ГБПОУ «Лабинский медицинский колледж»

министерства здравоохранения Краснодарского края

Рассмотрено на заседании ЦК
председатель ЦК

_____Плазун Т.И.
Протокол № 2
от «29» 09 2022г.

«Согласовано»
зам.директора поУР

_____Жукова Т.А.
от «29» 09 2022г.

РАЗРАБОТКА ВНЕКЛАССНОГО МЕРОПРИЯТИЯ БЕЗОПАСНЫЙ ИНТЕРНЕТ

Методическая разработка открытого классного часа

Преподаватель Киселева Л.В.

г.Лабинск
2022 г.

Методическая разработка внеклассного мероприятия «Безопасный интернет. Мошенничество в интернет – сети»

(90 минут)

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

Задачи:

1. Познакомить с видами Интернет-преступлений, в частности Интернет – мошенничества.

2. Формировать навыки эффективного поведения в случае мошенничества.

3. Развивать навыки достойного отказа.

4. Способствовать снятию психоэмоционального напряжения, вызванного использованием сетью Интернет.

5. Актуализировать у обучающихся полученных знаний.

6. Развивать навыки поведения в опасных ситуациях.

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

Ход мероприятия

I. Приветствие, психологический настрой (3 минуты)

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

Упражнение-энергизатор «Компьютер»

Ребята делятся на 3 группы: «монитор», «процессор», «клавиатура». Когда психолог говорит какое-либо из названий, участники группы меняются местами. Когда психолог говорит «компьютер» - меняются местами все участники занятия.

II. Правила поведения на занятии (1 минута)

Напоминаются правила работы в группе, при необходимости добавляются новые, которые подходят для данного занятия (добавляем символы).

III. Разминка (15 минут)

Упражнение «Что делать»

Обучающимся раздаются карточки с описанием спорных ситуаций, которые могут произойти в виртуальном пространстве (по 1 на группу). После обсуждения обучающиеся зачитывают свою ситуацию и отвечают на вопросы.

- какую угрозу несет данная ситуация?

- что бы вы предложили делать в данной ситуации?

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.

2. 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.).

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

4. 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).

5. Вам приходит сообщение насчет «нелегального доступа к услугам сайта», спама с вашей страницы, появляются угрозы выложить в сеть какие-либо Ваши материалы, где главным условием избавления от проблемы являются ваши действия по отправлению денежных средств шантажисту.

6. Вас приглашают в группу, предлагают принять участие в интересной игре – квесте, где нужно выполнять интереснейшие задания и размещать фотоотчёт в соцсетях.

- Как вы думаете, о чём сейчас пойдёт речь?

IV. Информационный блок (15 минут)

- Ребята, как вы уже поняли из предыдущего упражнения, нашей темой занятия станет мошенничество в интернете. 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.

1. Денежные «мышеловки»

1) «узнай местоположение по номеру телефона»

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»

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.

3) «магазин на диване»

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.

4) «увеличение дохода»

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.

5) «лотерея»

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.

2. «Попрошайничество»

1) помощь в трудной жизненной ситуации

Ситуация первая: 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.

Ситуация вторая: 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.

3. «Техподдержка»

Ситуация первая: 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.

3. Шантаж

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.

4. Механический ущерб

1) вирусы

«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. В любом случае, вы теряете некоторую сумму денег. 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 - стандартная мера, позволяющая повысить вашу безопасность.

2) сайты-фейки

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.

5. Романтические аферы

Этим пользуются злоумышленники, используя фото привлекательных девушек и юношей, привлекая психологов, программистов и посредством сайтов завязывают переписку с доверчивыми людьми. Взамен вечной любви они просят решить их финансовые проблемы, либо же отправляют своим пассиям подарки, за которые они сами должны расплатиться.

Как поступить. Познакомившись с человеком в интернете, имейте в виду, что он может оказаться мошенником. Требуйте встречи, если не соглашается – есть вероятность, что человек вас обманывает. Можете запросить у человека фотографию его лица на фоне чего-либо (например, газеты его города).

6. Работа в интернете

Интернет является одним из способов заработка, но человек, работающий фрилансером, 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.

Обсуждение: сталкивались ли вы с каким-то видом мошенничества в интернете?

V. Упражнения, направленные на развитие умений, необходимых для противостояния опасностям сети Интернет

Работа в группах «Создайте проект своего сайта» (20 минут)

- Участникам в 2-3 группах предлагается создать свои общие или тематические сайты для школьников, дать им интересное привлекательное название, указать для какого возраста, какие рубрики вы бы разместили на этих сайтах, вкладки, ссылки. Как будет организована навигация по сайтам, укажите правила работы на этих сайтах, как обеспечите безопасность сайтов и т.п.

IV.Релаксация (1 минута)

Упражнение «Гнев богов» или «Метание молний»

- В современном мире очень сложно оставаться спокойным, так как в век информационных технологий вся жизнь тиакже стремительно несётся вперёд, оставляя за собой океан стрессов, миллионы нереализованных стремлений, неудовлетворённых потребностей, море раздражения, негодования, агрессии. Если человек не успевает за этим стремительным темпом, то он будет в прямом и переносном смысле растоптан стремящейся вперёд толпой.

- Из мифов Древней Греции вы наверняка помните о громовежце Зевсе, который когда гневался – метал молнии. Да и другие боги и богини ненамного отставали в своём гневе. И были правы – метание молний – это ещё какая разрядка.

- Сейчас попробуем побыть в качестве богов и богинь в гневе. Становимся прямо, набираем побольше воздуха в лёгкие, сжимаем кулаки и резко опустив вниз «метаем молнии в землю» с резким громким выдохом: «Хук». Повторяем несколько раз, чтобы наступила разрядка.

VII. Рефлексия

Упражнение «Чемодан. Корзина. Мясорубка» (10 минут)

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.

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