МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РД
ГБПОУ РД «КОЛЛЕДЖ ЭКОНОМИКИ И ПРАВА»

ОТЧЕТ КЛАССНОГО ЧАСА

на тему

«Безопасность в сети Интернет»

Подготовили:

куратор гр 29 пб

Магомедова А.Н.

Дербент 2022г

Цель: знакомство с возможными угрозами в глобальной сети Интернет, правилами безопасной работы в сети.

Задачи:

образовательные:

- ✓ определить уровень знаний студентов о сервисах сети Интернет и возможных угрозах в сети;
- ✓ познакомить с правилами безопасной работы в сети Интернет;
- ✓ научить ориентироваться в информационном пространстве;

воспитательные:

- ✓ формировать ответственное отношение к работе в сети Интернет в режиме online;
- ✓ формировать информационную культуру обучающихся;

развивающие:

- ✓ развивать аналитическое, критическое мышление;
- ✓ развивать познавательный интерес к изучению компьютерных сетей.

Тип классного часа: беседа.

Методы и формы обучения:

- ✓ словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический;
- ✓ частично-поисковый, проблемный, метод мотивации интереса;
- ✓ интерактивная форма обучения (обмен мнениями информацией);

Оборудование: ПК базовой комплектации и проектор с экраном.

Программно-дидактическое обеспечение:

- ✓ Видеоролик о безопасности в сети Интернет,
- ✓ презентация «Безопасность в Интернете»;
- ✓ памятка по безопасности в сети Интернет.

Межпредметная связь: информатика, право, обществознание.

План мероприятия

1. **Организационный момент**

1.1. Мотивационно - ориентационная деятельность

Как вы думаете, чем будем заниматься на уроке?

Ребята поднимите руки те у которых дома есть компьютер или телефон, подключенный к Интернету.
- Я вижу, что большинство учащихся нашей аудитории пользуются Интернетом. А что же такое Интернет длявас? Это благо или зло?
Ответы студентов на вопрос :
-Однозначного ответа на этот вопрос найти, скорее всего нам не удастся. Это быстрый поиск новой и полезной информации, но это и грязь, которая, зачастую, льётся с экрана целыми потоками. И становится очень страшно, когда от этой грязи страдает самая уязвимая Интернет-аудитория – это вы-ребята!
Как вы думаете, чем будем заниматься на уроке?

Во всех школах россии в конце октября провели единый урок безопасности в сети интернет.

А 7 февраля мы будем отмечать Международный день безопасного Интернета, он был учрежден в 2004 году и с тех пор вышел за пределы Европы, в этом году его будут отмечать более 70 стран, в том числе и Россия.

-Какая же опасность нас может подстерегать в интернете? Посмотрим видеоролик. Просмотр Видеоролика о безопасности в сети Интернет, подготовленный портала "Сетевичок" совместно с НП "Лига безопасного Интернета

Генеральный прокурор Юрий Чайка в конце ноября 2017 года сообщил, что Киберпреступность в России выросла в шесть раз с 2013 по 2016 год. Произошли 3 крупные утечки данных о клиентах: РЖД – о 700 тыс. персональных данных сотрудников, Сбербанк – о 5 тыс.кредитных карт., Билайн – 8 млн.данных об абонентах. Один из самых поразительных случаев в 1 квартале 2017 года произошел в январе, когда был взломан официальный аккаунт New York Times в Twitter. Как только контроль был восстановлен, они удалили посты, размещенные хакерами. Пример одного из твитов, который был опубликован на взломанном аккаунте. В нем утверждается, что Россия собирается начать атаку против США.

2. Какие еще виды преступлений в Интернет вы знаете? (студенты озвучивают).

Используемые понятия(показ слайдов)

Интернет (англ.) - всемирная система объединенных компьютеров для хранения и передачи информации. Часто упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть.

Киберпространство (cyberspace) – это воображаемое пространство возможностей, создаваемое компьютерными системами, в частности Интернетом.

Кибербезопасность (cybersafety) – это состояние защищенности киберпространства;

2.1. Наиболее используемые сервисы Интернет

- Веб-страницы. Поиск информации с помощью: Yandex, Google, Rambler и др.
- Файловые архивы: DC, Torrent, Rapid и др.
- Электронная почта
- Блог
- Веб-форум
- Чат
- Социальные сети.

2.2. Основные источники киберпреступлений по данным Роскомнадзор:

- принятие субъектом пользовательских соглашений по умолчанию
- использование "серых" мобильных приложений
- фишинг
- передача персональных данных по незащищенным каналам связи;
- использование геолокационных сервисов
- распространение своих персональных данных в открытых источниках;
- общение с незнакомыми людьми в соцсетях и др.

3. Что такое фишинг?

Фишинг это сетевой вид мошенничества, при котором технически подкованные мошенники выманивают у людей конфиденциальную информацию. Это делают при помощи спама, почтовых и мгновенных сообщений, вредоносных интернет-сайтов.

