День Знаний 1 сентября 2011 года,
Всероссийский урок медиа-безопасности

Р.Р.Хусаинов, учитель истории и права
МБОУ Щёлковской гимназии
Щёлковского муниципального района
Московской области

Актуальность:

В связи с нарастающим глобальным процессом активного формирования и широкомасштабного использования информационных ресурсов особое значение приобретает информационная безопасность детей. Просвещение подрастающего поколения в части использования различных информационных ресурсов, знание элементарных правил отбора и использования информации способствует развитию системы защиты прав детей в информационной среде, сохранению здоровья и нормальному развитию. В ходе проведения данного мероприятия обучающиеся должны не только получить необходимый минимум знаний об информационной безопасности, но и высказать свою точку зрения на указанную проблематику.

Медиаобразование выполняет важную функцию защиты от противоправного и манипулятивного воздействия средств массовой коммуникации, а также способствует предупреждению криминальных посягательств на детей с использованием информационно-телекоммуникационных сетей.

Задачи:

Во время Дня медиа-безопасности следует 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 выкладывать в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

Ход урока

Ученица (Мешкова Майя) читает стихотворение.

Э. Успенский

Не ходите ночью,
Дети, в Интернет.
Ничего хорошего
В Интернете нет.

Там увидеть можно
Тётю голышом.
Что потом твориться
Будет с малышом!?

Там повсюду бегают

Монстры с автоматом
И со страшной силой
Стреляют по ребятам.

Страшные чудовища
Обитают там
И за малолетками
Мчаться по пятам.

Там на днях открылась
Чёрная дыра.
И четыре школьника
Сгинули вчера.

Не ходите, дети,
Ночью в Интернет:
Вдруг на вас с экрана
Выскочит скелет!
Он ужасный, он не струсит,
Он вам что-нибудь откусит.
И, копаясь в челюстях,
На своих пойдет костях.

Там увидеть можно
Злого паука -
Он тогда ребёнка
Съест наверняка.
Он огромными когтями
Вас запутает сетями.
Будут косточки хрустеть,
Но придётся потерпеть.
И повиснут в паутинке
Лишь трусишки да ботинки.

И имейте в виду, проказники,
Есть опасный сайт «Одноклассники» -
Все, кто туда попадают
На несколько лет пропадают.

Пусть мои нотации
Вам надоедают -
Но дети в Интернете
Часто пропадают.
Многие дети
Пропали в интернете.

Медиапространство, медиатехника, медиаугроза, медиабезопасность. В первую очередь уясним, что такое «медиа», а потом уже и поговорим о пространстве, технике, угрозе и безопасности.

Медиа (мн. ч. от лат. *medium* – промежуточное, посредствующее, посредник) – средства осуществления коммуникации между различными группами, индивидуумами и (или) доставки любых содержательных продуктов аудитории.

Новые цифровые коммуникации раскрывают перед нами мир, стирают границы, дарят ощущение неограниченных возможностей, упрощают жизнь. Сегодня можно жить, трудиться,

общаться, обеспечивать себя всем необходимым, путешествовать, не выходя из-за своего компьютера.

Но это могущество опасно. В эйфории мы забываем о безопасности, и это может дорого стоить человеку.

Вопрос: Назовите угрозы жизни в медиапространстве?

(*ожидаемая сущность ответа: социофобия, потеря личности, игромания и утеря реальности, мошенничество и т.п.*).

Сегодня мы остановимся на 4-х угрозах:

1) жизнь в социальных сетях;
2) мой пароль – моя крепость;
3) банальный вирус;
4) опасные сайты.

1. Виртуальная реальность социальных сетей

(Разговор можно предварить предложением высказаться о имеющихся на рынке социальных сетях, их достоинствах и возможностях, как используют сети сами учащиеся).

