



ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ГОРОДА СЕВАСТОПОЛЯ
"СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 26 ИМЕНИ Е.М.БАКУНИНОЙ"

План-конспект занятия
« Безопасность в интернете. Телефонное мошенничество»

Составитель: Сейтмететова Ф.Р.,
Педагог-психолог/Социальный педагог
ГБОУ СОШ №26 имени Е.М. Бакуниной

Севастополь
2025

План – конспект занятия

Тема занятия: « Безопасность в интернете. Телефонное мошенничество»

Цели: обеспечение информационной безопасности несовершеннолетних обучающихся путем привития им навыков ответственного и безопасного поведения в современной информационно-коммуникативной среде, познакомить несовершеннолетних с основными признаками телефонного мошенничества и способам защиты от него.

Актуальность: в последнее время участились случаи телефонного и интернет мошенничества среди подростков, так что умение правильно себя вести в таких ситуациях является весьма актуальным.

Задачи:

1. Обучающие:

- способствовать формированию навыков эффективного поведения в ситуации мошенничества,
- ознакомление с видами телефонного мошенничества,
- ознакомление с видами 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. Развивающие:

- способствовать развитию навыков отказа и принятия безопасного решения,
- способствовать развитию критического мышления

3. Воспитательные:

- способствовать соблюдению этических принципов при групповом взаимодействии и созданию ситуации психологического комфорта в группе сверстников,
- содействовать воспитанию у обучающихся чувства гуманизма, взаимопомощи, взаимоуважения,
- создавать условия для воспитания у обучающихся чувства ответственности за своё поведение в информационном поле.

В рамках данного занятия предполагается формирование у обучающихся УУД- универсальных учебных действий – познавательных, личностных, регулятивных, коммуникативных.

Целевая группа: учащиеся 5-7 классов

Форма проведения: занятие с элементами тренинга

Тип занятия: профилактический, познавательный.

Методы: фронтальная беседа, мозговой штурм (брейнстроминг), проблемно-поисковый, проектная работа, видеодискуссия.

Оборудование: магнитная доска, магниты, карточки по теме занятия, клей, аудио запись, колонка, ватман А1, бумага А4, ручки.

Время проведения: 45 минут

Место проведение: классный кабинет

Дата проведения: 26.02.2025 г.

Ход занятия

1 Этап (Вводный)

Ритуал приветствия (2 мин.)

Педагог приветствует учащихся, представляет себя.

- Здравствуйте, ребята! Меня зовут Фериде Рефатовна. Когда мы говорим при встрече «Здравствуй», мы желаем друг другу здоровья, удачи и хорошего настроения.
- Поэтому я предлагаю вам: повернуться к соседу по парте, посмотреть в глаза, улыбнуться друг другу и сказать: «Я желаю тебе хорошего настроения!». (*Ребята говорят пожелания друг другу.*)
- Очень хорошо!

Введение в тему (3 мин)

Педагог: ребята, прослушайте аудиозапись телефонного разговора. Как вы думаете, кто разговаривает на этой записи, какова цель этого звонка (ответы учащихся).

Ребята, вы догадались, какая тема сегодняшнего нашего занятия? Правильно, сегодня мы с вами поговорим об одной из наиболее распространенных угроз современности, о телефонном мошенничестве, а так же о безопасности в сети интернет. Мы поговорим о проблеме, с которой встречаются в современном мире очень многие люди. Это пользователи всевозможных сотовых телефонов. В наш век мы не представляем себя без них. Вводим всевозможные данные, проводим через это устройство по средствам сети интернет все возможные информационные и финансовые операции. А мошенники не дремлют, разрабатывая всевозможные схемы обмана.

Мозговой штурм (брейнстроминг - 5 мин): роль смартфона в жизни человека

Подросткам предлагается обсудить, какие положительные или негативные факторы смартфон привносит в различные области человеческой

жизнедеятельности: здравоохранение, образование, игровая индустрия, коммуникация, временные рамки.

II Этап (Основной)

1. Видеодискуссия (5 мин.) «как не попасться мошенникам».

А сейчас мы посмотрим видеоролик о том, какую угрозу может представлять пользование сетью Интернет вашей личной безопасности.

