Цель:

КИБЕРУРОК

«Как не попасть в сети Интернет-мошенникам» (для 8 класса)

Формирование и развитие навыков поведения в опасных ситуациях, связанных с Интернет-мошенничеством.

Задачи:

1. Познакомить с видами Интернет мошенничества.
2. Формировать навыки эффективного поведения в ситуации мошенничества.
3. Развивать навыки достойного отказа.
4. Способствовать снятию психоэмоционального напряжения, вызванного использованием сетью Интернет.
5. Актуализировать у детей и подростков полученных знаний.
6. Развивать навыки поведения в опасных ситуациях.

Оборудование: карточки с ситуациями, таблички с названиями опасностей в Интернете, скриншоты страниц с опасными предложениями, картинки с изображением чемодана, корзины, мясорубки.

Организационный момент

Организационный момент

Учитель: Предварительно класс делится на 4 подгруппы. Распределившись на команды, ребята садятся.

Ход занятия

1. Приветствие, психологический настрой (3 минуты)

- Поприветствуем друг друга разными способами по условному сигналу: хлопком ладонь к ладони, плечом и т.д.

Правила поведения на занятии (3 минуты)

Примерные формулировки правил поведения на занятии:

«можно»:

- не вставать с места при ответе;
- высказывать любое своё мнение и отстаивать его;
- уважать мнение своих товарищей;
- не бояться ошибиться, так как каждый человек имеет право на ошибку;
- помогать своему товарищу

«нельзя»:

- перебивать говорящего товарища, выкрикивать с места;
- смеяться над чужим мнением;
- смеяться над ошибками. И другие.

Ход классного часа

2. Просмотр видеоролика “Безопасность платежей в интернете”

https://ligainternet.ru/videouroki/

3. **Учитель:** Интернет-пространство расширяется, и с этим связано развитие кибер-мошенничества. Если люди уже научились распознавать мошенников в реальной жизни, и уже не «ведутся» на обычные шутки, то мошенников в интернете распознать гораздо сложнее. Как вы считаете, по каким причинам?
Да, глазами преступников не увидишь, и понять, что и как они могут сделать, непросто.
В кибер-пространстве мошенники работают по нескольким направлениям.

Учитель: Из каждой подгруппы приглашаются выйти по 1 представителю для выбора кейс-задания.

Организационный момент

Из каждой подгруппы вышли по 1 представителю для выбора кейс-задания. С выбранными заданиями представители сели на свои места. На выполнение кейс-задания дается 10-15 минут. По истечение предложенного времени, каждая подгруппа разбирает выбранный кейс и дает правильные ответы.

4. Упражнение «Чемодан. Корзина. Мясорубка»

Участники выбирают картинки чемодана, мусорной корзины или мясорубки в зависимости от полезности полученных знаний и отработанных навыков по теме безопасности в сети Интернет (или располагаются по принципу
«Четыре (три) угла» в соответствии с размещёнными там картинками чемодана, корзины и мясорубки.
Чемодан – знания, умения и навыки были полезными, я возьму их с собой и буду пользоваться.
Мусорная корзина – ничего для меня не было полезным, мне не пригодятся эти навыки.
Мясорубка – мне ещё нужно осознать то, что я узнал на занятиях, обсудить с кем-то.

Завершение занятия

Учитель: Ребята, наше занятие подошло к концу. Будьте внимательны и соблюдайте правила безопасности в интернете.

Приложение 1.

Кейс - задания в конвертах для 4 команды.

Задание 1. Денежные «мышеловки»
1) «узнай местоположение по номеру телефона»

Задание. Вам предлагается зарегистрировать программу распознавания либо бесплатно, либо со взносом определенной суммы; программа часто оказывается обыкновенным вирусом. В любом случае, человек что-то теряет – деньги со своего счета или же информацию со своих аккаунтов,

связанных с компьютером или телефоном. Либо незадачливого «шпиона» начинают терроризировать звонками и электронными письмами.

Как поступить. Правоохранители предупреждают, что узнать местоположение можно только с согласия абонента, либо по запросу в полиции (от оператора). Иные варианты не действуют. Поэтому откажитесь от слежки, не отправляйте смс и сообщения на указанные номера и уважайте приватность своих ближних.

2) «беспроцентный кредит»

Задание. Пользователю, желающему взять кредит, предлагают предоставить его быстро, легко и в любом объеме, если на счет мошенников будет перечислена круглая сумма. Действия преступников строятся как зеркальное отражение закона: к людям выезжают сотрудники, заполняются необходимые документы (получается согласие в том, что все добровольно и без претензий). Итог – ни денег, ни кредита.

Как поступить. Кредиты лучше не брать вообще; при необходимости сделайте заем у кого-нибудь из друзей или знакомых. При отсутствии возможности возьмите кредит в известном банке, придя лично в его филиал.

Задание 2. Денежные «мышеловки»
2.1. «Магазин на диване»

Задание. Вам предлагается приобрести желаемый товар по привлекательной цене (раз в 5 ниже среднестатистической), а возможно и вовсе бесплатно – вроде конфискат, вам делают подарок. Или к вам попадает журнал с товарами от известного магазина. Есть предложение – получить за заказ на ЭН-ную сумму ценный приз.

2.2. «Попрошайничество»

2.2. "Помощь в трудной жизненной ситуации"

Задание 1. К вам на почту поступает письмо с просьбой о материальной помощи, т.к. автор письма студент/начинающий/в сложной ситуации/денег нет, кушать нечего. На вас никто не давит, желаемая сумма может не указываться. Помочь человеку или нет – только ваше дело.

