**СЦЕНАРИЙ**

**воспитательного занятия по безопасному поведению в цифровой среде**

**для учащихся**

**1-4 классов**

**по теме**

**«Кто в сети рыбачит?»**

**Формат:** интерактивное занятие с мультфильмами, играми и практическими заданиями
**Продолжительность:** 40–45 минут

**Цели занятия:**

1. **Образовательная:**
* Познакомить детей с понятиями «цифровая гигиена» и «фишинг».
* Объяснить, как мошенники обманывают игроков в интернете.
1. **Развивающая:**
* Научить распознавать опасные сообщения и ссылки.
* Развить навык обращения за помощью к взрослым в подозрительных ситуациях.
1. **Воспитательная:**
* Сформировать ответственность за личные данные (пароли, номера телефонов).
* Поощрить привычку обсуждать с родителями незнакомые предложения в сети.

**Задачи занятия:**

1. На примере истории мальчика из Roblox показать последствия доверия к мошенникам.
2. Через мультфильм про семью Везуньчиковых смоделировать правильное поведение.
3. Отработать навыки через групповую работу с примерами сообщений.
4. Закрепить знания с помощью создания «Письма другу».

**Материалы:**

* + - Презентация с слайдами.
		- Распечатанные примеры сообщений (Приложение 1) — 4 на группу (2 безопасных, 2 опасных).
		- Брошюры «Правила цифровой гигиены» (шаблон в Приложении ).

**Организация:**

* + Столы для групповой работы (3 группы по 4–7 человек).
	+ Доска с магнитами для сортировки сообщений.

**Учитель:** Добрый день, дорогие ребята. Посмотрите на слайд, вам знаком этот персонаж? А кто это, из какой игры? (слайд 1)

Посмотрите на слайд, такие сообщения вам знакомы? (слайд 2)

*Учитель принимает ответы учащихся, дает им возможность поделиться своим опытом.*

 Как интересно, вы уже так много знаете! А я хочу рассказать вам одну новость, которую я встретила буквально на днях. (слайд 3)

*Недавно произошла история, которая может случиться с каждым, кто любит играть в онлайн-игры. Десятилетний мальчик очень хотел получить бонусы для своей любимой игры Roblox. В интернете он нашёл ссылку на Telegram-канал, где ему пообещали целых 4500 бесплатных бонусов!*

*Мальчик начал переписываться с человеком, который назвался «блогером Квинка». Сначала у него попросили его номер телефона, но потом сказали, что он «не подходит». Тогда мошенники попросили номера телефонов его мамы и папы.*

*Мальчик, не подозревая обмана, взял телефоны родителей, ушёл в другую комнату, чтобы его не заметили, и начал фотографировать SMS-сообщения, которые приходили на их телефоны. В этих сообщениях были специальные коды, которые мошенники использовали, чтобы украсть деньги.* *В тот же день родители мальчика заметили, что с их банковских счетов пропало 557 тысяч рублей! Они сразу поняли, что их сын стал жертвой мошенников, и обратились в полицию.*

***Учитель работает с вопросами для актуализации информации из истории.***

* **Почему мальчик решил поверить мошенникам?** (Что ему пообещали? Почему он решил, что это безопасно?)
* **Что случилось с деньгами родителей?** (Как мошенники использовали коды из SMS? Почему мальчик не смог сразу понять, что его обманывают?)

**Учитель:** Оказывается, таких историй множество! Посмотрите, сколько новостей о том, что мошенники обманывают детей в игре.Что бы не стать жертвой мошенников, нужно знать правила «**цифровой гигиены**».

А что такое **«цифровая гигиена»**, как вы думаете? Давайте разберемся!

*Учитель принимает ответы учащихся, делает вывод и демонстрирует слайд с определением (слайд 4)*

**Учитель:** Во время занятия мы будем записывать правила цифровой гигиены. Откройте брошюру, которая лежит у вас на парте. Запишем определение цифровой гигиены.

*Шаблон брошюры «Правила цифровой гигиены» представлен в дополнительных материалах к уроку. Учитель может использовать предложенный вариант или же разработать свой.*

**Цифровая гигиена** — это правила, которые помогают нам безопасно пользоваться интернетом, играми и гаджетами.

*Это как мыть руки перед едой, только для компьютеров и телефонов!*

**Учитель:** Предлагаю вам познакомиться с новыми героями, которые на своем примере помогут сделать наше пребывание в интернете еще более безопасным. Давайте посмотрим мультфильм про семью Везуньчиковых. (слайд 5)

*После просмотра первой части мультфильма учитель организует работу с вопросами*

* Как поступит Саша?
* А как бы вы поступили, получив такое сообщение?

Давайте посмотрим продолжение истории *(слайд 6)*

*После просмотра второй части мультфильма учитель организует работу с вопросами*

* Какой поступок совершил Саша?
* Он правильно поступил? Ведь он стал лучшим игроком!
* Как вы думаете, будут ли последствия его поступка?

