Кибербезопасность

Сценарий занятия

Для возраста

5-7 классы

Трудоемкость

45 минут

htweek.ru

Занятие "Кибербезопасность"

Сегодня мы познакомимся с понятием "кибербезопасность" и основными принципами безопасного использования интернета. Узнаем о схемах мошенничества в интернете и о том, какие действия предпринимать в случае противоправных действий, что такое «фишинговые» сайты и как их распознавать, подумаем о личной стратегии защиты от мошенников в интернете.

Карта занятия

№ п/п	Ориентировочное время выполнения, мин	Задание / активность	Задачи
1	10	О кибербезопасности	Познакомить с понятием «кибербезопасность» и основными принципами безопасного использования интернета.
2	15	Безопасность в социальных сетях	Познакомить со схемами мошенничества в интернете, а также рассмотреть порядок действий в случае противоправных действий
3	15	Финансовое мошенничество	Рассмотреть порядок действий при распознавании мошенничества с банковскими картами
4	5	Завершение занятия	Способствовать формированию личной стратегии защиты от мошенников

Подготовка к уроку

Перед началом урока подготовьте экран или проектор для показа презентации, а также 3 рабочих места для групповой работы. Столы и стулья расставьте таким образом, чтобы все могли видеть экран и общаться с учителем. Количество посадочных мест рассчитывается, исходя из количества людей в классе. На каждый стол заранее положите лист А4. При необходимости обеспечьте подростков пишущими материалами (ручками, карандашами). Заранее распечатайте раздаточный материал: текст сообщения (у каждой команды будет свой индивидуальный текст), анкету злоумышленников (3 экземпляра, по 1 на команду).

Когда все соберутся в классе, предложите самостоятельно разбиться на 3 команды и занять одно из заранее подготовленных мест.

Ход занятия

1. О кибербезопасности

Педагог. Сегодня мы будем говорить о кибербезопасности. Поднимите руку те, у кого хотя бы раз взломали страницу в социальных сетях? А теперь те, у кого пароль содержит дату рождения? А теперь те, кто меняет пароль каждый месяц?

Сегодня мы рассмотрим опасности, которые подстерегают нас в сети Интернет, и поговорим о том, как защитить себя от них.

Какими советами по безопасному поведению в интернете вы уже пользуетесь?

Педагог: Предлагаю каждому написать на стикере, какую информацию о себе он не хотел бы видеть в интернете. 1 стикер=1 утверждение. Стикеры не нужно подписывать. Дайте подросткам 1-2 минуты на формулирование ответов. *Попросите подростков прикрепить стикеры на стену, предложите сгруппировать ответы.*

Вопросы для обсуждения:

- Что общего в ответах?
- Стоит ли публиковать свое полное имя, адрес, номер телефона онлайн?

- Когда можно поделиться фото или видео с кем-то другим?
- Можно ли когда-либо сообщить чужую секретную или личную информацию — почему / почему нет? Что, если вы думаете, что это шутка?

Педагог: Интернет позволяет легко общаться с семьей, друзьями — и вообще со всеми. Мы отправляем сообщения, обмениваемся фотографиями, присоединяемся к чату и прямому эфиру — иногда не задумываясь о том, кто их увидит, прямо сейчас или в совершенно другое время. Изображение или сообщение, которое вы считаете смешным и безобидным, могут быть неправильно поняты людьми, о которых вы никогда не думали, что их увидят — сейчас или когда-нибудь в будущем. Когда что-то появляется, трудно удалить это навсегда — ведь люди могут скопировать информацию, сделать снимок экрана и поделиться ею.

Помните:

• То, что вы публикуете или чем делитесь в интернете, могут увидеть люди, с которыми вы никогда не встретитесь.

• Как только что-то о вас появится в сети, это может остаться в интернете навсегда. Это что-то вроде перманентного маркера: его тяжело стереть с любой поверхности.

• Та информация, которые становится общедоступной и которую трудно стереть, — создают вашу репутацию.

Хорошая новость в том, что вы можете контролировать то, чем вы делитесь в интернете. Вот почему важны настройки конфиденциальности.

2. Безопасность в социальных сетях

Педагог. Не секрет, что без интернета сейчас жить сложно. Однако он кроет в себе не только много возможностей, но и угроз. Мошенники придумывают новые способы получения нашей личной информации с целью обмануть нас или украсть наши деньги.

Давайте представим ситуацию: вам приходит сообщение в ВК от Вани Дудикова. Вы открываете и читаете его.

Раздайте каждой команде распечатанное сообщение, (см. Приложение 10.1. Соц. сети) Дайте 20 секунд ознакомиться с ним.

Педагог. В глубине души у вас зарождается сомнение, что эти слова действительно написал ваш друг. Какими способами можно проверить, он ли это? У вас есть 2 минуты. Запишите свои варианты в бланк, который вы получили.

Включите таймер на 2 минуты. Когда время истечет, предложите командам по очереди зачитать вслух сообщение, которое они получили от Вани, и перечислить способы, с помощью которых они могут проверить, кто написал это сообщение.

