможны следующие формы проведения урока: урок - пресс-конференция, урок-викторина, урок-соревнование, урок-презентация проектов, урок-практикум, урок-встреча с системными администраторами и т.д.

Полезные ссылки:

1) http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma_rooma.html - молодѐжная история с элементами интерактива;

2) http://content-filtering.ru/aboutus - информационно-аналитический ресурс «Ваш личный Интернет»;

3) www.icensor.ru – Интернет-фильтр.

В качестве примера для учащихся 5-7 классов предлагается **урок - беседа «**10 правил безопасности в интернете».

В начале урока учащимся рекомендуется показать видео, где объясняются основные правила безопасности в интернете -

http://www.youtube.com/watch?v=wVDsCpYSpeo

Каждый современный человек, ежедневно проводит время в интернете. Но интернет — это не только источник информации и возможность общаться на расстояние, но и угроза компьютерной безопасности. Вы можете скачать из сети компьютерный вирус, Вашу учетную запись или адрес электронной почты, могут взломает злоумышленник.

Правила безопасности в интернете.

1) Используйте надежный пароль. Первое и главное правило сохранности Ваших данных, учетных записей, почтовой пересылки это надежный пароль! Много раз хакеры взламывали страницы в социальных сетях или почтовые адреса из-за того, что пользователь ставил простой пароль. Вы ведь не хотите, чтобы Ваши личную переписку узнал кто-то чужой? Используйте генератор паролей, чтобы получить надежный пароль.

Генератор паролей создается, чтобы помочь вам с придумыванием устойчивых к взлому и легко запоминающихся паролей.

Часто бывает: вы зарегистрировались где-нибудь, а там просят: «введите пароль». В спешке приходится вводить что-нибудь типа qwerty или

12345. Последствия могут быть фатальными для вашего аккаунта: при попытке взлома такие пароли проверяются в первую очередь. Чтобы этого не происходило, надо создавать сложный пароль, желательно состоящий из букв разного регистра и содержащий цифры и другие символы.
Для создания таких паролей существуют специальные программы. Но, на наш взгляд, гораздо легче набрать наш адрес и просто выбрать понравившийся пароль.

Советы:

- Выбирайте пароль посложнее, состоящий из символов разного регистра, с цифрами и для абсолютной надёжности - знаками препинания.

- Не используйте пароль, связанный с теми данными, которые могут быть о вас известны, например, ваше имя или дату рождения.

- Пароли, которые вы видите на экране создаются в реальном времени на вашем компьютере, поэтому исключена возможность перехвата пароля по сети. Разные посетители сайта видят разные пароли. Если вы зайдете на сайт второй раз, пароли будут другими.

- Вы можете выбрать пункт меню браузера "Файл|Сохранить как...", чтобы пользоваться генератором паролей в оффлайне.

- Генератор паролей полностью прозрачен: скачайте файл passwd.js, чтобы увидеть, как создается пароль, и убедиться в абсолютной надежности.
Источник- http://genpas.narod.ru/

2) Заходите в интернет с компьютера, на котором установлен фаервол или антивирус с фаерволом. Это в разы уменьшит вероятность поймать вирус или зайти на вредоносный сайт.

3) Заведите один основной почтовый адрес и придумайте к нему сложный пароль. При регистрации на форумах, в соц. сетях и прочих сервисах Вы будете указывать его. Это необходимо если Вы забудете пароль или имя пользователя. Ни в коем случае не говорите, никому свой пароль к почте, иначе злоумышленник сможет через вашу почту получить доступ ко всем сервисам и сайтам, на которых указан Ваш почтовый адрес.

4) Если Вы хотите скачать какой-то материал из интернета, на сайте где не нужна регистрация, но от Вас требуют ввести адрес своей электронной почты, то, скорее всего, на Ваш адрес будут высылать рекламу или спам. В таких случаях пользуйтесь одноразовыми почтовыми ящиками.

5) Скачивайте программы либо с официальных сайтов разработчиков. Не скачивайте программы с подозрительных сайтов или с файлообменников. Так Вы уменьшите риск скачать вирус вместо программы.

6) Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они не были. В лучшем случае, Вы поможете автору сайта получить деньги, а в худшем — получите вирус. Используйте плагины для браузеров, которые отключают рекламу на сайтах.

7) Если Вы работаете за компьютером, к которому имеют доступ другие люди (на роботе или в интернет кафе), не сохраняйте пароли в браузере. В противном случае, любой, кто имеет доступ к этому компьютеру, сможет зайти на сайт, используя Ваш пароль.

8) Не открывайте письма от неизвестных Вам пользователей (адресов). Или письма с оповещением о выигрыше в лотереи, в которой Вы просто не участвовали.

9) Не нажимайте на вплывающие окна, в которых написано, что Ваша учетная запись в социальной сети заблокирована. Это проделки злоумышленников! Если Вас вдруг заблокируют, Вы узнаете об этом, зайдя в эту социальную сеть, или администрация отправит Вам электронное письмо.

10) Периодическим меняйте пароли на самых важных сайтах. Так Вы уменьшите риск взлома вашего пароля.

Пользуясь этими правилами безопасности в интернете, Вы существенно уменьшите риск получить вирус на свой компьютер или потерять учетную запись на любимом сайте

Варианты работы с этой информацией.

1. Обсуждение и дополнение основных 10 правил.

Учащимся предлагается обсудить и дополнить эти основные правила с учетом уже имеющегося у них опыта работы в интернете.

2. **Рисуем инфографику**

Учащимся предлагается нарисовать плакат в стиле современной инфографики, где размещаются основные правила безопасной работы в интернет.

http://www.ligainternet.ru/encyclopedia-of-security/article.php?id=464

В качестве примера для учащихся 8-9 классов предлагается занятие

«Киберугрозы современности: главные правила их распознавания и предотвращения»

Форма занятия: семинар.

Цель: расширение знаний о киберугрозах, формирование навыков их распознавания и оценки рисков.

Возраст обучающихся: 8-9 класс.

План занятия:

1. Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете. Составление листовок «Правила защиты от киберугроз» (20 мин.);
2. Практикум «Опасность 419» (20 мин.);
3. Подведение итогов занятия (5 мин.).

Ход занятия.

Занятие начинается показом социального видеоролика «Безопасный интернет - детям!»[3]. После просмотра ролика учитель объявляет тему занятия и предлагает ученикам самим сформулировать цель занятия.

[3] http://www.youtube.com/watch?v=9uvNVZMdeIk&feature=player_embedded

1. Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете.

У каждого ученика на столе лежит чистый лист бумаги – заготовка листовки по безопасности в Интернете. Перед тем, как начать работать учитель объясняет, что по ходу обсуждения каждый ученик должен заполнять листовку правилами, которые ему кажутся необходимыми и важными. После того, завершения обсуждения, отдельные ученики зачитывают свои листовки, остальные могут добавлять правила. Листовки собираются после урока для того, чтобы их раздать ученикам других классов.

Учитель начинает обсуждение с вопроса к аудитории: «Что вы знаете об угрозах, которые исходят из Интернета?» Просит учеников перечислить опасности, которые могут угрожать человеку, его персональному компьютеру, мобильным устройствам. На доске фиксируются ответы учеников.

После короткого обсуждения учитель приводит данные «Лаборатории Касперского» За последний год 91% компаний, представители которых приняли участие в опросе, сталкивались с угрозами информационной безопасности. В России этот показатель еще выше – 96%. Более того, ситуация становится только хуже: почти половина участников исследования утверждает, что количество кибератак за этот период увеличилось.

