ГБПОУ КК «Краснодарский музыкальный колледж им. Н.А. Римского-Корсакова»

Единый урок по безопасности в сети «Интернет»

г. Краснодар
2 декабря 2022 г.

Единый урок по безопасности в сети «Интернет»

представляет собой цикл мероприятий, направленных на повышение уровня информационной безопасности детей и молодежи и привлечение внимания родительской и педагогической общественности к проблеме обеспечения безопасности и развития детей в информационном пространстве.

Нормативно-правовые аспекты проведения

Единого урока по безопасности в сети «Интернет»

- Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ;
- пункт 63 распоряжения Правительства РФ от 23 января 2021 г. № 122-р «Об утверждении плана основных мероприятий, проводимых в рамках Десятилетия детства, на период до 2027 г.»;
- пункты 2.11.38 - 2.11.48 распоряжения Правительства РФ от 6 мая 2008 г. N 671-р «Об утверждении Федерального плана статистических работ»;
- решение парламентских слушаний «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве» (Совет Федерации, 17 апреля 2017 г.);
- пункт 5 Приказа Минцифры России № 236 «О перечне федеральных мероприятий, направленных на обеспечение информационной безопасности детей, производство информационной продукции для детей и оборот информационной продукции, на 2022 – 2027 годы» (утвержден 22 марта 2022 №226).

Организаторы

Единого урока по безопасности в сети «Интернет»

- Министерство просвещения Российской Федерации
- Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
- АНО «Агентство поддержки государственных инициатив»
- Органы исполнительной власти субъектов Российской Федерации

Единый урок по безопасности в сети «Интернет»

является одним из крупнейших мероприятий в сфере детства, благодаря чему с каждым годом растет информационная культура и цифровая грамотность российских детей, что является важнейшим фактором сохранения информационного суверенитета нашей страны, формирования всех сфер информационного общества, а также развития цифровой экономики РФ.

Информационная безопасность детей

это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию

(ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ).

Интернет – это безграничный мир информации, «мир новых возможностей» и перспектив для учёбы, работы, досуга, отдыха и общения

Интернет как архив «цифровых активов»

- деньги;
- бонусы ;
- персональные данные, включая медицинские;
- аккаунты в социальных сетях, страницы и каналы;
- цифровые авторские права на сайты, блоги, фото, видео и другой контент;
- тайна частной жизни;
- репутация - один из самых дорогих активов;
- переписка, деловая и личная, в электронной почте и мессенджерах;
- цифровые коллекции;
- виртуальные вещи;
- контакты и заметки;
- домены и сайты;
- цифровые ресурсы;
- цифровая техника;
- автомобиль;
- умный дом .

Интернет как источник «негатива»

- вредоносные программы;
- сайты с азартными играми;
- «онлайное пиратство»;
- материалы «нежелательного содержания»;
- интернет-зависимость;
- кибербуллинг или травля в соцсетях;
- попытки вербовки в преступные организации;
- вовлечение в деструктивные сообщества;
- вымогательство, шантаж или преступления на сексуальной почве.

В сети Интернет следует вести себя осторожно и строго следовать правилам поведения. Неправильное поведение в киберпространстве может нанести вред не только вам, но и вашим родным и близким

Опасности в сети Интернет и основные способы их избежать

Атаки с использованием вредоносных программ

В этом случае компьютерная система или сеть заражаются компьютерным вирусом или другим вредоносным ПО (вирусы, черви и «троянские кони», фишинговые атаки (отправка спама); распределенные DoS-атаки (нацелены на вывод из строя какой-либо системы или сети). После этого киберпреступники могут использовать компьютер для хищения конфиденциальной информации, повреждения данных и других преступных действий, среди которых распространение своих вирусных копий на компьютеры ваших друзей, родственников, а также по всей глобальной сети.

Как с этим бороться:

- регулярное обновление ПО и операционной системы;
- использование антивирусных программ и их регулярное обновление;
- привычка не открывать вложенные файлы в письмах (за исключением тех случаев, когда вы ожидаете получение вложения и точно знаете содержимое такого файла);
- привычка не переходить по ссылкам в спам-письмах и на подозрительных веб-сайтах;
- осторожность при передаче личной информации;
- общение по официальным каналам;
- внимательность при посещении веб-сайтов;
- регулярная проверка банковских выписок;
- использование надежных паролей.

Использование надежных паролей

Создавайте надежный пароль на своих технических устройствах, руководствуясь основными правилами:

- основной пароль должен быть длинным и сложным (не менее 8 символов, включая цифры, буквы и знаки), и его надо запомнить.
- ни в коем случае не держите его записанным на компьютере или на бумажке рядом с ним;
- используйте двухфакторную аутентификацию для входа в аккаунт браузера, если вы пользуетесь встроенным менеджером паролей.
- настройте безопасный вход в менеджер паролей в соответствии с инструкциями производителя, если вы используете специальное программное обеспечение.
- используйте антивирусную программу, т.к. она может заметить подозрительную активность и пресечь атаку на вас.
- не давайте свои устройства посторонним лицам и всегда блокируйте его, если вам нужно отойти.

Сайты с азартными играми

Разница между игровыми сайтами и сайтами с азартными играми состоит в том, сайты с азартными играми содержат игры, связанны с выигрышем или проигрышем настоящих денег.

Как с этим бороться:

Помните, что никогда нельзя играть на деньги!!!!!

Всегда игроки больше теряют деньги, нежели выигрывают. Играйте в не менее увлекательные игры, которые не предполагают использование наличных или безналичных проигрышей или выигрышей.

