***Урок-дискуссия по теме: «Дети в Сети: ловушки и кошмарики».***

**Цель**: Разобрать негативное влияние на примерах их жизни использования социальных сетей.

**Задачи**: 1. Познакомить с сетевыми вредоносными программами.

2. Рассмотреть классификацию вредоносных программ, и какую угрозу они представляют для безопасности информации;

3. Разобрать алгоритмы работы вредоносных программ и пути их внедрения в систему;

**Тип урока:** урок-обобщение полученных знаний в практической работе.

**Оборудование:**доска, компьютер, компьютерная презентация (Приложение 6), проектор, раздаточный материал (Приложение 4).

**План урока:**I. Орг. момент. (2 мин)
II. Актуализация знаний. (5 мин)
III. Практическая часть. (15 мин)
IV. Итог урока. (5 мин)
V. Д/з (3 мин).

**Формы работы:**

1. беседа;
2. фронтальная работа;
3. практическая работа
4. индивидуальная работа.

**Ход урока.**

I. Орг. момент. (2 мин)
(Приветствие. Объяснение хода урока.)

Здравствуйте. ребята!

Давайте поговорим сегодня об увлечении подростка социальными сетями, поговорим, чем может обернуться это для подростков, и постараемся найти пути для решения этих проблем.

Я уверена, что наш урок станет творческим сотрудничеством.

II. Актуализация знаний. (5 мин)

Увлечение подростка социальными сетями может обернуться для семьи серьезными неприятностями. Скоро мамы и бабушки будут следить не только за тем, чтобы их ребенок не остался один на улице. Теперь главный контроль будет за безопасностью детей в Интернете. Помимо «вредных» сайтов, неумелая активность в социальных сетях, где ребята заводят аккаунты еще в яслях, может обернуться очень большими проблемами для всей семьи. В группе техподдержки компании G Data Software, которая занимается компьютерной безопасностью, таких историй накопилось множество.

III. Практическая часть. (15 мин)

Пример 1. «ВЕЛИКИЙ ПУТЕШЕСТВЕННИК»

- Когда мы вернулись из Таиланда, у нас в доме все было вверх дном, - рассказывает москвичка Светлана. - Воры! Денег там почти не было, но вот компьютер, аудиовидеотехника - все исчезло. В полиции сказали, что кто-то явно действовал по наводке. Стали перебирать друзей, коллег, даже родственников. Кто же из своих оказался наводчиком? Семья не смогла вычислить предателя. Навели порядок, сменили замки, купили новый компьютер, решили забыть об ограблении и жить дальше.

- Однажды смотрю, сын Ваня у компьютера сидит грустный-грустный, - вспоминает Светлана. - Оказывается, перед отъездом появился у него в Одноклассниках друг на пару лет старше. Он с Ваней общался, обо всем говорили, а сейчас пропал.

Светлана забеспокоилась, что их сын мог узнать от неизвестного виртуального друга. Вечером зашла под его аккаунтом в соцсеть, посмотрела диалоги. Найти среди реальных одноклассников нового «друга» оказалось очень легко - фотография подростка и речь взрослого человека, который очень обстоятельно узнавал и о грядущем отъезде, и об адресе, и о входной двери... И Ваня доверчиво своему новому «другу» обо всем рассказал.

Давайте сделаем выводы, как мы должны поступать в подобных ситуациях.

*Совет экспертов по безопасности:*

- Сетевым знакомым нельзя сообщать больше, чем чужим людям на улице. Анонимность в Интернете - вещь очень мнимая, а самый милый случайный знакомец может оказаться настоящим злодеем.

Пример 2. «ВИРТУАЛЬНЫЙ КАСТИНГ»

Родители старшеклассницы Вики умоляли сотрудников техподдержки помочь им без лишнего шума найти злодеев и забрать у них фотографии дочери.

- Мне в соцсети написала девушка, сказала, что она из модельного агентства и я им очень подхожу для рекламы известного бренда, - рассказала Вика. - Чтобы пройти отбор, надо перевести им вступительный взнос - 1500 рублей - и прислать мои фотографии: в купальнике и голышом.

«Позаимствовав» деньги с папиной карточки и упросив подругу поработать фотографом, девушка отправила все, что просили. И стала ждать, когда ее позовут на настоящую съемку.

А тут с папиной карты стали пропадать деньги. Он обратился в службу безопасности банка, и там выяснили, что первый сомнительный платеж был произведен по Интернету в один из выходных дней. Папа сопоставил дату и время платежа, а потом без лишних слов спросил у дочки:

- Кому и за что ты платила моей карточкой?

После недолгой беседы Вика созналась. Теперь ее родители ломают голову, как из этой ситуации выкручиваться. Украденных денег жаль, но страшнее другое: кто и как будет пользоваться фотографиями девушки в стиле ню и чем это потом для нее обернется в будущем?

Давайте сделаем выводы, как мы должны поступать в подобных ситуациях.

*Совет экспертов по безопасности:*

- Подростки должны знать, что брать деньги без спроса нельзя. И уж точно не надо отправлять их абы куда. Модельное агентство никогда не попросит прислать фотографии обнаженных несовершеннолетних кандидаток - это незаконно.