Главная задача фишинга — получение логина и пароля пользователя для определённого сайта, с дальнейшим их использованием. Это могут быть идентификационные данные вашего банковского кабинета или ПИН-код с номером карточки для вывода на свой счёт ваших денег. Часто фишинг используют для доступа к аккаунтам в соцсетях. В любом случае, когда ваш логин и пароль становятся известны жуликам, последствия для вас будут весьма удручающие.

Представим себе следующую ситуацию:

Например, вам на телефон поступил звонок:

Алло, это _____? – Да.

Вас приветствует сотрудник ВТБ Марина. Вы являетесь клиентом банка ВТБ? – Да.

_____, с вашей карты был произведен перевод, вы подтверждаете перевод? – Нет.

Тогда нам надо отменить перевод, подскажите ваш номер карты и пароль к личному кабинету.

3.1.Как защититься от фишинга

При любых проблемах с банковской картой или счетом банк только блокирует карту или счет. И всё. Сотрудники банка не звонят по телефону с такими вопросами.

Помните, что пароль – только ваш, ни одна организация не станет требовать его от вас. Он необходим только для доступа к определённому сервису и только вы должны знать его.

Внимательно проверяйте каждое полученное почтовое сообщение с неизвестного адреса на предмет наличия всевозможных просьб перейти по ссылке.

Всегда проверяйте с помощью адресной строки, на том ли сайте вы вводите свои идентификационные данные. Обычно подделывается и домен, поэтому он бывает похожим на свой оригинал. Различие может заключаться лишь в одной букве (например, mail.ru легко превращается в meil.ru).

Используйте последние версии интернет-браузеров и лицензионные антивирусные программы.

При входе на банковские сайты следите за тем, чтобы было установлено защищённое соединение https.

Если вы подозреваете, что подверглись атаке фишеров, то сразу же поменяйте пароль своего аккаунта. После этого обратитесь в службу безопасности компании, данные от которой получили мошенники.

4. Социальные сети

Представим себе такую ситуацию. Денис пришел устраиваться на работу (здесь сценка)

Денис: Здравствуйте! Это отдел кадров?

Л.К.: Да, проходите.

Денис: Я Иванов Денис, пришел устраиваться на работу. Вот моё резюме.

Л.К.: Так, так. Окончили _____. Средний бал 4.9. Хорошо. А вообще, чем увлекаетесь, в свободное время что делаете?

Денис: нууу ммм.

Л.К.: Страница есть в социальных сетях?

Денис: Да

Л.К.: Ну посмотрим…Спасибо, Денис, что пришли к нам. Я вам перезвоню.

После сценки:

Информация о вас может повлиять сейчас и в будущем (репутация, работа).

Вы можете заинтересовать не только кибер, но и других преступников (воры).

Можно спровоцировать травлю себя со стороны пользователей сети.

4.1. Что делать?

- Ограничить список друзей.
- Не указывать пароли, телефон, адрес, дату рождения.
- Следить за репутацией.

- Настройки конфиденциальности аккаунта (только друзья или др.).
- Запросы в друзья только тех, кого знаете.
- Не размещать фото и видео с друзьями без их разрешения.
- Не открывать подозрительные ссылки.

5. **Безопасность в публичных сетях**
    - Не передавать личную информацию через общедоступные сети WI-FI сети.
    - Обновлять антивирус и брандмауэр.
    - При использовании WI-FI отключить функцию «Общий доступ к файлам и принтерам».
    - В мобильном телефоне отключить «Подключение к WI-FI автоматически».
6. **Защита беспроводной сети и маршрутизатора**
    - Не используйте пароль, установленный по умолчанию
    - Не разрешайте беспроводному устройству сообщать о своем присутствии. Отключите вещание сетевого имени (SSID)
    - Измените SSID устройства
    - Шифруйте данные.
    - Обязательно установите надежный антивирус на всех компьютерах и устройствах.
7. **Уголовный кодекс РФ**

предусматривает за нарушения в сфере информации, как денежные штрафы, так и лишение свободы сроком до 5 лет.

Статья 282. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (по национальному, религиозному признаку и др.).

Статья 242. Незаконное изготовление и оборот порнографических материалов или предметов.

Статья 280. Публичные призывы к осуществлению экстремистской деятельности.

Экстреми́зм (от лат. extremus — крайний, чрезмерный) — приверженность крайним взглядам, методам действий. Провокация беспорядков, террористические акции, насильственное свержение власти.

8. **Подведение итогов**

Есть такая шутка: компьютер защищен на 100%, когда он находится в сейфе, сейф залит бетоном и находится в середине океана. Мы с вами сегодня уже не можем обойтись без компьютеров и интернета. Поэтому, если мы будем соблюдать рекомендации, которые были озвучены сегодня, это поможет нам минимизировать проблемы при использовании интернета на компьютере, смартфоне и любом устройстве. Надеюсь, что мероприятие было для вас полезным. Спасибо за внимание!