Педагог. Хорошо. Проанализировав ситуацию, вы приходите к выводу, что аккаунт вашего друга взломали. А теперь подумайте и ответьте, как именно злоумышленники хотели обмануть вас, чем бы это закончилось, если бы у них получилось? *У каждой команды своя легенда, поэтому каждая предлагает свой сценарий развития событий. Предоставьте подросткам возможность ответить.*

Педагог. Как мы уже выяснили, чтобы втереться к нам в доверие, злоумышленники использовали личную информацию Вани, которую они собрали из разных источников. Сейчас я раздам вам анкету злоумышленников, которую они создали.

Раздайте каждой команде распечатку анкеты злоумышленников и скриншот страницы Вани, (см. Приложение 10.2 Анкета, Страница Вани)

Педагог. Перед вами личная страница Вани Вконтакте, которая находится в открытом доступе в интернете, и ее может увидеть любой желающий. Ваша задача — заполнить пропуски в анкете преступников, опираясь на эти данные. У вас есть 2 минуты. *Включите таймер на 2 минуты.*

Когда время истечет, попросите подростков ответить на вопросы: Что удалось выяснить злоумышленникам и какую именно личную информацию Вани они использовали, чтобы втереться к вам в доверие? Насколько легко было собрать недостающую информацию о вашем друге? Какие меры надо было предпринять вашему другу, чтобы злоумышленники не смогли использовать его личные данные против него? Предложите каждой команде высказать свои идеи, которые соотносятся с их сообщением.

Педагог. Как видно из анкеты преступников, Ваня придумал не самый надежный пароль, чтобы защитить свой аккаунт: злоумышленники с легкостью его взломали. На столе у каждой команды находится лист А4. Ваша задача — придумать и написать в 2 столбика по 5 паролей: в первом будут ненадежные пароли, которые не следует использовать, а во втором — 5, которые преступники не смогут подобрать. Учтите, что пароль должен содержать 6 символов, включая латиницу и цифры. У вас есть 3 минуты на выполнение этого задания.

Включите таймер на 3 минуты, когда время истечет, попросите команды остановить обсуждение.

Педагог. Команда №1, озвучьте простые пароли, которые вы придумали. Другие команды: у вас в качестве примеров были такие же пароли? Если да, то к какому выводу можно прийти?

А теперь каждая команда по кругу озвучивает по 3 примера сложных паролей.

О чем надо помнить, когда вы создаете пароль для личных аккаунтов? Какие параметры нужно учитывать? *Предоставьте подросткам возможность ответить.*

Педагог. Итак, с паролями разобрались. Но Ваню уже взломали, и надо что-то предпринять. Что можно сделать в этой ситуации?

Поняв, что друга взломали, первое, что необходимо сделать – предотвратить действия мошенников. Для этого следует написать письмо в службу поддержки и пост, информирующий других людей о том, что Ваню взломали. Напишите их на обратной стороне вашего листа А4. У вас есть 5 минут.

Включите таймер на 5 минут, когда время истечет, попросите каждую команду зачитать то, что у них получилось.

Педагог. Какая информация должна содержаться в обращении в службу поддержки и посте для общих друзей? Какие требования нужно соблюсти при написании? *Предоставьте подросткам возможность ответить.* Все правильно, вы оповестили службу поддержки и друзей, чтобы те не проходили по ссылкам, не указывали реквизиты своих карт и не отправляли смс на незнакомые номера.

3. Фишинговые сайты

Педагог. Мошенники могут подстерегать нас в интернете на каждом шагу, они пытаются воспользоваться нашей доверчивостью и невнимательностью в своих корыстных целях. Один из способов, которым они пользуются — создают фишинговые сайты.

Что это такое? Представьте себе: вам на почту приходит письмо с новостью о том, что ваш банк проводил лотерею, и вы выиграли крупную сумму денег. Желание быстро обогатиться берет верх над возникшими сомнениями, и вы уже кликаете по ссылке. Перед собой вы видите известный и знакомый вам сайт, остается только ввести данные карты, чтобы начислить выигрыш, однако, вы чувствуете, что с этим сайтом что-то не так: какая-то непонятная реклама, которой раньше не было, другие цвета и дизайн…

Как вы могли понять, это фишинговый сайт, который был создан мошенниками, с целью завладеть вашими личными данными. Давайте подумаем, а какие данные интересуют мошенников, которые создают подобные сайты?

Важные заметки:
Если подросткам сложно ответить, помогите им:
1. Паспортные данные
2. Данные карт
3. Логины и пароли

Педагог. Мы определились, какая информация нужна мошенникам, а теперь давайте подумаем, какие сайты они клонируют, чтобы добраться до нашей информации?

Важные заметки:
Если подросткам сложно ответить, помогите им. Обычно это все, где можно выудить личную информацию, но особенно часто для этого используются сайты:
1. Банковских организаций
2. Авиакомпаний и туристических агентств
2. Социальных сетей
3. Страницы оплаты интернет-магазинов
4. Сайты с объявлениями о купле-продаже и многие другие.

Педагог. Как фишинговые сайты попадают в наше поле зрения, как мы можем оказаться на них?