<https://rutube.ru/video/88aa7e7972d80a465d2762c5fbde5646/?r=a>

После просмотра видеоролика педагог предлагает обучающимся обсудить возможные варианты развития событий, в случае если бы мальчик послушался советов совы.

2. Упражнение (фронтальная беседа, получение новых знаний-10 мин)

Ребята, а теперь давайте представим, что мы находимся в магазине, где хотим купить смартфон или компьютер. Чем мы будем руководствоваться при выборе? (Цвет, камера, современный, модный, цена и т д)

-Хорошо, это все важно. Итак, я вам продам смартфоны, но с «бонусом».

(Педагог раздаёт детям распечатанные смартфоны, на них приклеены листочки с надписями «кибермошенничество», «фишинг», «вишинг», «смишинг», «соц.сети с угрозами», вредоносные программы с вирусами, троянами, и т д»).

– Скажите, пожалуйста, кому какие бонусы попались? (дети перечисляют)

– А кто знает, что это такое?

– А где мы можем подхватить такие «бонусы»? что мы должны использовать, чтобы зайти в те же самые социальные сети?(Интернет)

– Давайте познакомимся поближе со словами, которые нам встретились.

На доску вешаются распечатанные на листках А4 следующие термины:

– Вредоносные программы

Вредоносные программы — это разнообразное программное обеспечение, умышленно созданное для нанесения вреда электронным устройствам или похищения информационных ресурсов, данных.

Кибермошенничество

Это один из видов киберпреступления, хакер незаконно получает доступ и каким-либо образом использует вашу личную информацию.

Фишинг — это преступная тактика, используемая интернет-мошенниками с целью обогащения, за счет кражи персональной информации жертвы.

Для фишинга характерны:

– Неожиданные сообщения в мессенджерах, смс, соцсетях и электронной почте от имени авторитетной организации (например, банка, платежной системы, онлайн-магазина и т.д.) с побуждением, будь то угроза или просьба, перейти по фишинговой ссылке, либо ввести информацию в прикрепленную к письму форму.

Вишинг – вид телефонного мошенничества, когда злоумышленники звонят и под видом сотрудника банка, финансовой организации и проч. выманивают у жертв реквизиты банковской карты или побуждают совершить какие-либо действия с банковским счетом.

Смшинг – вид фишинга через смс.

– Ребята, а как нам быть, чтобы избежать этого?

(ответы учащихся)

– Давайте отправимся в другой магазин. Магазин «Безопасный интернет».

– Как вы думаете, что мы можем приобрести в таком магазине?

– Сейчас, я вам дам время (3 минуты), чтобы вы в группах обсудили, какие могут быть правила поведения в сети Интернет.

– презентация работ, учащихся: один участник от группы зачитывает вслух правила.

3. Упражнение (проблемные ситуации -6 мин)

Ребята давайте представим себе такие ситуации, какие будут ваши действия:

- вам позвонил незнакомый номер и тут же сбросил звонок (ответы учащихся).

Совет: игнорируйте, ни в коем случае не перезванивайте! Мошенники часто используют платные номера – если вы перезвоните на такой номер, с вас начнет списываться поминутная оплата.

- вам позвонили, спрашивают про ваших родителей, говорят, что с работы и не могут им дозвониться, а срочно нужны их данные, дата рождения и т.д. (ответы учащихся).

Совет: немедленно положите трубку! Запрос личной информации – самый явный признак мошенничества, чем дольше вы разговариваете, тем больше подвергаете себя и взрослых опасности.

- в мессенджере от вашего друга пришло сообщение «Привет! Я участвую в конкурсе, проголосуй за меня, вот ссылка» (ответы учащихся)

Совет: не переходите по ссылке, аккаунт вашего друга могли взломать. Такие действия могут привести к установке на ваш телефон вирусного ПО, а

также кражей данных и денежных средств. Позвоните вашему другу, чтобы проверить информацию.

- вы играете в вашу любимую игру и вам предлагают перевести ваш выигрыш в деньги, но для этого вам необходима карточка взрослого человека, так как детская не подходит. Вам предлагают сделать маме или папе сюрприз, но для этого они не должны знать, что вы взяли их банковскую карту, попросят продиктовать все цифры изображённые на этой карте. (ответы учащихся).