Задание 2. Вам приходит письмо с официального сайта благотворительной организации (детдома, приюта) с просьбой о материальной помощи какой-либо категории людей/человеку в социально опасном/затруднительном положении.

Как поступить. При желании помочь – проверьте адрес сайта (не дублер ли это), на кого оформлены реквизиты для перечисления денег. Позвоните в

организацию (посетите ее), уточните номер счета и достоверность размещенной информации.

Задание 3. Денежные «мышеловки»

3.1. «Увеличение дохода»

Задание. Вы получаете письмо, где указывается, что денежный сайт предлагает эффективный способ удвоения капитала, (отправь 100 р, получи 500).
Или вам приходит сообщение о смерти дальнего родственника, наследником которого являетесь вы, однако нужно переслать налог на наследство.

Как поступить. Ни в коем случае ничего не высылайте; проверьте, действительно ли у вас был четвероюродный внучатый дядя из Канады, и ждите адвоката. Все юридические вопросы решаются с глазу на глаз, а не в интернете.

3.2. «Техподдержка»

Задание. вам приходит письмо с уведомлением, что аккаунт на каком-либо сайте взломан, или может быть заблокирован или удален (и т.д.), чтобы этого не случилось, необходима оплата (даже когда вы даже не регистрировались на сайте).

Как поступить: не оплачивать, не переходить по ссылкам (можете подхватить вирус) и не вводить данные. Зайдите на сайт с проверенного адреса, обновите страницу, можете обратиться к администратору сайта с вопросом.
Если все же успели ввести пароль, сразу же смените его.

Задание 4. Денежные «мышеловки»

4.1. «Лотерея»

Задание. Вам приходит письмо о крупном выигрыше: вы выиграли деньги/машину/что-то еще, приз будет выслан/счет активирован, как только вы переведете некоторую сумму (пошлина, транспортные расходы и тд.). Вы не участвовали в конкурсе – неважно. Даже не слышали о нем – тем более. Это очень интересно, просыпается азарт – получить нечто, при этом ничего не делая.

Как поступить. Вспомните, принимали ли вы участие, знаете ли организацию, откуда у нее ваши контакты; не знаете ответа на вопрос – забудьте о сообщении и ничего не переводите.
6) отправка смс

Ситуация первая. «Ваш аккаунт блокирован, подтвердите смс… вы выиграли, отправьте смс… помоги выиграть в голосовании…, получи доступ к сайту…» Стоимость СМС - в 5-10 раз больше обычной.

4.2. "Шантаж"

Задание. В эту категорию относятся все сообщения насчет «нелегального доступа к услугам сайта», спама с вашей страницы, угроз выложить в сеть какие-либо материалы, где главным условием избавления от проблемы являются ваши действия по отправлению денежных средств шантажисту.

Как поступить. Можете написать провайдеру о спаме с угрозами, либо в техподдержку сайта, услугами которого вы якобы пользуетесь. Любую угрозу можно заскринить, распечатать и обратиться в полицию.

5. "Механический ущерб" 5.1."Вирусы"

Задание. «Вы реальный человек – введите свой номер телефона». Вам либо приходит смс для ответа, либо вы автоматически подписываетесь на какую- то телефонную услугу и у вас со счета списывается ежедневно пара десятков рублей. Если вы получили сообщение со ссылкой на скачивание открытки, музыки, картинки или какой-нибудь программы, не спешите открывать её. Перейдя по ссылке, вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Как поступить. Внимательно читать всю информацию, особенно мелким шрифтом, со страниц, в частности - внизу сайта. Если не помогло, немедленно обратитесь в салон связи отключать услугу. Посмотрите, с какого номера было отправлено вам сообщение. Даже если сообщение прислал кто-то из знакомых вам людей, убедитесь в этом, позвонив оппоненту. Если отправитель вам не знаком, не открывайте письмо.

Помните, что установка антивирусного программного обеспечения на компьютер или мобильное устройство повышает вашу безопасность.

5.2. "Сайты-фейки"

Задание. Вы заходите на сайт, на котором вы уже зарегистрированы, по ссылке, но вам надо заново вводить почту и пароль от нее.

Как поступить. Проверьте адрес сайта и перейдите по проверенной ссылке.

6. "Работа в интернете"

Задание. Интернет является одним из способов заработка, но человек может стать жертвой мошенников: когда он выполнит работу по переводу текста или написанию реферата, то может остаться без обещанной платы.

Как поступить. Собираясь работать в сети, помните, что главный принцип

– сначала оплата (хотя бы половинная), потом – работа.

Учитель предлагает ребятам поиграть в большую ролевую игру «Опасности сети Интернет»

- Учащимся раздаются роли (таблички с названиями опасностей в Интернете). На внешней стороне таблички написана приемлемая роль (например СМС, электронное письмо, Друг, Реклама, Интересный сайт, Антивирус, но с обратной стороны (невидимой для окружающих) на многих из них написана истинная роль, которую нужно будет грамотно сыграть: вирусы, спам, вредоносные ПО (программное обеспечение), Интернет-хам (тролль), поддельный сайт, Интернет-мошенник (попрошайка), Незнакомец, который хочет заманить куда-нибудь, вызвать на встречу и другие. Несколько ребят играют роль пользователей, которые должны взаимодействовать с остальными (носителями пользы и вреда в Интернет-пространстве) и грамотно принимать или отсеивать поступающую информацию.