Важные заметки:

Если подросткам сложно ответить, помогите им. Способов существует множество, вот некоторые из них:

1. Рекламные баннеры, в том числе всплывающие, в социальных сетях и на других информационных сайтах
2. Письмо на личную почту со ссылкой на сайт и красочным описанием того, что жертва может получить, пройдя по ней
3. Sms-сообщение со ссылкой, если номер телефона находится в открытом доступе

Педагог. Как мы можем обезопасить себя от фишинговых сайтов и негативных последствий, которые могут наступить?

Важные заметки:

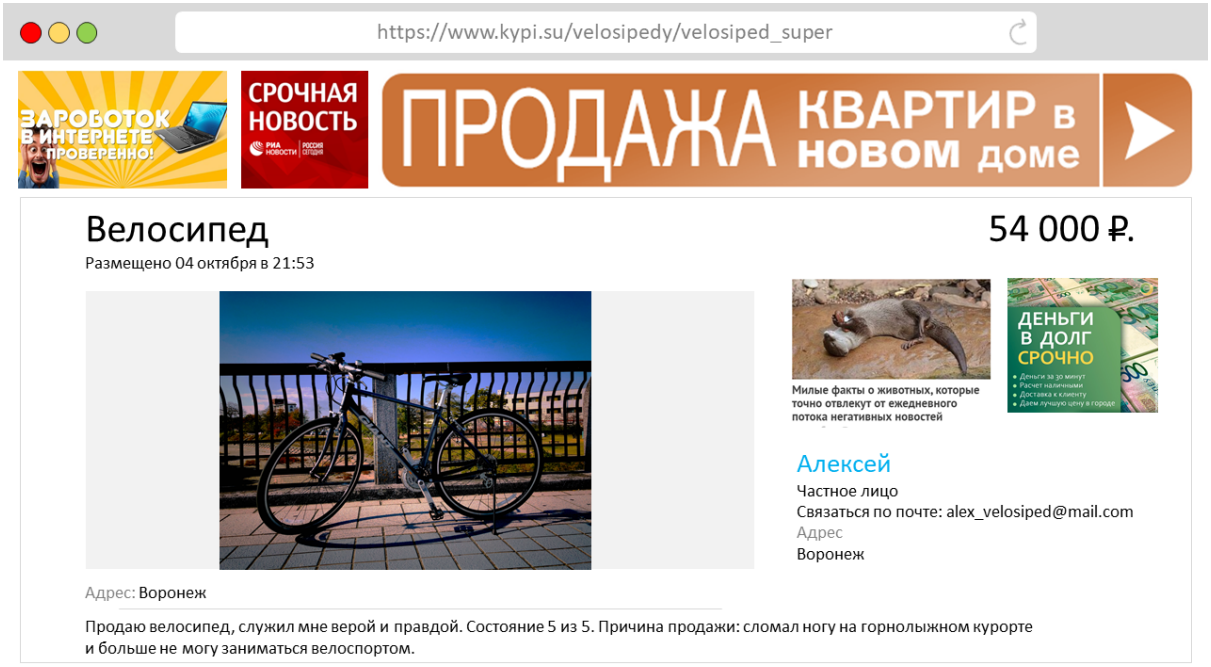
Если подросткам сложно ответить, помогите им.

1. Не переходить по ссылкам от незнакомцев
2. Не переходить по коротким ссылкам, например, goo.gl, даже если они приходят от друзей
3. Используйте антивирус
4. Используйте браузеры, которые блокируют фишинговые сайты, и вы не можете на них зайти
5. Установите многофакторную систему авторизации там, где это возможно
6. Сохраняйте адреса сайтов, которые вы часто используете.

Педагог. А если уже прошли по ссылке, то как распознать, что перед нами фишинговый сайт?

Давайте посмотрим на 2 странички: какой из этих сайтов настоящий, а какой фишинговый? Как вы это поняли? Чем они отличаются?

Выведите на экран изображения, презентацию можно найти в электронных материалах к данному модулю (Приложение 10.3. Обьявления с сайтов)



Педагог. Давайте сделаем шпаргалку у себя в тетради, где укажем, на что надо обратить внимание, чтобы распознать фишинговый сайт. Еще раз проговорим и запишем в нее то, что успели обсудить.

А что вы еще можете добавить в этот список?

Важные заметки:
Если подросткам сложно ответить, помогите им. Выпишите пункты на доску, подростки могут записывать пункты в личную тетрадь или блокнот. В списке могут быть представлены следующие пункты:
1. Название сайта (ссылка).
2. Общее оформление: дизайн, цвета, реклама.
3. Опечатки в тексте.
4. Некоторые кнопки и ссылки на странице могут никуда не вести и быть просто красивой «упаковкой».
5. Несуществующие или подозрительные телефонные номера и адреса в графе «Контакты».

4. Завершение занятия

Педагог. *Что нового вы сегодня узнали? Какие принципы безопасного поведения в интернете вы можете назвать?*
Какие еще способы мошенничества в интернете вам известны? Какие действия стоит предпринять, чтобы не стать жертвой злоумышленников?
Отвечают желающие, устно, всему классу.