Перечисляя киберугрозы, которые представляются им самыми значительными, большинство участников исследования во всем мире ставят на первое место вирусы, шпионское ПО и другие вредоносные программы (61%). Спам назвали источником угрозы 56% респондентов. Третье место (36%) заняли фишинговые атаки, за ними идут сбои, вызванные проникновением в корпоративную сеть (24%), и DDoS-атаки (19%)[4].

Таким образом, можно выделить 3 группы серьезных киберугроз:

1. Шпионское программное обеспечение и другие вредоносные программы;
2. Спамы;
3. Фишинговые атаки.

Обсуждение основных правил защиты от главных киберугроз. Все ответы детей записываются на доске.

При обсуждении внимание учеников обращается на то, откуда могут исходить опасность. На первом месте в этом списке стоят социальные сети.

---

[4] Доклад «Киберугрозы и информационная безопасность», сайт http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf

Хотя в последнее время стал распространенными атаки на компьютер через мобильные устройства памяти (флешки).

«Сегодня большинство вредоносных программ создаются либо для того, чтобы рассылать спам, либо для того, чтобы красть у пользователя важные данные.

Если данные действительно важные и дорогостоящие, то для их похищения злоумышленники специально разрабатывают троян, который гарантированно будет работать на компьютерах в той организации, откуда нужно украсть данные. Осуществить внедрение такого вредоносного ПО обычно гораздо проще не через интернет, а с помощью записанных на флэшках «троянов». Флэшки могут подбрасываться как в здание, где располагается организация, так и размещаться, скажем, на парковке рядом с ним, где их с большой долей вероятности наверняка найдёт именно сотрудник нужной организации. Поэтому если вы нашли на улице или в здании флэшку, не торопитесь радостно вставлять её в свой компьютер – лучше сначала отдайте системному администратору, который просканирует её и при необходимости обезвредит.

Бывают и более банальные, но не менее эффективные способы заразить компьютер недостаточно осторожного пользователя. Например, от знакомого по Skype Вам может прийти сообщение в духе «Посмотри, на этой фотографии он так похож на нашего друга (одноклассника)!», ну и, конечно, ссылка на саму эту фотографию. При переходе по ссылке фотография почему-то не открывается в браузере, а сохраняется на жесткий диск, но мало кто на это обращает внимание. Хотя они-то как раз и должны насторожить! В общем, когда «фото» не открывается, пользователь «входит» в папку с ним, и видит, что это не просто abcd.jpg, а abcd.jpg.scr, то есть, исполняемый файл, а его компьютер уже заражен вирусом».[5]

После обсуждения листовок на доске должен быть записаны основные правила защиты от киберугроз.

2. Практикум «Угроза 419».

Цель: формирование навыков распознавание спама в «нигерийских письмах».

[5] Дрозд А. Основные методы сетевых мошенников (ликбез). Материал с сайта http://www.securitylab.ru/blog/company/securityinform/90304.php

Одной из разновидностей спама являются «Нигерийские письма» или другое название «Угроза 419». «Нигерийские письма» - вид мошенничества, получивший наибольшее развитие с появлением спама. Называется так потому, что письма особое распространение получили в Нигерии, причем еще до распространения Интернета они распространялись по обычной почте, начиная с середины 1980 годов. С появлением интернета «Нигерийские письма» стали нарицательным понятием.

Как правило, у получателя письма просят помощь в многомиллионных операциях, обещая солидные проценты с сумм. Если получатель согласится, у него выманиваются всё большие суммы денег на сборы, взятки и т. д. В худших вариантах жертве предлагается полулегально прибыть в Нигерию, где его либо арестовывали за незаконное прибытие в страну и у него вымогаются деньги за освобождение, либо похищали с целью получения выкупа.

Мошенничество профессионально организовано: у мошенников есть офисы, работающий факс, часто мошенники связаны с правительственными организациями, и попытка получателя письма провести самостоятельное расследование не обнаруживает противоречий в легенде. Сделка подаётся как «безвредное» беловоротничковое преступление, что мешает жертве обратиться к властям. Разумеется, обещанных денег жертва в любом случае не получает: их просто не существует.

Спамеры оперативно реагируют на ситуацию в мире, отслеживая очаги нестабильности. Поэтому постоянно появляются новые разновидности «Нигерийских» писем — например, «кенийские» или «филиппинские». Во время войны в Ираке активно шли спамерские рассылки «иракского» спама.
Подавляющее большинство «нигерийского» спама идет на английском языке, но в 2004-2005 гг. спамеры взялись активно осваивать Рунет. Появился «нигерийский» спам на русском языке, эксплуатирующий горячие события российской политической жизни.

«Нигерийские письма» являются дидактическим инструментом для формирования навыков распознавания спама и фишинговых атак.

Учитель делит аудиторию на 4 группы. Каждой группе выдает конверт, в котором содержится образец «нигерийского письма» (см. Приложения) и задание:

1. Внимательно прочитайте текст письма.
2. Выделите в нем моменты, указывающие на то, что это спам.

3. Перечислите факты, указанные в письме, которые кажутся вам недостоверными, подозрительными.

После того, как группы выполнят задание, начинается коллективное обсуждение. Вопросы для обсуждения:

1. Как можно распознать «нигерийское письмо»?
2. Как вы думаете кто авторы «нигерийских писем»?
3. Какую цель преследуют авторы «нигерийских писем»?
4. Можно ли считать безвредными «нигерийские письма»?

Результаты работы группы представляет один ученик. Все остальные ученики могут задавать вопросы и высказывать свое мнение. Учитель на доске записывает главные особенности «Нигерийских писем», которые нашли ученики, дополняет, систематизирует.

Подведение итогов занятия.

Приложения.

Карточка 1.

«Меня зовут Бакаре Тунде, я брат первого нигерийского астронавта, майора ВВС Нигерии Абака Тунде. Мой брат стал первым африканским астронавтом, который отправился с секретной миссией на советскую станцию «Салют-6» в далеком 1979 году. Позднее он принял участие в полете советского «Союза Т-163» к секретной советской космической станции «Салют-8Т». В 1990 году, когда СССР пал, он как раз находился на станции. Все русские члены команды сумели вернуться на землю, однако моему брату не хватило в корабле места. С тех пор и до сегодняшнего дня он вынужден находиться на орбите, и лишь редкие грузовые корабли «Прогресс» снабжают его необходимым.

Несмотря ни на что мой брат не теряет присутствия духа, однако жаждет вернуться домой, в родную Нигерию. За те долгие годы, что он провел в космосе, его постепенно накапливающаяся заработная плата составила 15 000 000 американских долларов. В настоящий момент данная сумма хранится в банке в Лагосе. Если нам удастся получить доступ к деньгам, мы сможем оплатить Роскосмосу требуемую сумму и организовать для моего брата рейс на Землю. Запрашиваемая Роскосмосом сумма равняется 3 000 000 американских долларов. Однако для получения суммы нам необходима ваша помощь, поскольку нам, нигерийским госслужащим, запрещены все операции с иностранными счетами.

Вечно ваш,

доктор Бакаре Тунде,

ведущий специалист по астронавтике».

Карточка 2.

«Дорогой друг, Я послан к вам по поводу моего покойного клиента, фамилия которого совпадает с вашим. Хотя мы еще не встречались друг с другом и раньше, но я верю, что судьба свела нас на ссылке на purpose.It будет лучше, мы утверждаем, и использовать деньги, чем позволить Ecobank топ-чиновников делиться и отвлекать его в своих соответствующих частных счетов, как заброшенный месторождения. Если закон не мог по конституции банка предоставить их должностными лицами право на наследование месторождения умершего клиента, вы и у меня больше прав, потому что умерший может быть ваш дальний родственник, так как он является гражданином вашей страны.