Совет: никогда не диктуйте номер карта и цифры на обратной стороне банковской карты, как только вас просят сделать, что то тайно от взрослых, это мошенники, которые хотят обманным путём украсть деньги с карты ваших родителей.

-вам позвонили с полиции и сказали, что ваши личные данные (номер телефона и т.д.)используют преступники.

Совет: бросайте трубку, сотрудники полиции, банков и так далее, никогда не звонят несовершеннолетним, только родителям или в школу.

Ребята, мы с вами обсудили только несколько примеров телефонного мошенничества, а таких может быть десятки и даже сотни, и поэтому самый главный совет - что бы не случилось, обязательно сообщайте обо всем вашим родителям. Они всегда вам помогут, найдут правильное решение, и, если ситуация будет серьезная, обратятся в соответствующие службы.

III Этап (Завершающий)

Подведение итогов.

4. Упражнение (проектная работа - 6 мин)

Я рада, что у нас получилась такая продуктивная беседа, а теперь давайте вместе с вами подготовим плакат, на тему «Предупреждён, значит вооружён», который поможет нашим друзьям и близким узнать больше информации о телефонном мошенничестве и безопасности в сети.

Инструкция: педагог раскладывает на столе карточки на которых написаны виды мошенничества и советы по борьбе с ними. Задача ребят расклеить эти карточки на заранее заготовленный плакат.

Рефлексия.

Ребята вам понравилось занятие? А что особенно понравилось? Что было трудным?

Ну, что, мы можем теперь с вами сказать, что вооружены знаниями и не попадёмся в ловушку телефонных мошенников?

А для того, что бы эту информацию узнали ваши одноклассники, что бы обезопасить и их, вы можете повесить этот информационный плакат у себя в классе.

Упражнение «Я сегодня...» (5 мин.)

Ребятам предлагается описать то, что нового они узнали на занятии, чему научились. Подростки передают друг другу мячик по очереди и заканчивают фразу «Сегодня я научился...»

Ритуал завершения занятия. (3 мин.)

Ребята на этом наше занятие закончено, не забывайте все правила, которые мы с вами сегодня разобрали и в завершении я раздам вам памятки «Защити себя», которыми вы сможете поделиться со своими одноклассниками и родными.

Досвидания, до новых встреч.

Используемые образовательные ресурсы:

Основные

[Интернет - мошенничество - презентация онлайн \(ppt-online.org\)](http://ppt-online.org)

[Презентация на тему "Телефонное мошенничество" \(infourok.ru\)](http://infourok.ru)

[Телефонные мошенники \(videouroki.net\)](http://videouroki.net)

Дополнительные

https://gspm.ranepa.ru/video/fingram2022/fg2022_videoleksia_part22.mp4

Проверка домена

<https://cctld.ru/>

Противодействие мошенническим практикам (Банк России)

https://cbr.ru/information_security/pmp/

Видео

<https://rutube.ru/video/88aa7e7972d80a465d2762c5fbde5646/?r=a>

Глоссарий:

1. Мессенджер (англ. *Instant messaging, IM*) — это тип синхронной компьютерно-опосредованной коммуникации, предполагающей мгновенную (в реальном времени) передачу сообщений между двумя или более сторонами через интернет или другую компьютерную сеть;

2. Акка́унт (от англ. *account* «учётная запись, личный счёт») — хранящая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам;

3. Фíшинг (англ. *phishing* от *fishing* «рыбная ловля, выуживание»^[1]) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям;

4. Вишинг – Телефонное мошенничество (англ. *vishing*, от *voice phishing*^[1]) — один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определённую роль (сотрудника банка, оператора сотовой связи или правоохранительных органов, покупателя и т.д.), под разными предлогами выманивают у держателя платёжной карты, конфиденциальную информацию;

5. Смíшинг^{[1][2][3]} (англ. *SMiShing* — от «SMS» и «фишинг») — вид фишинга через SMS;

Групповое занятие на тему: «Безопасность в интернете. Телефонное мошенничество» апробировала в своей практике Сейтмететова Фериде Рефатовна, педагог-психолог, социальный педагог ГБОУ СОШ №26 имени Е.М. Бакуниной

г. Севастополя, в ходе реализации развивающей программы «Безопасный интернет».

Программа опубликована на официальном сайте образовательного учреждения <https://shkola26.edusev.ru/>