Социальные сети создают ощущение, что человек становится космополитом («гражданином мира»), что расширяется круг общения, возможности. И ещё, присутствует эффект вагонного знакомства, когда человек изливал попутчику всю свою душу, зная, что больше никогда с ним не увидится. Но глобальная система Интернет и социальные сети отличаются тем, что всё, что вы вынесли в них, сохраняется навсегда и никогда не стирается, и главное – становится доступным для заинтересованных лиц. А так как мы перенесли часть жизни в Интернет, то эта информация может быть использована во вред нам.

Какие опасности таит жизнь в Интернете?

Во-первых, фишинг.

Фишинговыми письмами называют поддельные уведомления от имени администраторов, провайдеров и социальных сетей. Цель письма – побудить вас перейти по фальшивой ссылке на фальшивый сайт и ввести свои логин и пароль. Как правило эти фальшивые сайты и адреса имеют очень схожие с официальными и полностью копируют их дизайн и интерфейс.

Например:

http://vkiontkate.ru/ вместо **http://vkontkate.ru/**

http://odnoklasniki.ru вместо **http://odnoklassniki.ru**

После ввода логина и пароля вас перенаправляют на официальный сайт, а ваши данные остаются в руках мошенников.

Защита простая, входите на официальный сайт напрямую, а не по предлагаемым ссылкам. Для защиты от взлома вашей странички тщательно продумывайте пароль и регулярно его сменяйте.

Есть несколько простых рекомендаций по созданию пароля:

1) пароль должен содержать от 7 до 20 символов;

2) пароль должен содержать буквы как нижнего так и верхнего регистра (т.е. и заглавные и прописные);

3) пароль должен содержать цифры и знаки пунктуации (1-9, !@#$%);
4) пароль не должен совпадать с вашим логином (логин - это ваше имя пользователя).

Во-вторых, неправомерное использование фотографий.

Даже если свои фотоальбомы в социальных сетях вы блокируете для просмотра, они доступны для людей, которые могут использовать их в своих интересах. В определённом возрасте некоторым девушкам хочется представляться более старшими и сексуальными и они выставляют на просмотр отдельным категориям альбомы с фотографиями в жанре «ню» (эротического характера). Эти фотографии потом могут появиться на сайтах эротической направленности.

Есть и вторая угроза – эти фотографии могут привлечь внимание людей с нарушенной психикой, что может привести к преследованию со стороны этих людей.

В-третьих, информация об отпусках и поездках может привлечь внимание криминал, специализирующийся на квартирных кражах.

2. Интернет-угрозы

Кроме угроз жизни в социальных сетях существует множество угроз от обычной работы в Интернете.

Во-первых, компьютерные вирусы.

На сайтах, предлагающих аудио- или видеопродукцию часто можно встретить предупреждение, что для прослушивания или просмотра контента необходимо обновить плеер, ссылка на который тут же прилагается. В итоге, вместо обновления плеера (или вместе с ним) вы получаете и вирусную программу, которая может либо блокировать работу вашего компьютера, пока вы по требованию не переведете деньги и не получите код, или будет копировать всю информацию с вашего компьютера и пересылать ее своим разработчикам.

Во-вторых, опасные сайты.

Существуют сайты, направленные на пробуждение в человеке низменных чувств, противопоставлению обществу и общественным нормам, ведущих человека в зависимость от разработчиков этих сайтов.

Это порносайты, формирующие извращенное представление о сексуальных отношениях, ставящих плотское выше духовного).

Это онлайн-игровые сайты, ведущие к отрыву от реальности и социофобии.

Это экстремистские сайты, разжигающие ненависть и рознь. Подобные сайты через образ врага (виноватого во всем) предлагают поднять собственную самооценку.

Как правило, эти сайты ищут жертв, которые впоследствии становятся либо источниками доходов, либо послушными исполнителями чужих планов.

3. Социальная инженерия

(Вначале можно попробовать выяснить, знакомо ли учащимся понятие «социальная инженерия», и если нет, то какое значение они вкладывают в него - положительное или отрицательное).

Социальная инженерия – это метод несанкционированного доступа к информационным ресурсам основанный на особенностях психологии человека.

Какие человеческие слабости используются социальными инженерами?