Проверим наши предположения, продолжаем следить за историей Саши. *(слайд 7)*

**Учитель:** Саша стал жертвой мошенников!

*Учитель организует работу с вопросами*

* **Почему Саша решил купить броню у незнакомца?** (Что он хотел получить? Почему он решил, что это безопасно?)
* **Что случилось с аккаунтом Саши?** (Почему он не смог войти в игру? Как мошенники использовали его данные?
* **Как Саша мог поступить иначе?** (Что он должен был сделать, если хотел купить броню? Кому он мог рассказать о предложении незнакомца?)
* **Какие ошибки совершил Саша?(**Почему нельзя фотографировать банковскую карту и отправлять её незнакомцам? Почему опасно переходить по подозрительным ссылкам?)

*Учитель демонстрирует продолжение мультфильма, где представлены ошибки, которые совершил Саша (слайд 8).*

**Учитель:** Саша стал жертвой мошенников, он не только предоставил данные карты своего папы мошенникам, но и открыл фишинговое письмо. А вы знаете, что такое фишинг? Запишем определение Фишинг в нашу брошюру Цифровая гигиена*.(слайд 9)*

**Фишинг** — это когда мошенники притворяются добрыми и честными людьми, чтобы обмануть тебя.

Это как наживка для рыб, только вместо рыбы ловят людей, чтобы украсть их информацию. Фишинговыми бывают не только сообщения, но и звонки, сайты.

**Групповая работа**

**Учитель:**Теперь поработаем в командах. Представьте, что вы получили сообщения в игре. Вам необходимо ознакомиться с ними и определить, являются ли они безопасными или нет. Обоснуйте свой вывод. *(слайд 10)*

* Время для групповой работы – 7 минут
* Представление результатов работы группы – до 3 минут на команду.
* Каждая команда работает с 2 безопасными и 2 опасными сообщениями.

*Примеры сообщений в Приложении 2.*

*Учителю необходимо подготовить распечатанные сообщения (****без комментариев – они необходимы только для работы учителя****), доску и магниты для распределения сообщений детьми на «безопасные» и «опасные».*

*После распределения сообщений учитель предлагает записать в брошюру «Правила безопасности» отличительные признаки безопасных и опасных сообщений.**(слайд 11)*

**Учитель:** Ребята, давайте теперь сделаем вывод и запишем, как же отличить безопасные и опасные сообщения.

*Учителю следует поддерживать и фиксировать идеи детей, помогая им вывести отличия сообщений и представляет выводы на слайде. Дети записывают правила в брошюру.*

**Учитель:** каким же правилам должен был следовать Саша, что бы не попасть в ловушку мошенников?

*Учитель поддерживает предположения учащихся и предлагает записать правила в брошюру*. *(слайд 12)*

*Примеры отличий опасных и безопасных сообщений, правил безопасности приведены в Приложении.*

**Учитель :** Ребята, давайте вспомним историю, с которой мы начали наше занятие. *(слайд 13)*

* Как вы думаете, почему мальчик поверил другому игроку? Действительно ли это был блогер «Квинка»?
* **Какие ошибки совершил мальчик?** (Почему нельзя сообщать номера телефонов родителей незнакомцам? Почему опасно фотографировать SMS-сообщения и отправлять их кому-то?)
* **Как мальчик мог поступить иначе?**(Что он должен был сделать, если хотел получить бонусы? Кому он мог рассказать о предложении «блогера Квинка»?)
* **Почему важно быть осторожным в интернете?**(Какие ещё опасности могут подстерегать в играх или соцсетях?)

**Учитель**: А ваши друзья играют в Роблокс? Я думаю, что каждому из вас и вашим друзьям важно знать правила Цифровая гигиена и соблюдать их. **Домашнее задание:** Представьте, что вы пишете письмо своему другу, который не был на нашем занятии. Вы хотите рассказать ему, что нового узнали и как теперь будете себя вести в интернете. Письмо можно начать с приветствия, а затем продолжить, используя незаконченные предложения».

*Шаблон письма и пример представлены в Приложении 2*

**Учитель:** Вы молодцы! Отлично работали в командах, разбирали хитрые сообщения и даже написали письма друзьям, чтобы предупредить их об опасности. Теперь вы — настоящие супергерои кибербезопасности!

Помните: если мошенники попытаются вас обмануть, вы уже знаете, как защититься. А если вдруг забудете правила — загляните в свои брошюры, которые мы сегодня заполнили.

Приложение 1

**Пример 1: Бесплатные робуксы**

**Сообщение:**
«Привет! Ты выиграл 10 000 робуксов! Перейди по ссылке [поддельная ссылка], чтобы получить их прямо сейчас. Успей, предложение действует только 10 минут!»