Прежде всего, я работал на него в течение многих лет, поэтому я верю, что он будет счастлив с нашим расположением, чтобы претендовать на фонд особенно когда противоположное состояние деньги незнакомым выступает в подобных старший staffs.You Ecobank, должны понимать, что в финансовые возможности учреждения, подобные этой, общей, но не слышал. Люди вкладывают свои деньги в финансовые институты и некоторые из этих счетов являются либо закодированы или конфиденциально ссылка на operated.Normally, когда нечто подобное происходит в финансовом учреждении, сообщается в управлении. Он не опубликованы и соответствующие финансовые учреждения только информирует адвокат своего клиента в зависимости от обстоятельств может быть и ждет реальный наследник, чтобы показать. По истечении указанного периода определяется банком получателя, чтобы придумать, руководство отправляет деньги своим «долгом Re-преобразования Департамента и закрытия счета.

Теперь вопрос в том, кто управляет «Долг Re-преобразования Департамента", а кто управления? Ответ прост: они председателей, управляющих директоров и членов Правления. Эти люди разделили деньги, и никто не задает вопросы. На самом деле, такой вопрос даже не обсуждается вне заседаний совета директоров. Если мое расположение обращаюсь к вам, и я получить ваше согласие работать в качестве партнеров в передаче фонда, я буду начинать с необходимой правовой процесс, как покойный адвокат. В сущности, мне нужно будет быть

предоставлена информация ниже, так что я могу начать с правовой процесс создания ближайших родственников с умершим;

1. Ваше полное имя

2. Возраст

3. Адрес

4. Частная Телефон

5. Профессия

6. Национальность

7. Другой адрес электронной почты ссылка на yahoo.com, ссылка на hotmail.com.

После этого, я должен подготовить и отправить Вам образцы письмо-заявку, которая будет представлена в банке, положив претендовать на его балансе US $ 10,500,000.00. Фонд может быть оплачен на банковский счет, вы будете назначать в установленном порядке или по видам чек кассира обращается в ваше имя и пользу.

Хотя трудно точно оценить время, которое потребуется, чтобы заключить этот вопрос, но я уверен, что весь процесс не займет до 10 рабочих дней с момента вы официально обратиться с банком transfer.I фонда " м предлагается 40% от общего фонда как вознаграждение за вашу помощь, моя будет составлять 50%, и мы будем дарить 9% (US $ 945 000) для благотворительной организации нашего выбора в то время как 1% (US $ 105,000) будет установлена в сторону, с учетом всех прочих расходов, которые могут возникнуть в процессе transfer.I фонда надеемся, что вы оцените это предложение, как я взял многие вещи во внимание, прежде чем предлагать такое соотношение обмена.

Наконец, я хочу, чтобы вы знали, что я столкнулся с трудностями, пытаясь отправить это письмо к вам, как простой сообщении. Именно поэтому я прикрепил его. Поэтому мой скромный совет, который вы открываете новый адрес электронной почты либо в ссылка на hotmail.com, ссылка на yahoo.com и ссылка на Gmail.com содействовать нашей электронной корреспонденции. Вы также можете связаться со мной через номер +22890945333.

С наилучшими пожеланиями,

Г-н Джонсон Slami Esq.»

Карточка 3.

«Уважаемый Добрый день! Я юрист, г-н Карл Алекс Хендерсон. Юрист в семье покойного президента Мусу Yaradua, мне было поручено семья в поисках хорошей инвестицией в вашей стране, предпочтительно недвижимость, я должен был обеспечивать конфиденциальность и доверие в этой сделке, так что вы находитесь в лучшем положении, знать больше, чем меня на этом инвестиции.

Деньги наличными $ 25,2 млн., Муса Yaradua семей хотят инвестировать эти деньги в вашу страну с вашей поддержкой, и мы обнаружили, что этот план, чтобы переместить его с помощью дипломатических средств.

Пожалуйста, это очень конфиденциальная и совершенно секретной, я буду лететь вниз, чтобы посмотреть вам в лицо подписывать документы, необходимые для инвестиций, как только вы получите фонд.

Мы предлагаем 10% от общей суммы за вашу помощь в этом проекте, в то время как 5% будет использоваться для любых непредвиденных расходов, которые могут возникнуть при переводе средств.

Я с нетерпением жду вашего ответа на это письмо.

Если вы примете мое предложение, я хотел бы иметь следующую информацию ниже, чтобы начать процесс.

1. Ваше полное имя:

2. Ваш номер телефона:

3. Ваш возраст:

4. Ваш пол:

5. Род занятий:

6. Вашей страны:

С уважением,

Адвокат г-н Карл Алекс Хендерсон

Сотовые +2348020574082

факс +23417641464»

Карточка 4.

«From: Prince Joe Eboh

Date: Wednesday, April 21, 2004 12:53 PM

Subject: TRANSFER

Принц Джо Эбох

Уважаемый господин, /госпожа,

Надеюсь, что это послание найдет Вас в хорошем здравии. Я - Принц Джо Эбох, Председатель "Комитета заключения контрактов", "Нигерийской Комиссии Развития Дельты (NDDC)", являющейся филиалом нигерийской Национальной Нефтяной Корпорации (NNPC).

Нигерийская Комиссия Развития Дельты (NDDC) была создана покойным Главой государства, генералом Сани Абача, который умер 18-ого июня 1998 года, для управления прибылью, образующейся от продаж нефти и ее субпродуктов.

Предполагаемый ежегодный доход на 1999 год составил свыше 45 миллиардов долларов США, сведения об этом содержаться в отчете Генерального аудитора Федеративной республики Нигерия (FMF A26 ONE 3B Параграф "D") за ноябрь 1999 года.

Я - Председатель Комитета заключения контрактов, и мой комитет исключительно ответственен за то, как и куда должны распределяться денежные средства. Во всех случаях мы действуем от имени Федерального правительства Нигерии. Мой Комитет заключает контракты с иностранными подрядчиками для разработки нефтяных месторождений в районе дельты Нигера.

Так случилось, что в одном из контрактов нам удалось сэкономить US$25,000,000. Но, из-за существования некоторых внутренних законов, запрещающих государственным служащим в Нигерии открытие иностранных счетов, мы не имеем возможности перевести эти деньги за границу.

Однако, эти деньги US$25,000, 000 могут быть оформлены в форме оплаты иностранному подрядчику, поэтому мы хотели бы использовать ваш счет в банке как держателя бенефициария фонда. Мы также достигли соглашения, о том, что Вам будет предоставлена награда за содействие в этой операции в размере 20 % полной суммы, переданной как нашему иностранному партнеру, в то время как 5 % будут сохранены на непредвиденные расходы, которые обе стороны понесут в ходе реализации этой сделки, а остаток в 75 % будет сохранен для членов комитета.

Если Вы решите принять наши условия, Вы должны послать мне немедленно детали вашего счета или открыть новый счет в банке, куда мы сможем осуществить перевод денег в сумме US$25,000, 000, держателем которой вы будете, до тех пор, пока мы не прибудем в вашу страну за нашей долей. Для нас не важно, каким бизнесом вы занимаетесь.