1) Жажда лёгкой и быстрой наживы (русская «халява»). На этом основано интернет-мошенничество. Вам предлагается лёгкий заработок или поздравляют с выигрышем, и требуется лишь от вас оплатить первоначальный взнос или регистрационные услуги. В этом случае вспоминайте народную мудрость, что «бесплатный сыр только в мышеловке».
2) Страх. Это качество присуще обычным пользователям, не знающим, как самостоятельно справиться с аппаратным или программным сбоем. Их запугивают сообщениями о взломе персональной странички или ее блокировке. Что-то вроде: «Пройдите по ссылке, иначе ваш аккаунт будет заблокирован» или «если в течение 10 минут после прочтения письма вы не пошлете SMS-сообщение на короткий номер, ваш почтовый ящик будет удален». Времени на размышление нет, специалиста рядом нет, а есть страх остаться без интернет-наркотика, к которому уже сформировалась зависимость.
3) Наивность, желание помочь. В последнее время все больше появляется ресурсов с призывами о помощи и акциями сбора денег. Подавляющее большинство подобных акций – мошенничество. Для желающих помочь существуют официальные благотворительные фонды, которые никогда не занимаются рассылками спама (например, «Российский фонд помощи» http://www.rusfond.ru/).
4) К человеческим слабостям, которые позволяют нам поддаться на предложение или совершить ошибку можно ещё отнести любопытство и невнимательность.

4. Выводы

В рамках одного урока рассмотреть все опасности, которые таит медиа-пространство, невозможно.

Если обобщить все угрозы, затронутые нами сегодня, то можно сделать вывод, что Интернет – это минное поле, где невнимательность и скоропалительность может привести к серьёзным проблемам, касающихся вас лично и ваше окружение.

Существует несколько простых правил, которые смогут если не обезопасить полностью, то значительно снизить угрозы:

1. Пользоваться антивирусом. Современный, регулярно обновляемый антивирус обеспечит надежной защитой от разнообразных интернет-угроз.
2. Регулярно загружать обновления: обновления программ закрывают уязвимости, которыми могут воспользоваться злоумышленники.
3. Не оставлять своих персональных данных на открытых ресурсах: данные, оставленные в интернете, собирают роботы злоумышленников, которые в дальнейшем могут использовать их в своих целях (например, присылать на ваш почтовый ящик больше спама).
4. Не загружать ничего со случайных сайтов: высока вероятность того, что вместе с загруженной программой/книгой/фильмом вы получите и вредоносную программу.
5. Не проходить по ссылкам в спамовых письмах: такие ссылки зачастую ведут на мошеннические, либо заражённые вредоносными программами сайты.

6. Не открывать приложения в письмах, если есть хоть какие-то сомнения в надежности адресанта. Высока вероятность того, что в приложении содержится вредоносная программа (даже если это документ Word).
7. Не пытаться «отписаться» от спама (особенно в том случае, когда в спамерском письме есть соответствующая ссылка). Избавиться от спама это не поможет, скорее наоборот. Существуют два наиболее вероятных варианта развития событий: 1) спамеры регулярно запускают автоматическую проверку и чистку своих баз от несуществующих адресов; отвечая на письмо, вы подтверждаете, что ваш адрес (который, был, возможно, подобран автоматически) действительно существует, его действительно читают. Это побудит спамеров внести его в отдельные, «чистые» базы, вследствие чего вам будет приходить еще больше спама; 2) пройдя по ссылке, вы попадете на зараженный сайт и получите вредоносную программу на свой компьютер.
8. Не откликаться на заманчивые предложения, особенно если они связаны с получением быстрых денег. Откликнувшись, вы или потеряете свои деньги, или, что гораздо хуже, окажетесь замешаны в преступные махинации.

Относительно Интернета можно сказать, что безопасность в виртуальной реальности зависит изначально только от самого пользователя.

Использован материал:

Как защититься от мошенничества в интернете. Практические советы. / «Securelist – Всё об интернет-безопасности»
(http://www.securelist.com/ru/analysis/208050669/Kak_zashchititsya_ot_moshennichestva_v_internete_Prakticheskie_sovety.)