Кибербуллинг

Кибербуллинг – использование современных ИКТ с целью виртуального террора, травли, запугивания, оскорбления, насилия подростков и младших детей в сети Интернет.

Как с этим бороться:

- никогда не отвечайте на буллинг
- делайте скриншоты всех сообщений
- блокируйте булли и сообщайте администраторам ресурса
- обязательно поговорите о попытках кибербуллинга с кем-нибудь, в идеале со своим родителям

Посочувствуйте и пожалейте агрессора, ведь психологи утверждают, что агрессия другого человека - это просьба о любви.

Онлайн-пиратство

Онлайн-пиратство – это незаконное копирование и распространение материалов, защищенных авторским правом – например, музыки, фильмов, игр или программ – без разрешения правообладателя.

Как с этим бороться:

Помните! Пиратство, по сути, обычное воровство, и вы, скорее всего, вряд ли захотите стать вором. Знайте, что подлинные (лицензионные) продукты всегда выгоднее и надежнее пиратской продукции. Официальный производитель несет ответственность за то, что он вам продает, он дорожит своей репутацией, чего нельзя сказать о компаниях – распространителях пиратских продуктов, которые преследуют только одну цель – обогатиться и за счет потребителя, и за счет производителя.

Приобретая лицензионный продукт, потребитель поддерживает развитие этого продукта, выход новых, более совершенных и удобных версий. Ведь в развитие продукта свой доход инвестирует только официальный производитель.

Материалы «нежелательного содержания»

К материалам «нежелательного содержания» относятся: материалы порнографического, ненавистнического содержания, материалы суицидальной направленности, сектантские материалы, материалы с ненормативной лексикой.

Как с этим бороться:

- научитесь критически относиться к содержанию «онлайновых» материалов и не доверять им.
- используйте средства фильтрации нежелательного материала (платные или бесплатные), но помните, что они не могут полностью решить проблему и не всегда распознаются фильтрами.

Важно поддерживать доверительные отношения с родителями!

Интернет-зависимость

Современные технологии принесли в наш мир новые виды зависимостей:

- постоянный веб-серфинг или бесконечные путешествия по Всемирной сети Интернет, не обусловленные учебной или профессиональной деятельностью;
- зависимость от компьютерных игр (в том числе азартных!);
- зависимость от социальных сетей;
- использование Интернета как преобладающего средства коммуникации;
- пристрастие к виртуальным знакомствам;
- влечение к созданию вредоносных программ (без какой-либо цели);
- ненужные покупки в Интернет-магазинах или постоянные участия в интернет-аукционах.

Как с этим бороться:

Самый простой и доступный способ решения зависимости это приобретение другой зависимости. Любовь к здоровому образу жизни, общение с живой природой и «живыми» людьми, путешествия по родному краю, творческие прикладные увлечения, занятия спортом, как правило, выводят человека из зависимости.

Попытки вербовки в преступные организации. Вовлечение в деструктивные сообщества. Вымогательство, шантаж или преступления на сексуальной почве.

В социальных сетях и блогах, на которых ребенок оставляет о себе немало настоящей информации, завязывает небезопасные знакомства, нередко подвергается незаметной для него деструктивной психологической и нравственно-духовной обработке.

Как с этим бороться:

Не рассказывайте о себе! Никогда не сообщайте свои имя, номер телефона, адрес проживания или место учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.

Обязательно расскажите о попытках вербовки и вовлечения вас в преступные и деструктивные организации своим родителям!

Расскажите о вымогательствах и шантаже!!! Этим вы обезопасите себя, своих родных и еще многих потенциальных жертв!!!

Памятка
10 правил-советов, которые помогут обеспечить безопасность в Интернете

1. Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.
2. Используйте нейтральное экранное имя, не выдающее никаких личных сведений.
3. Защитите свой компьютер.
4. Используйте надежные пароли и храните их в секрете.
5. Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.
6. Не допускайте грубости в интернете, блокируйте веб-агрессоров.
7. Не добавляйте незнакомых людей в свои контакты
8. Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
9. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.
10. Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Расскажите об этом родителям!

Использование Интернета – это радость. Получайте максимум удовольствия, оставаясь в безопасности.

Заметайте свои цифровые следы самостоятельно!
Соблюдайте правила, которые собраны в этой презентации для вас, и расскажи о них своим знакомым и друзьям!

Иногда всего лишь соблюдение банальных правил может сохранить вам жизнь, а вашим «цифровым активам» - целостность!!!!

Рекомендуемые материалы для самостоятельного ознакомления с вопросами безопасности в сети «Интернет»

(использованные в подготовке презентации):

1. Солдатова Г.У. Цифровое поколение России: компетентность и безопасность / Г.У. Солдатова, Е.И. Рассказова, Т.А. Нестик // Монография. - М.: Смысл, 2017. - 375 с. – Режим доступа: http://detionline.com/assets/files/research/2017cifrovoe_pokolenie_rossii.pdf
2. Макаров С. Прекрасный, опасный, кибербезопасный мир. Всё, что важно знать детям и взрослым о безопасности в интернете / С. Макаров - М.: 2022. - 568 с.: ил. - Режим доступа: https://www.company.rt.ru/social/book_cybersecurity/files/_SMakarov_fullBook_light.pdf
3. Мама, я буду блогером! / Интерактивный сериал от Kaspersky. - Режим доступа: https://kids.kaspersky.ru/serial/
4. Кибербезопасность для детей и взрослых / Серия видео-роликов. – Российская электронная школа. - Режим доступа: https://resh.edu.ru/page/cyber-project

Презентация выполнена в рамках научно-исследовательского проекта на тему «Кибербезопасность» учеником 10 А класса школы-гимназии 88 Вертиевец А.А.