|  |  |
| --- | --- |
| Автор (ФИО, образовательное учреждение): | Атконова Александра Николаевна, МБОУ ЛИТ |
| Название модуля и тема внутри модуля (ненужное удалить): | **Модуль 4. Цифровое потребление**   * Мошенничество в сети |
| Форма (ненужное удалить): | фрагмент классного часа |
| Класс: | Родители и учащиеся (5-7 класс) |
| Тема урока (собрания, выступления и т.д.): | Мошенничество в сети |
| Цель: | Расширение знаний учащихся о возможных угрозах при работе и общении в сети Интернет |

|  |  |
| --- | --- |
| Задача: | Ознакомить учащихся с основными видами мошенничества в сети. Рассмотреть основные способы защиты от интернет угроз. |
| Необходимые медиа материалы: | [**http://www.youtube.com/watch?v=TJkYp8Z1sLs**](http://www.youtube.com/watch?v=TJkYp8Z1sLs)  [**http://www.youtube.com/watch?v=AMCsvZXCd9w**](http://www.youtube.com/watch?v=AMCsvZXCd9w) |
| Время проведения: | 45 минут |

**Процедура проведения**

**Прослушаем информацию** [**http://www.youtube.com/watch?v=TJkYp8Z1sLs**](http://www.youtube.com/watch?v=TJkYp8Z1sLs)

Сталкивались ли вы с такой ситуацией, как агрессия, вызванная интернетом?

Как вы считаете, какая информация в Интернете является самой опасной?

**Какие меры безопасности ты можешь посоветовать друзьям?**

**Просмотрим видео** [**http://www.youtube.com/watch?v=AMCsvZXCd9w**](http://www.youtube.com/watch?v=AMCsvZXCd9w)

Чтобы не попасть на крючок злоумышленников нужно знать:

* **Кибермошенничество — один из видов киберпреступления, целью которого является обман пользователей:**
* Ни под каким предлогом не выдавай незнакомым людям свои личные данные (домашний адрес, номер телефона и т.д.) и пароли.
* Перед тем, как воспользоваться развлекательными услугами Интернета (скачать музыку, фильм и т.д.), проверь, что после этого тебя не попросят заплатить деньги.
* Не верь всему, что видишь в Интернет.
* Старайся остерегаться новых предложений и услуг, все они требуют вложения крупной суммы денег (например, местонахождение человека по номеру его мобильного, повышение рейтинга в социальной сети и т.д.)
* Советуйся со взрослыми перед тем, как загрузить, скачать или установить ту или иную услугу.
* Очень внимательно выбирай сайты, на которых ты хочешь сделать покупки и удостоверься в их надежности. Собери как можно больше информации о сайте, спросив, например, название, адрес и номер телефона центрального офиса, описания общих положений контракта и, особенно о том, как отменить заказ; кроме того выясни о защите и управлении личными данными и безопасности оплаты; и сравни цены, отыскав такой же предмет на других сайтах.
* Если ты получил неожиданное электронное письмо, в котором тебе предлагается невероятно выгодная сделка, вероятность того, что это мошенничество, очень велика.
* **Вредоносные программы — различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и хранящимся на нем данным**
* Не открывай материал, присланный незнакомцами.
* Не открывай сомнительный файл с вложениями, даже если ты получил его от своего знакомого. Свяжись с другом, от которого ты получил сообщение, и уточни у него, действительно ли он является автором послания
* Не запускай и не скачивай файлы (например, музыку, фильмы, игры) из сомнительных источников.
* Старайся не нажимать на рекламные баннеры, даже если они кажутся тебе очень заманчивыми.
* Старайся не посещать сомнительные сайты или ресурсы.
* Для защиты от спама:
  + Не выдавай в Интернет своего реального электронного адреса, есть риск использования твоего почтового ящика в качестве рассылки спама.
  + Старайся чаще менять пароли к электронной почте, к страничке в социальной сети и др.
* Заведи себе два адреса — частный, для переписки (приватный и малоизвестный, который ты никогда не публикуешь в общедоступных источниках), и публичный — для публичной деятельности (форумов, чатов и так далее).
* Если ты не пользуешься компьютером, старайся отключать его от соединения с Интернетом.

**Меры предосторожности:**

* Не сообщай свои данные агрессору (реальное имя, фамилию, адрес, телефон, номер школы и т.п.). Когда злоумышленнику становятся известны твои анкетные данные, происходит так называемый «троллинг» или травля.
* Не открывай доступ к своей страничке незнакомым людям.
* Следи за информацией, которую ты выкладываешь в Интернете
* Придерживайся правил сетевой этики, не отвечай грубо на сообщения, этим ты можешь спровоцировать собеседника. Игнорируй сообщения от незнакомых, агрессивных и подозрительных личностей. Нужно понимать, что онлайн-общение не является приватным. Другие пользователи могут скопировать, распечатать или переслать твою личную переписку.
* Если ты видишь или знаешь, что твоего друга запугивают, поддержи его и сообщи об этом.
* Не посылай сообщения или изображения, которые могут огорчить кого-нибудь.
* **Груминг — установление дружеских отношений с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника**
* Следи за информацией, которую ты выкладываешь в Интернете. Не выкладывай свои личные данные в Интернете (домашний адрес, номер телефона, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.). Помни, любая информация может быть использована против тебя, в том числе в корыстных и преступных целях
* Используй псевдоним при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), пользовании он-лайн играми и других ситуациях
* Не размещай и не посылай свои фотографии незнакомцам
* Будь осторожен при общении с незнакомыми людьми. Старайся рассказывать как можно меньше информации о себе.

**Источники:**

1. <http://www.youtube.com/watch?v=TJkYp8Z1sLs>
2. [**http://www.youtube.com/watch?v=AMCsvZXCd9w**](http://www.youtube.com/watch?v=AMCsvZXCd9w)