Все, что нам необходимо, это название вашей компании, ваш личный номер телефона / факса, полное имя, адрес и детали вашего счета в банке, на который будет осуществлен перевод через Apex Bank .
Отметьте, что эта сделка, как ожидается, должна будет реализована в пределах 21 рабочего дня со дня, когда мы предоставим все необходимые сведения Федеральному Министерству финансов, которое одобрит необходимое валютное распределение для перемещения этих средств на ваш счет. Пожалуйста, рассматривайте вышесказанное как конфиденциальные сведения.
Прошу Вас ответить мне как можно скорее.
Спасибо за ваше сотрудничество. Искренне ваш, Принц Джо Эбох»

Подведение итогов занятия.
Занятие завершается ответом на вопрос «Как и для чего нужно знать основные правила безопасной работы в Интернете?».
Для подготовки и проведения занятий по безопасной работе детей в Интернете рекомендуем использовать материалы журнала для педагогов, психологов и родителей «Дети в информационном обществе», который издается Фондом Развития Интернет (http://detionline.com).

Третий раздел: старшая школа (10 - 11 классы).

В рамках урока «Интернет-безопасность» в старших классах целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве (см. рекомендации для проведения урока Интернет–безопасности в среднем звене).

Необходимо обратить внимание обучающихся на классификацию вредоносных информационных ресурсов:
- информация, причиняющая вред здоровью и (или) развитию детей;
- информация, запрещенная для распространения среди детей;
- информация, ограниченная для распространения среди детей определенных возрастных категорий.

На уроке необходимо затронуть следующие аспекты:
- перечень рисков, подстерегающих ребенка в сети Интернет;
- рекомендации по грамотному использованию электронной почты;
- технологии безопасного общения в средах мгновенного обмена сообщениями.

Необходимо обеспечить обучающихся:

- инструкциями по безопасному общению в чатах;
- советами по профилактике и преодолению Интернет- зависимости;
- общими правилами по безопасности детей в сети Интернет.

Также рекомендуется рассмотреть следующие объекты, являющиеся опасными в Интернете:

- нежелательные программы;
- защита личных данных;
- мошенничество;
- виртуальные «друзья»;
- пиратство;
- on-line-игры;
- этика;
- критический подход к информации.

Важно обеспечить обучающихся информацией о программном обеспечении, позволяющим осуществлять безопасную работу в сети Интернет, контентной фильтрации, а также ознакомить с адресами помощи в случае интернет- угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Возможные формы проведения урока в 9-11 классах – лекция, деловая игра, урок-презентация проектов, мозговой штурм «Интернет-безопасность», дискуссия, дебаты, встреча со специалистами медиа-сферы, системными администраторами и т.д.

Полезные ссылки:

1) http://www.kaspersky.ru – антивирус «Лаборатория Касперского»;
2) http://www.onlandia.org.ua/rus/ - безопасная web-зона;
3) http://www.interneshka.net – международный онлайн-конкурс по безопасному использованию Интернета;
4) http://www.saferinternet.ru – портал Российского Оргкомитета по безопасному использованию Интернета;
5) http://content-filtering.ru – Интернет СМИ «Ваш личный Интернет»;
6) http://www.rgdb.ru – Российская государственная детская библиотека.

Для **учащихся старших классов средней школы будет** актуальным урок с использованием кейс-технологии.

Кейс «Новый смартфон для отца»

Илья Комаров, студент 4-го курса экономического факультета, вернулся домой после сдачи последнего экзамена зимней сессии. Экзамен был сдан на «отлично», и настроение у Ильи было соответствующим. Тем более что на телефон пришло сообщение от банка о начисление первой заработной платы от крупной энергетической компании, где он проходил стажировку.

Особенно его обрадовало начисление обещанной премии в размере 15000 рублей. Теперь у Ильи наконец-то появились деньги для покупки подарка ко дню рождения отца.

Выбирать подарок Илье не пришлось, недавно у его отца, Петра Петровича Комарова, сломался телефон. Вирусное приложение не только «съело» все деньги со счета отца, но и безвозвратно повредило операционную систему старенького смартфона. Илья однозначно решил подарить отцу новый смартфон.

Он привычным движением открыл ноутбук и начал изучать предложения различных магазинов, сравнивая цены и параметры предлагаемых моделей.

Полчаса поисков в интернете привели Илью на сайт интернет-магазина, предлагающего современные устройства по низкой цене.

Информация с сайта интернет-магазина:

1. ***Интернет адрес:*** http://i-crop.ru/
2. ***Указанный адрес:*** г. Калининград.
3. ***Происхождение товара:*** таможенный конфискат.
4. ***Цены на товары:*** на 50% меньше рыночных.
5. ***Способ оплаты:*** кошелек QIWI.
6. ***Сроки доставки:*** от 1-го до 20-ти дней.
7. ***Гарантии:*** Опись вложения содержимого бандероли.

Характеристика роли в ситуации. Представьте себя на месте советника по личной информационной безопасности, к которому обратился Илья Комаров.

Постановка задачи. Помогите Илье оценить безопасность покупки в данном интернет-магазине. Ответьте на поставленные вопросы:

1. Какая представленная информация вызывает доверие у потенциального клиента?
2. Выделите незнакомые понятия, которые присутствуют в тексте, и дайте им определение.
3. Какая информация на сайте не вызывает вашего доверия?

4. Каким образом можно проверить добросовестность интернет-магазина? Перечислите как можно больше способов.
5. Какой совет вы бы дали Илье Комарову?

За дополнительной информацией вы можете обратиться на сайт или в приложение к кейсу (см. ниже).

Приложение

О магазине. *Мы находимся в г. Калининград и успешно работаем с 2005 года! Аппараты были изъяты у различных фирм и предпринимателей при попытке контрабандного ввоза в Россию, без уплаты таможенной пошлины и соответствующих налогов. Как правило, предприниматели, желающие сэкономить на уплате налогов, пытаются провезти контейнеры со смартфонами и планшетами под видом радиодеталей или радиоэлектронного лома, на которые таможенная пошлина на ввоз существенно ниже, чем на мобильные телефоны и планшетные компьютеры. Наша цель - максимально быстро реализовать товар, поэтому мы устанавливаем столь доступные цены.*

Вся продукция - оригинальная, от официальных производителей. Техника поставляется из США и Европы. Мы не продаем китайские подделки. На весь товар предоставляется гарантия 1 год. Гарантийное обслуживание обеспечивают официальные сервисные центры на территории РФ. Все телефоны русифицированы. Комплектация полная (заводская).

Мы всегда отправляем заказы своим клиентам посылкой с описью вложения содержимого. В этом случае сотрудники почты обязаны в Вашем присутствии вскрыть посылку до оплаты наложенного платежа, чтобы сверить содержимое посылки с описью. Таким образом, Вы сможете убедиться, что в посылке действительно находится мобильный телефон или планшетный компьютер надлежащего качества. Перед отправкой посылки заказчику, товар проверяется на отсутствие дефектов или брака. Данные условия гарантируют отсутствие в изделии дефектов и удовлетворяют законным требованиям Потребителя в течении гарантийного срока с момента передачи товара потребителю».

Доставка и оплата. *Доставка осуществляется Почтой России или курьером службы экспресс-доставки DHL по всей территории РФ и СНГ. Самовывоза нет. Оплата только через QIWI кошелек (VISA QIWI Wallet). СПОСОБЫ ДОСТАВКИ:*

1. Доставка курьером экспресс-почты DHL: 1-3 дня (только при условии полной предоплаты заказа).

