Мастер-класс

Название/Тема: Цифровой след в сети Интернет
Автор: Кузнецов А.Г., педагог дополнительного образования Центра цифрового образования детей «IT-куб»
Направленность: техническая

Цель: повысить уровень цифровой грамотности в сети Интернет.
Задачи:

1. Повысить уровень знаний обучающихся о правилах использования и опасностях при использовании сети Интернет.
2. Развить внимательное отношение к информационным ресурсам.

ПАСПОРТ ПРАКТИКИ

УСЛОВИЯ РЕАЛИЗАЦИИ		
Время	**Форма**	**Методы**
90 минут	Групповая	Теоретический и практический
КАТЕГОРИЯ ОБУЧАЮЩИХСЯ		
Возраст	**Особенности**	**Количество участников в рабочей группе**
12-16	Не адаптирован для детей ОВЗ	7-10
РЕСУРСЫ		
Оборудование и материалы	**Базовые знания из других областей**	**Уровень сложности и Место в структуре курса**
Компьютер (ноутбук), интерактивная панель	Нет требований	Автономное мероприятие
ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ		
Hard-skills, предметные навыки	**Soft-Skills, метапредметные навыки**	**Личностные**
Работа в сервисе «Have I been pwned?	Работа в команде	Отсутствуют
ОПЫТ РЕАЛИЗАЦИИ		
Инструкции для педагога	**Открытая информация о результатах**	**Участие в конкурсах**
Дидактический материал (Приложение 2)	Кибергигиена. Основы информационной безопасности. – Stepik	IT-CUBE.ЛИПЕЦК (vk.com) Центр дополнительного образования (vk.com) Чемпионат по программированию «Цифровые старты» (vk.com)

Этап 1. ПОСТАНОВКА ЦЕЛИ

Рекомендованное время: 10 минут
Задание/Активность: Ответы на проблемные вопросы
(педагог демонстрирует или озвучивает вопросы обучающимся, они пытаются сформулировать правильный ответ)

Блок 1

1. Какие ресурсы сети вы используете?
2. Какими ресурсами пользуются ваши родители?
3. Какие сайты посещаем?
4. Какие ресурсы запрашивают ввод данных о нас? Какие это данные?

5. На сколько востребованы Интернет ресурсы в повседневной жизни?
6. Что изменится в нашей жизни, если отказаться от сети Интернет?

Блок 2

1. Можем ли мы быть уверены в полной защищенности наших данных в социальных сетях и Интернет-магазинах?
2. На чем основывается наша уверенность и неуверенность в защищенности наших данных?
3. Что необходимо для создания учетной записи?
4. Каковы причины утечки данных?

Итог обсуждения: можем ли мы быть на 100% уверены в защищенности наших данных в сети? Какую цель нашего мастер-класса мы сформулируем

Риски этапа: Обучающие не смогут обосновать правильность своего ответа и в последствии сформулировать цель
Варианты минимизации рисков: Педагог должен быть готов наводящими вопросами подвести участников к формированию цели.

Этап 2. ОСНОВНАЯ ЧАСТЬ

Рекомендованное время: 65 минут
Задание/Активность:
Задание 1:
«Проверка аккаунтов учащихся – взламывались ли они» (Приложение 1 (Презентация: Слайд №3).

Педагог предлагает обучающимся при помощи сервиса «Have I been pwned?» (https://haveibeenpwned.com/) проверить взламывались ли аккаунты учащихся.
Педагог предлагает обучающимся обсудить следующие вопросы:

1. Для чего взламывают аккаунты пользователей? Как их потом используют злоумышленники? К какой информации получают доступ злоумышленники?
2. Какие меры можно предпринять против взлома аккаунта?

Задание 2:
«Действия при взломе аккаунта»

Педагог предлагает обучающимся объединиться по группам. Каждая группа работает с одной из социальных сетей. Находим в разделе «Помощь» или «Поддержка» в социальной сети информацию о действиях при взломе аккаунта.