Пример 3. «ТАКОЙ ПРИКОЛЬНЫЙ МЕССЕНДЖЕР»

Иногда обычное детское любопытство приводит к большим проблемам - достаточно ткнуть мышкой в яркий баннер где-то на полях экрана.

- Сын Виталик - ему 10 лет - пытался поставить новый ICQ-клиент, и теперь компьютер показывает одну похабную картинку, - пожаловалась сотрудникам техподдержки Валентина. Рекламные места на страницах соцсетей продают всем. Среди заказчиков попадаются и непорядочные люди. Расчет прост. В баннер с рекламой новой «бесплатной» программы кто-нибудь обязательно кликнет. А перед скачиванием ему предложат заполнить анкету: имя, фамилия, адрес, номер паспорта...

Дальше возможны варианты. Или компьютер просто заразят вредоносной программой. Она незаметно ворует аккаунты, личные сведения, а от имени пользователя в соцсетях рассылается спам.

Здесь был другой вариант. После установки на компьютер новая программа заблокировала его работу и потребовала заплатить 100 долларов за право пользования некими услугами новой программы. Иначе грозили полицией и судом - якобы в принятых (но, разу¬меется, не прочитанных) правилах пользования такая сумма прописана.

Что делать? Или заплатить (без всякой гарантии, что это поможет, и с риском для банковской карточки), или идти к специалистам, которые смогут разблокировать компьютер. А их услуги тоже стоят денег.

Обращение в полицию в этой ситуации бесполезно: пользователь сам попался в ловушку, не прочитав, и нарушил лицензионное соглашение.

*Совет экспертов по безопасности:*

- Устанавливайте бесплатные программы только с сайтов разработчиков и никогда - с торрентов. Заполнять подробную анкету сейчас никто не просит.

Давайте сделаем выводы, как мы должны поступать в подобных ситуациях.

Пример 4. «НЕЧАЯННАЯ ВЕЧЕРИНКА»

Марина захотела красиво отпраздновать свой шестнадцатый день рождения. Для координации с гостями создала специальную группу в Faсebook. Но забыла выставить настройки конфиденциальности, и информация о грядущем праздновании стала доступной всем. Про вечеринку узнали чужие ребята и задумали флешмоб. Они разослали приглашения тысячам абсолютно посторонних людей. Идея прийти на день рождения к юной красавице понравилась многим. В день праздника, когда гости только собирались у Марины в квартире, снизу вдруг раздалось громкое скандирование: «Марина, с днем рождения!», «Марина, мы пришли!» Ничего не понимающая девушка вышла на балкон и увидела, что у подъезда собрались несколько сотен молодых людей. Все пришли к ней на праздник по приглашениям из Facebook.

«Незваные гости» покуражились внизу и разошлись, но праздник оказался испорченным - именинница слишком перенервничала от своей такой неожиданной популярности.

Давайте сделаем выводы, как мы должны поступать в подобных ситуациях.

*Совет экспертов по безопасности:*

- Всегда проверяйте настройки приватности в социальных сетях. Над Мариной пошутили вполне по-доброму. Но не всегда сетевые хулиганы бывают столь милостивы к своим жертвам.

IV. Итог урока. (5 мин). **Рефлексия**. Ребята по кругу высказываются одним предложением, выбирая начало фразы из рефлексивного экрана. ( Приложение 5)

 *Рефлексивный экран*

 я узнал…

 было интересно…

 было трудно…

 я выполнял задания…

 я понял, что…

 теперь я могу…

 я почувствовал, что…

 я приобрел…

 я научился…

 у меня получилось …

 я смог…

 я попробую…

 меня удивило…

 занятия дали мне для жизни…

 *мне захотелось…*

VI. Д/з (3 мин).

**Домашнее задание:** Сделайте выводы, которые помогут избежать вам подобных ошибок и запишите их в тетрадь.

**Использованные ресурсы:**

1. Сычев Ю.Н. Основы информационная безопасность Учебно-практическое пособие. – М.: Изд. центр ЕАОИ, 2007.
2. Мешков В.М., Григорьев А.Н., Проценко Н.Ю. Компьютерные преступления и защита компьютерной инфор-мации: Научно-практическое пособие. – Калининград: Калининградский ЮИ МВД России, 2003.
3. «Компьютерные преступления», http: [www.crime-research.ru](http://www.crime-research.ru).
4. «Проблемы: СМИ и Интернет, Право и Интернет. Интернет-услуги, Компьютеры и преступность, Приватность в российском Интернете», <http://sergo.msk.ru/intlaw/books/index.htm>
5. Журнал «Право и Интернет», <http://www.russianlaw.ru>
6. Киберпреступники украли у юзеров сто миллиардов Дата: 24.09.2012, Источник: Securelist.com, Автор: Татьяна Никитина
7. В России растет число Интернет-мошенничеств, Дата: 01.10.2012, Источник: News.siteua.org
8. «Комсомольская правда», из выпуска от 18-05-2012
9. www.themegallery.com