2. Доставка бандеролью наложенным платежом: 7-20 дней (требуется оплата гарантийного взноса 500 рублей).*

**Гарантийный взнос - это обязательное и неоспоримое условие, которое гарантирует серьезность Вашего намерения приобрести товар. Сумма гарантийного взноса не зависит от модели телефона или планшетного компьютера и составляет 500 рублей за каждую единицу товара. Доставка по России и СНГ - бесплатно. Экспресс-доставка курьером DHL также осуществляется бесплатно, но только после полной предоплаты заказа.*

ОПЛАТА ЧЕРЕЗ QIWI КОШЕЛЕК:

1. Зарегистрируйтесь на сайте QIWI кошелька "VISA QIWI Wallet" (используйте тот же номер телефона, который укажете в заказе).

2. Пополните счет QIWI кошелька на сумму равную стоимости заказа или гарантийный взнос 500 рублей (см. способы пополнения).

3. На сайте WWW.QIWI.COM войдите в свой кошелек и выберите ПЕРЕВЕСТИ -> ПО E-MAIL.

4. В форме перевода укажите сумму, равную стоимости заказа или гарантийный взнос 500 рублей и e-mail platezh@i-crop.ru. Оплатите.

5. Сообщите на наш e-mail (info@i-crop.ru) номер заказа, номер Вашего телефона, сумму платежа, дату и время перевода.

6. Заказ будет отправлен на следующий день. Мы сообщим Вам трек-номер для отслеживания посылки.

Пополнить QIWI кошелек можно через QIWI терминалы, банковской картой, со счета мобильного телефона и многими другими способами.

Если Вы выбрали способ "доставка наложенным платежом", то при получении посылки Вас попросят оплатить наложенный платеж в кассе почтового отделения.

Для чего требуется гарантийный взнос: это вынужденная мера с нашей стороны, поскольку у нас часто бывают случаи, когда заказчик, по независящим от нас причинам, не является на почту и не выкупает посылку с заказом, в результате чего нам приходится платить за пересылку посылки в оба конца + почтовый сбор за хранение посылки на почте сверх установленного срока. В связи с этим, чтобы избежать лишних финансовых потерь, мы просим Вас оплатить гарантийный взнос. Схема здесь действует следующая: если Вы не являетесь на почту и не выкупаете посылку, то сумма гарантийного взноса покрывает наши расходы,

затраченные на пересылку товара в оба конца. Никакого перерасхода с Вашей стороны не будет, так как при отправке заказа сумма гарантийного взноса вычитается из его стоимости. Просим Вас с пониманием отнестись к данным условиям.

Материалы для учителя по обсуждению кейса

Какая информация призвана вызвать доверие у клиента:

Срок существования магазина

Указанная информация призвана вызывать доверие к магазину у покупателей. Однако написать на сайте все что угодно. Поэтому подобной информации не следует доверять.

Что такое Русификация?

Русифика́ция в информатике - приспособление аппаратного и программного обеспечения к работе с русским языком; переход на использование русского языка в интерфейсе компьютеров и компьютеризованной бытовой техники.

Самое интересное что одним из признаков контрабандного товара(которым якобы торгуют владельцы магазина) является отсутствие русификации. А если заводская(лицензионная) русификация на оборудовании все таки произведена значит оборудование уже на заводе планировалось поставлять в Россию. Тогда как он мог стать контрабандным?

Не знакомые понятия:

Что такое QIWI КОШЕЛЕК?

Электронная платежная система QIWI кошелек создана в 2006 году. С помощью QIWI кошелька можно не только оплачивать услуги связи, но и покупки в интернет магазинах. Сам по себе QIWI кошелек безопасен. Вызывает подозрение то, что интернет магазин работает ТОЛЬКО С QIWI КОШЕЛЬКОМ!!!

Что такое ТАМОЖЕННЫЙ КОНФИСКАТ?

Понятно, что это импортный товар, который прошел через таможню.

Но вот словом "конфискат" обычно в русском языке означают что-то конфискованное. По закону, всё конфискованное на таможне храниться до решения суда. А после вынесения решения суда конфискованный (без слова таможенный) товар либо продают (безопасный товар) либо сжигают (небезопасный товар).

Что такое Наложный платеж?

Нало́женный платёж — денежная сумма, которую почта взыскивает по поручению отправителя с адресата при вручении последнему почтового

отправления, и которая пересылается отправителю (или указанному им лицу) почтовым или телеграфным переводом.

Т.е. вы оплачиваете свою покупку на почте, когда забираете товар. А почтовые работники отправляют полученные средства продавцу. Наложный платеж является одним из самых безопасных способов оплаты интернет-покупки. Особенно если производится Опись содержимого посылки.

Трек-номер (Почтовый идентификатор)

При помощи почтового идентификатора, возможно, узнать о местонахождении и состоянии почтового отправления.

Добросовестные продавцы действительно отправляют своим клиентам Трек-номера, которые позволяют следить за доставкой.

Мошенники всегда стараются вызвать доверие мнимой прозрачностью своей деятельности.

Что такое ОПИСЬ ВЛОЖЕНИЯ БАНДЕРОЛИ?

Опись вложения – это бланк утвержденной формы, который заполняет отправитель. В бланке перечисляются все вложения, каждому вложению присваивается оценочная стоимость. Опись вложения защищает от воровства на ПОЧТЕ. А значит гарантией честности магазина быть не может.

Информация, не вызывающая доверия:

Отсутствие полного юридического адреса.

Мошенники всегда стараются скрыть свою личность. Если на сайте нет указания юридического адреса продавца. То скорее всего владельцы сайта мошенники. И в том случае если ваша покупка не будет вам доставлена вы даже не сможете написать заявление в правоохранительные органы.

Гарантийный платеж

Тревожный признак. Согласитесь, странно получается, с одной стороны продавец уверяет что товар вам понравиться, и он надлежащего качества, с другой он боится, что вы откажетесь от доставленного товара. Эти 500 рублей мошенники оставят себе, и конечно же никакого товара вы не получите.

Полная предоплата как обязательное условие

Тревожный признак. Полная предоплата, тем более проведенная переводом с QIWI кошелька, фактически означает что вы просто подарили мошенникам деньги. Достойные доверия интернет-магазины не работают по такой схеме.

Отсутствие самовывоза

Тревожный признак. Скорее всего, у мошенников нет даже офиса. Работают и отвечают клиентам из интернет-кафе или с домашнего компьютера.

Перевод через QIWI кошелек по электронному адресу

Тревожный признак. E-mail нельзя отследить, и соответственно очень сложно установить личность продавца.

Для проверки добросовестности магазина можно предпринять следующие действия:

1. Проверить отзывы о магазине на форумах. Если отзывы отрицательные воздержитесь от покупки.
2. Проверить входит ли магазин в черный список на сайте: http://www.stop-list.ru/spisok/nedobrosovestnyy-internet-magazin. Если магазин входит в черный список воздержитесь от покупки
3. Проверить срок регистрации сайта (с помощью сервиса http://r01.ru/domain/whois/) Если срок регистрации домена очень мал и не соответствует заявленному сроку существования интернет-магазина. Воздержитесь от покупки.
4. Проанализируйте всю открытую информацию. Найдите все незнакомые понятия и узнайте, что они значат.

Совет Илье Комарову:

Воздержаться от покупки. Приобрести телефон в надежном интернет-магазине.