После проделанной работы обучающиеся обмениваются результатами
Задание 3: Безопасные пароли

Педагог демонстрирует на экране статью (Приложение 1 (Презентация: слайд №5); Приложение 2 (раздел «Статья»): интернет-предпринимателя, который входил в социальную сеть под простейшим паролем – хакеры.

Педагог предлагает детям ответить на следующие вопросы:

1. Какой пароль использовал интернет-предприниматель для своего аккаунта в социальной сети, согласно информации статьи в Ведомостях?
2. Приведите примеры легких для взлома паролей
3. Безопасный пароль – какой он должен быть?

Педагог после обсуждение фиксирует примеры обучающихся, тезисы на доске. Обобщает.

Задание 4: Разбор входящих спам писем (Приложение 1 (Презентация: Слайд №6-7).

Педагог демонстрирует на экране два спам письма.

Обучающиеся разбирают письма.

Задание 5: Работа над кейсами (Приложение 1 (Презентация: Слайд №8-12); Приложение 2 (раздел «Кейсы»).

Педагог демонстрирует на экране мини кейсы. Обучающиеся разбирают сообщения.

Занятие можно выстроить двумя способами: обсуждение или индивидуальное выполнение заданий.

Педагог совместно с обучающимися обсуждает правильность выполнения.

Задание 6: Ребусы (Приложение 1 (Презентация: Слайд №13-22).

Педагог демонстрирует на экране ребусы и предлагает обучающимся вспомнить правила разгадывания ребусов и разгадать их.

Задание 7: Фактчекинг

Педагог предлагает участникам обсудить следующие темы:

1. Что такое фактчекинг?
2. Распространение не проверенных фактов.
3. Что такое факт?
4. Кто создает фейки?

Педагог демонстрирует на экране два факта (Приложение 1 (Презентация: Слайд №23-26); Приложение 2 (разделы: «Фактчекинг. Задачи» и «Фактчекинг. Ответы»). Обучающиеся разбирают факты, работая индивидуально в сети Интернет.

Риски этапа: Неработоспособность сервиса «Have I been pwned?», обучающимся покажутся сложными задания 5 и 6, не стабильное подключение к сети Интернет затруднит выполнение задания 7.

Варианты минимизации рисков: предусмотреть задания, которые не связаны с работой в сети Интернет.

Этап 3. РЕФЛЕКСИЯ/ИТОГИ

Рекомендованное время: 15 минут

Задание/Активность:

На мастер-классе рассмотрели возможности безопасного и рационального использования интернет-пространства. Ответственность каждого пользователя цифровых сервисов – быть внимательным и стремиться повышать уровень цифровой грамотности. Прочитайте предложение и продолжите.

Мне было интересно узнать…

Мне понравилось…

Меня удивило…

Мне захотелось…

Риски этапа: участники мастер-класса не смогут провести самоанализ полученной информации и своего состояния

Варианты минимизации рисков: предусмотреть наводящие вопросы.

ПРИЛОЖЕНИЕ 1

https://docs.google.com/presentation/d/1zHKDyLlJQi9bEaXx6TFhu6t_9AvA9wh_/edit?usp=sharing&ouid=110085626965797015250&rtpof=true&sd=true

ПРИЛОЖЕНИЕ 2

Кейсы:
https://docs.google.com/document/d/14KdjNFwQXiP_juSuAlewiCEIK4O5zZ_A/edit?usp=sharing&ouid=110085626965797015250&rtpof=true&sd=true

Фактчекинг. Задачи:
https://docs.google.com/document/d/12vO9hvyFNelJVfGuCpF5MwM-qRtH0nLv/edit?usp=sharing&ouid=110085626965797015250&rtpof=true&sd=true

Фактчекинг. Ответы:
https://docs.google.com/document/d/1VjiyYQNEl7QfSgCF0vmK-XZCISzREjpO/edit?usp=sharing&ouid=110085626965797015250&rtpof=true&sd=true

Статья:
https://drive.google.com/file/d/15HdiKiabYxG1RW4_BaoZUEITdyOYblz_/view?usp=drive_link
https://drive.google.com/file/d/17z0eX-p91m7CdSFDyznAlu_PJgfBss26/view?usp=drive_link