***Почему это опасно:*** *Ссылка может вести на фишинговый сайт, где попросят ввести личные данные или данные карты родителей.*

**Пример 2: Секретный промокод**

**Сообщение:**
«Только для тебя! Секретный промокод на 5000 робуксов: ROBLOXFREE. Введи его на сайте [поддельная ссылка], чтобы получить подарок!»

***Почему это опасно:*** *Сайт может быть поддельным, и после ввода данных аккаунта мошенники украдут его.*

**Пример 3: Подписка на канал за бонусы**

**Сообщение:**
«Подпишись на наш канал в Telegram [ссылка], и получи 3000 робуксов бесплатно! Только для избранных игроков!»

***Почему это опасно:*** *В Telegram мошенники могут попросить данные телефона родителей или коды из SMS.*

**Пример 4: Конкурс с призами**

**Сообщение:**
«Ты стал участником конкурса! Чтобы получить приз — 7000 робуксов, отправь нам номер телефона твоих родителей и код из SMS, который придёт на их телефон.»

***Почему это опасно:*** *Мошенники используют коды из SMS для доступа к банковским счетам.*

**Пример 5: Обновление аккаунта**

**Сообщение:**
«Внимание! Твой аккаунт Roblox будет заблокирован, если ты не подтвердишь его. Перейди по ссылке [поддельная ссылка] и введи логин и пароль, чтобы сохранить доступ.»

***Почему это опасно:*** *Это попытка украсть твой аккаунт, чтобы потом продать его или использовать для мошенничества*.

**Пример 6: Бесплатные предметы**

**Сообщение:**
«Хочешь получить редкий меч или скин бесплатно? Добавь меня в друзья и отправь мне пароль от своего аккаунта. Я подарю тебе всё, что захочешь!»

***Почему это опасно:*** *Никогда нельзя делиться паролями! Мошенники украдут аккаунт и всё, что на нём есть.*

Вот примеры **безопасных сообщений**, которые могут появляться в играх, например, в Roblox. Эти сообщения не содержат подозрительных ссылок, не просят личные данные и соответствуют правилам безопасности. Их можно использовать, чтобы показать детям, как выглядят нормальные, неопасные уведомления.

**Пример 1: Официальное уведомление от игры**

**Сообщение:**
«Привет! Не пропусти новое обновление в Roblox. Заходи в игру и проверь новые задания и призы!»

***Почему это безопасно:*** *Сообщение не содержит ссылок и не просит личные данные. Оно просто информирует об обновлении*.

**Пример 2: Напоминание о безопасности**

**Сообщение:**
«Не забывай: никогда не сообщай никому свой пароль от аккаунта. Будь в безопасности!»

***Почему это безопасно:*** *Это полезное напоминание, которое помогает детям запомнить правила безопасности.*

**Пример 3: Официальный конкурс**

**Сообщение:**
«Участвуй в нашем конкурсе! Создай крутой аватар и опубликуй его в своём профиле. Победители получат робуксы! Подробности на официальном сайте Roblox.»

***Почему это безопасно:*** *Сообщение не содержит подозрительных ссылок и предлагает участие в конкурсе через официальные каналы.*

**Пример 4: Новости о событиях**

**Сообщение:**
«Скоро начнётся масштабное событие “Роблокс-фест”! Готовься к новым играм, заданиям и призам. Следи за новостями в игре.»

***Почему это безопасно:*** *Сообщение информирует о событии, не требуя никаких действий, кроме участия в игре.*

**Пример 5: Награда за активность**

**Сообщение:**
«Ты получил 50 робуксов за ежедневный вход в игру! Продолжай играть и получай ещё больше наград.»

***Почему это безопасно:*** *Это стандартное уведомление о награде, которое не требует перехода по ссылкам или ввода данных.*

**Пример 6: Советы по игре**

**Сообщение:**
«Хочешь узнать, как пройти сложный уровень? Загляни в раздел “Помощь” на официальном сайте Roblox. Там есть полезные советы!»

***Почему это безопасно:*** *Сообщение направляет на официальный сайт игры, где нет риска столкнуться с мошенниками.*

Приложение 2

Шаблон письма:

«Привет, [имя друга]!

Сегодня я узнал(а), что...

Теперь я буду...

Мне было сложно...

Самое важное правило, которое я запомнил(а)...

Напиши мне, как ты себя ведёшь в интернете!

До встречи, [твоё имя]».

«Привет, Саша!

Сегодня я узнал(а), что мошенники могут обмануть детей, предлагая бесплатные подарки в играх.
Теперь я буду всегда спрашивать родителей, если мне что-то кажется подозрительным.
Мне было сложно понять, как мошенники используют коды из SMS.
Самое важное правило, которое я запомнил(а), — никогда не сообщать никому данные родителей.

Напиши мне, как ты себя ведёшь в интернете!
До встречи, Маша».