При подготовке урока, посвященного интернет безопасности школьников, можно использовать следующие материалы:

1. Электронные ресурсы по теме «Безопасный Интернет»

1. http://www.saferinternet.ru/ - Безопасный Интернет. Портал Российского Оргкомитета по проведению Года Безопасного Интернета. Мероприятия, Интернет и законодательство, проблемы и решения, международные ресурсы;
2. http://www.saferunet.ru/ - Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Интернет-угрозы и эффективное противодействием им в отношении пользователей;
3. http://www.fid.su/ - Фонд развития Интернет. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета;
4. http://www.microsoft.com/Rus/athome/security/kids/etusivu.html - Безопасность в Интернете. "Основы безопасности детей и молодежи в

Интернете" — интерактивный курс по Интерент-безопасности, предлагаемый российским офисом Microsoft в рамках глобальных инициатив Microsoft "Безопасность детей в Интернете" и "Партнерство в образовании". В разделе для учащихся (7-16 лет) предлагается изучить проблемы информационной безопасности посредством рассказов в картинках. В разделе для родителей и учителей содержится обновленная информация о том, как сделать Интернет для детей более безопасным, а также изложены проблемы компьютерной безопасности;

5. http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=cs_teach_kids – Club Symantec единый источник сведений о безопасности в Интернете. Статья для родителей «Расскажите детям о безопасности в Интернете». Информация о средствах родительского контроля;

6. http://www.nachalka.com/bezopasnost - Nachalka.com предназначен для учителей, родителей, детей, имеющих отношение к начальной школе. Статья «Безопасность детей в Интернете». Советы учителям и родителям;

7. http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html - Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным;

8. http://www.ifap.ru/library/book099.pdf - «Безопасность детей в Интернете», компания Microsoft. Информация для родителей: памятки, советы, рекомендации;

9. http://www.interneshka.net/children/index.phtml - «Интернешка» - детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному использованию сети Интернет;

10. http://www.oszone.net/6213/ - OS.zone.net - Компьютерный информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль»;

11. http://www.rgdb.ru/innocuous-internet - Российская государственная детская библиотека. Ресурс для детей и родителей. Правила безопасного Интернета. Обзор программных продуктов для безопасного Интернета. Как защититься от Интернет-угроз. Ссылки на электронные ресурсы, информирующие об опасностях и защите в Сети;

12. https://www.google.ru/safetycenter/families/start/basics/ - Центр безопасности. Краткие рекомендации помогут обеспечить безопасность членов семьи в Интернете, даже если вечно не хватает времени;

13. https://ege.yandex.ru/security/ - Тесты по безопасности;
14. http://www.slideshare.net/shperk/ss-47136465 - Безопасность в Интернете. Анатолий Шперх;
15. http://shperk.ru/v-seti/prokrustovo-lozhe.html - Прокрустово ложе для информационной картины. Как мы читаем тексты в интернете;
16. http://shperk.ru/sovety/avtoritet.html - Как отличить фейк от настоящего материала? Дело о летающем дьяке Крякутном;
17. http://habrahabr.ru/company/mailru/blog/252091/ - Советы по безопасности.

Приложение

Материал для проведений родительского собрания, родительского лектория, заседания родительского клуба «Основные правила защиты наших детей от Интернет опасностей»

Интернет постепенно проникает в каждую организацию, общественное и учебное учреждение, в наши дома. Число пользователей Интернета в России стремительно растет и молодеет, доля молодежи и совсем юной аудитории среди пользователей Всемирной сети очень велика. Для многих из них, он становится информационной средой, без которой они не представляют себе жизнь. Вместе с тем, в Интернете содержатся огромные массивы информации, которая является запрещенной для детей, так как может нанести вред их физическому и психическому здоровью, духовному и нравственному развитию.

Согласно ст. 5 Федерального Закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», к информации, запрещенной для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера.

Для защиты детей от опасностей в Интернете необходима активная позиция родителей. И, это не удивительно: ведь в Интернете можно найти информацию для реферата или доклада, послушать любимую мелодию,

проверить свои знания в интернет конкурсах или on-line тестированиях, купить понравившуюся книгу или обсудить горячую тему на многочисленных форумах.

Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна: в ней появилась своя преступность, хулиганство, вредительство и прочие малоприятные явления. Виртуальность общения предоставляет людям с недобрыми намерениями дополнительные возможности причинить вред детям. В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания.

Взрослым нужно помнить о существовании подобных угроз и уделять повышенное внимание вопросу обеспечения безопасности детей в Интернете.

Правило 1.

Установите вместе с детьми четкие правила посещения сайтов. Определите, какие сайты они могут посещать, какие – посещать нельзя. Выберите сайты, которые можно посещать вашему ребенку, и заблокируйте доступ к неподходящим материалам. Настройте параметры безопасности вашего компьютера.

Правило 2.

Помогите детям выбрать правильное регистрационное имя и пароль. Убедитесь в том, что они не содержат никакой личной информации.

Правило 3.

Объясните детям необходимость защиты их конфиденциальности в сети Интернет. Настаивайте на том, чтобы они никогда не выдавали своего адреса, номера телефона или другой личной информации; например, места учебы или любимого места для прогулки.

Правило 4.

Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу. Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг, кибербуллинг и др.). Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В

некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы. Специалисты используют специальный термин «груминг», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.
Предупреждение груминга: Будьте в курсе, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются.

Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать интернет-знакомым свои фотографии. Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу. Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу; Интересуйтесь тем, куда и с кем ходит ваш ребенок.
Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство, социальное бойкотирование с помощью различных интернет-сервисов. Предупреждение кибербуллинга: Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать. Научите детей правильно реагировать на обидные слова или действия других пользователей. Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз. Старайтесь следить за тем, что Ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

На что следует обращать внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:

1) Беспокойное поведение. Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим

поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.

2) Неприязнь к Интернету. Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.

3) Нервозность при получении новых сообщений. Негативная реакция ребенка на звук электронного письма должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Правило 5.

Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

Правило 6.

Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование и использование чужой работы – текста, музыки, компьютерных игр и других программ – является кражей.

Правило 7.

Обращайте внимание, сколько времени проводят ваши дети в Интернете, чтобы вовремя заметить признаки возникающей интернет-зависимости. Предвестниками «интернет-зависимости» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство») являются: навязчивое стремление постоянно проверять электронную почту; предвкушение следующего сеанса онлайн; увеличение времени, проводимого онлайн; увеличение количества денег, расходуемых онлайн. Если Вы считаете, что ваши дети, страдают от чрезмерной увлеченности компьютером, что наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь.

Например, на сайте «Всероссийская Линия помощи «Дети онлайн» http://detionline.com/ открыта линия телефонного и онлайн-консультирования, которая оказывает психологическую и информационную поддержку детям и подросткам, столкнувшимся с различными проблемами в Интернете. На

линии помощи «Дети Онлайн», созданной в 2009 г., работают психологи Фонда Развития Интернет и выпускники факультета психологии МГУ имени М.В. Ломоносова, которые оказывают психологическую и информационную помощь по проблемам безопасного использования Интернета. Целевая аудитория — дети, подростки, родители и работники образовательных и воспитательных учреждений.

Служба Линия помощи «Дети Онлайн» включена в базу единого федерального номера телефона доверия для детей, подростков и их родителей. Обратиться на Линию помощи можно по телефону 8-800-25-000-15, бесплатно позвонив из любой точки страны, либо по электронной почте: helpline@detionline.com. Звонки принимаются в рабочие дни с 9.00 до 18.00 по московскому времени.

Контролируйте деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и с какой целью. Однако открытое, честное общение всегда предпочтительнее вторжения в личную жизнь.

Поощряйте детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми. Если ваш ребенок ведет интернет дневник, регулярно посещайте его. Будьте внимательны к вашим детям! Помните, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются дети за компьютером.

Приложение

Обеспечение безопасности детей при работе в Интернет

(Сайт «Информация для всех» http://www.ifap.ru)

Безмалый В.Ф.
MVP in Windows Security
Vladimir_Bezmaly@ec.bms-consulting.com
http://vladbez.spaces.live.com

Сегодня все больше и больше компьютеров подключаются к работе в сети Интернет. При этом все большее распространение получает подключение по высокоскоростным каналам, как на работе, так и дома. Все большее количество детей получает возможность работать в Интернет. Но вместе с тем все острее встает проблема обеспечения безопасности наших детей в Интернет. Так как изначально Интернет развивался вне какого-либо контроля, то теперь он представляет собой огромное количество информации, причем далеко не всегда безопасной. В связи с этим и с тем, что

возраст, в котором человек начинает работать с Интернет, становится все моложе, возникает проблема обеспечения безопасности детей. А кто им может в этом помочь, если не их родители и взрослые? Следует понимать, что, подключаясь к Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Объяснить ему это обязаны родители перед тем, как разрешить ему выход в Интернет.

Какие угрозы встречаются наиболее часто? Прежде всего:

• **Угроза заражения вредоносным ПО**. Ведь для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.

• **Доступ к нежелательному содержимому**. Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые материалы. А это насилие, наркотики порнография, страницы подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна содержащие любую информацию, чаще всего порнографического характера;

• **Контакты с незнакомыми людьми с помощью чатов** или электронной почты. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи;

• **Неконтролируемые покупки.** Несмотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.

Именно обеспечению безопасности наших детей при пребывании в сети Интернет и будет посвящена наша статья. Интернет — это прекрасное место для общения, обучения и отдыха. Но стоит понимать, что, как и наш реальный мир, всемирная паутина так же может быть весьма и весьма опасна.

Приведем несколько рекомендаций, с помощью которых посещение Интернет может стать менее опасным для ваших детей:

1. Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернет;

2. Объясните детям, что если в Интернет что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством;

3. Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа Skype, WhatsApp, Viber, Microsoft Messenger и т.д.), использовании он-лайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации;

4. Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.;

5. Объясните своему ребенку, что в реальной жизни и в Интернет нет разницы между неправильными и правильными поступками;

6. Научите ваших детей уважать собеседников в Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни;

7. Скажите им, что никогда не стоит встречаться с друзьями из Интернет. Ведь люди могут оказаться совсем не теми, за кого себя выдают;

8. Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернет– правда. Приучите их спрашивать о том, в чем они не уверены;

9. Не забывайте контролировать детей в Интернет с помощью специального программного обеспечения. Это поможет вам отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает. Как научить детей отличать правду ото лжи в Интернет?

Следует объяснить детям, что нужно критически относиться к полученным из Интернет материалам, ведь опубликовать информацию в

Интернет может абсолютно любой человек. Объясните ребенку, что сегодня практически каждый человек может создать свой сайт и при этом никто не будет контролировать, насколько правдива размещенная там информация. Научите ребенка проверять все то, что он видит в Интернет. Как это объяснить ребенку?

- Начните, когда ваш ребенок еще достаточно мал. Ведь сегодня даже дошкольники уже успешно используют сеть Интернет, а значит нужно как можно раньше научить их отделять правду от лжи;
- Не забывайте спрашивать ребенка об увиденном в Интернет. Например, начните с расспросов, для чего служит тот или иной сайт.
- Убедитесь, что ваш ребенок может самостоятельно проверить прочитанную в Интернет информацию по другим источникам (по другим сайтам, газетам или журналам). Приучите вашего ребенка советоваться с вами. Не отмахивайтесь от их детских проблем.
- Поощряйте ваших детей использовать различные источники, такие как библиотеки или подарите им энциклопедию на диске, например, «Энциклопедию Кирилла и Мефодия» или Microsoft Encarta. Это поможет научить вашего ребенка использовать сторонние источники информации;
- Научите ребенка пользоваться поиском в Интернет. Покажите, как использовать различные поисковые машины для осуществления поиска;
- Объясните вашим детям, что такое расизм, фашизм, межнациональная и религиозная вражда. Несмотря на то, что некоторые подобные материалы можно заблокировать с помощью специальных программных фильтров, не стоит надеяться на то, что вам удастся отфильтровать все подобные сайты.

Семейное соглашение о работе в Интернет

Если ваши дети хотят посещать Интернет, вам следует выработать вместе с ними соглашение по использованию Интернет. Учтите, что в нем вы должны однозначно описать права и обязанности каждого члена вашей семьи. Не забудьте четко сформулировать ответы на следующие вопросы:

- Какие сайты могут посещать ваши дети и что они могут там делать;
- Сколько времени дети могут проводить в Интернет;
- Что делать, если ваших детей что-то беспокоит при посещении Интернет;
- Как защитить личные данные;
- Как следить за безопасностью;
- Как вести себя вежливо;

• Как пользоваться чатами, группами новостей и службами мгновенных сообщений.

Не забудьте, что формально составленное соглашение не будет выполняться! Регулярно, по мере необходимости, вносите изменения в данное соглашение. Не забывайте, что вы должны проверять выполнение соглашения вашими детьми.

Научите вашего ребенка использовать службу мгновенных сообщений

При использовании службы мгновенных сообщений напомните вашему ребенку некоторые несложные правила безопасности:

• Никогда не заполняйте графы, относящиеся к личным данным, ведь просмотреть их может каждый;

• Никогда не разговаривайте в Интернет с незнакомыми людьми;

• Регулярно проверяйте список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются;

• Внимательно проверяйте запросы на включение в список новых друзей. Помните, что в Интернете человек может оказаться не тем, за кого он себя выдает;

• Не следует использовать систему мгновенных сообщений для распространения слухов или сплетен. Родителям не стоит надеяться на тайную слежку за службами мгновенных сообщений, которыми пользуются дети. Гораздо проще использовать доброжелательные отношения свашими детьми.

Может ли ваш ребенок стать интернет-зависимым?

Не забывайте, что Интернет — это замечательное средство общения, особенно для стеснительных, испытывающих сложности в общении детей. Ведь ни возраст, ни внешность, ни физические данные здесь не имеют ни малейшего значения. Однако этот путь ведет к формированию Интернет-зависимости. Осознать данную проблему весьма сложно до тех пор, пока она не становится очень серьезной. Да и кроме того, факт наличия такой болезни как Интернет-зависимость не всегда признается. Что же делать? Установите правила использования домашнего компьютера и постарайтесь найти разумный баланс между нахождением в Интернет и физической нагрузкой вашего ребенка. Кроме того, добейтесь того, чтобы компьютер стоял не в детской комнате, а в комнате взрослых. В конце-концов, посмотрите на себя, не слишком ли много времени вы проводите в Интернет.

Советы по безопасности для детей разного возраста

Как показали исследования, проводимые в сети Интернет, наиболее растущим сегментом пользователей Интернет являются дошкольники.
В этом возрасте взрослые будут играть определяющую роль в обучении детей безопасному использованию Интернет.

Что могут делать дети в возрасте 5-6 лет?

Для детей такого возраста характерен положительный взгляд на мир. Они гордятся своим умением читать и считать, а также любят делиться своими идеями. Несмотря на то, что дети в этом возрасте очень способны в использовании игр и работе с мышью, все же они сильно зависят от вас при поиске детских сайтов. Как им помочь делать это безопасно?

• В таком возрасте желательно работать в Интернет только в присутствии родителей;

• Обязательно объясните вашему ребенку, что общение в Интернет – это не реальная жизнь, а своего рода игра. При этом постарайтесь направить его усилия на познание мира;

• Добавьте детские сайты в раздел Избранное. Создайте там папку для сайтов, которые посещают ваши дети;

• Используйте специальные детские поисковые машины, типа MSN Kids Search (http://search.msn.com/kids/default.aspx?FORM=YCHM);

• Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;

• Научите вашего ребенка никогда не выдавать в Интернет информацию о себе и своей семье;

• Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.

Ваши дети растут, а, следовательно, меняются их интересы.

Возраст от 7 до 8 лет

Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей. В результате, находясь в Интернет ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому в данном возрасте особенно полезны будут те отчеты, которые вам предоставит Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системе Windows Vista).

В результате, у вашего ребенка не будет ощущения, что вы глядите ему через плечо на экран, однако, вы будете по-прежнему знать, какие сайты посещает ваш ребенок. Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернет. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.

По поводу использования электронной почты хотелось бы заметить, что в данном возрасте рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку. Помочь вам запретить ребенку использовать внешние бесплатные ящики сможет такое программное обеспечение, как Kaspersky Internet Security версии 7.0 со встроенным родительским контролем.

Что можно посоветовать в плане безопасности в таком возрасте?

• Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения;

• Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;

• Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь;

• Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый «белый» список Интернет с помощью средств Родительского контроля. Как это сделать, мы поговорим позднее;

• Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;

• Используйте специальные детские поисковые машины, типа MSN Kids Search (http://search.msn.com/kids/default.aspx?FORM=YCHM);

• Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;

• Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса;

• Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО;

• Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей;
• Научите детей не загружать файлы, программы или музыку без вашего согласия;
• Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы. Подробнее о таких фильтрах http://www.microsoft.com/rus/athome/security/email/fightspam.mspx;
• Не разрешайте детям использовать службы мгновенного обмена сообщениями;
• В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией;
• Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни;
• Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых»;
• Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Дети с 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности в этом возрасте:

• Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения;
• Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;
• Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь;
• Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;

• Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;
• Не забывайте беседовать с детьми об их друзьях в Интернет;
• Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет;
• Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними;
• Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет;
• Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение;
• Создайте вашему ребенку ограниченную учетную запись для работы на компьютере;
• Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях;
• Расскажите детям о порнографии в Интернет;
• Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами;
• Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Подростки с 13 до 17 лет

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо боле чувствительны к сексуальным домогательствам в Интернет.

Что посоветовать в этом возрасте?

• Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет1, руководство по общению в Интернет (в том числе в чатах);

• Компьютер с подключением к Интернет должен находиться в общей комнате. Часы работы в Интернет могут быть легко настроены при помощи средств Родительского контроля Kaspersky Internet Security 7.0

• Не забывайте беседовать с детьми об их друзьях в Интернет, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями чтобы убедиться, что эти люди им знакомы.

• Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

• Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование моделируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

• Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из Интернет.

• Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.

• Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

• Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих

угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

• Расскажите детям о порнографии в Интернет.

• Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

• Приучите себя знакомиться с сайтами, которые посещают подростки.

• Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

• Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что по закону дети не могут играть в эти игры. Обеспечивать родительский контроль в Интернет можно с помощью различного программного обеспечения.

Рекомендации Центра безопасности

Наши краткие рекомендации помогут вам обеспечить безопасность членов вашей семьи в Интернете, даже если вам вечно не хватает времени.

1. **Поговорите с ребенком о безопасности в Интернете**. Объясните основные правила, возможности различных технологий и последствия нарушений. Самое главное: убедите ребенка, что в любой непонятной или пугающей ситуации ему следует обращаться к родителям, чтобы найти безопасное решение.

2. **Используйте компьютер и смартфон вместе с детьми**. Это хороший способ научить их правилам безопасности в Интернете. При этом дети поймут, что решать возможные проблемы лучше всего вместе.

3. **Расскажите детям больше о сайтах и сервисах в Интернете.** Поговорите о том, что их интересует в Интернете и какие страницы им можно посещать.

4. **Безопасные пароли**. Помогите своей семье приобрести правильные привычки в отношении паролей. Расскажите об их использовании. Напомните, что пароли никому нельзя передавать, за исключением лиц, которым можно доверять, например, родителям. Убедитесь, что у детей вошло в привычку выходить из своих аккаунтов, когда они используют общественные компьютеры в школе, кафе или библиотеке.

5. **Используйте настройки конфиденциальности и управления доступом**. В Интернете немало сайтов, на которых можно публиковать свои комментарии, фото и видео, рассказывать о том, что с вами произошло, как

вы живете и т. д. Обычно такие сервисы позволяют определить уровень доступа к вашей информации ещё до ее публикации. Поговорите с членами своей семьи и определите, о чем не следует рассказывать всем. Научите детей уважать конфиденциальность друзей и родных.

6. **Проверьте возрастные ограничения**. Многие онлайн-сервисы, в том числе Google, предоставляют доступ ко всем функциям только совершеннолетним. А создавать аккаунты Google могут только пользователи не моложе 13 лет. Прежде чем ваш ребенок зарегистрируется на том или ином сайте, самостоятельно проверяйте условия его использования и соответствие материалов правилам, принятым в вашей семье.

7. **Научите детей ответственному поведению в Интернете**. Помните золотое правило: то, что вы не сказали бы человеку в личном общении, не стоит отправлять ему по SMS, электронной почте, в чате или комментариях на его странице. Поговорите с детьми о том, как другие могут воспринимать их слова, и разработайте для своей семьи правила общения.

8. **Посоветуйтесь с другими взрослыми**. Привлеките к обсуждению этой темы друзей, родственников и педагогов. Другие родители и специалисты по работе с детьми могут оказать вам неоценимую помощь в том, как научить детей и родственников правильному использованию самых разных информационных технологий.

9. **Защитите свой компьютер и личные данные**. Используйте антивирусное программное обеспечение и регулярно его обновляйте. Поговорите со своей семьей о типах личной информации – например, номер социального страхования, номер телефона или домашний адрес – эти данные не должны быть размещены в Интернете. Научите свою семью не принимать файлы или открывать вложения в электронной почте от неизвестных людей.

10. **Не останавливайтесь на достигнутом**. Безопасность в Интернете требует постоянного внимания, поскольку технологии непрерывно совершенствуются. Старайтесь всё время держать руку на пульсе. Пересматривайте правила пользования Интернетом в семье, следите за тем, как ваши близкие осваивают новые технологии, и время от времени давайте им советы.

Если вы нуждаетесь в консультации специалиста по вопросам безопасного использования Интернета или если ваш ребенок уже столкнулся с рисками в Сети, обратитесь «Всероссийская Линия помощи «Дети онлайн» по телефону: 8 800 25 000 15 (звонок по России бесплатный). На линии помощи профессиональную психологическую и информационную

поддержку оказывают психологи факультета психологии МГУ имени М.В.Ломоносова и Фонда Развития Интернет.
https://www.google.ru/safetycenter/families/start/basics/

Советы о безопасности детей в Интернете от Григория Остера

Посмотрите и обсудите с детьми образовательное видео, в котором Григорий Остер, Тутта Ларсен, Светлана Журова, Григорий Гладков и Ева Христенко делятся своим опытом о том, как научить ребенка правилам безопасности в Интернете и сделать его опыт в Сети полезным и позитивным.

https://www.youtube.com/watch?t=67&v=jhjnTT5KmEI

Больше информации - в Справочнике семейной безопасности Google.