**ЛИЧНОЕ НЕ ПУБЛИЧНОЕ
ИЛИ ПРАВИЛА ПОВЕДЕНИЯ В СОЦСЕТЯХ**

*При проведении данного занятия рекомендуется использовать подготовленную Национальным центром защиты персональных данных презентацию. Приведенный далее текст содержит указания на слайды, к которым относится соответствующая информация.*

**1. Введение**

*(Слайд 1)* ”Социальные сети помогают нам общаться с друзьями и семьей, делиться своими интересами с другими людьми или узнавать последние новости. Одновременно с этим использование социальных сетей может подвергать риску нашу безопасность, особенно если мы активно делимся личной информацией. Наши действия, направленные на распространение персональных данных (опубликование фото и видео, оставление комментариев под постами и т.д.), помогают злоумышленникам узнать о нас больше и использовать такие сведения против нас“.

*(Слайд 2)* ”Контроль за собственным поведением в социальных сетях – важный элемент безопасности, поэтому на сегодняшнем занятии мы поговорим о наших цифровых следах и выработаем советы о том, как сделать использование социальных сетей более безопасным“.

**2. Теоретическая часть**

*(Слайд 3)* ”Персональные данные – это информация о человеке, которая помогает его точно определить. Персональными данными являются не только ваши фамилия, имя, отчество, возраст, дата рождения, номер телефона, номер школы и класса, где вы учитесь.

К персональным данным относятся также ваше изображение на фотографиях и видео, комментарии под постами, которые вы размещаете в социальных сетях, отметки под фотографиями с вашим местоположением и т.д.“.

*(Слайд 4)* ”Все эти сведения помогают другим людям узнать, кто вы, где вы находитесь, что вам нравится и многое другое. Некоторые из таких людей имеют добрые намерения, но некоторые из них хотят получить информацию для контроля за вашим поведением. Люди могут злоупотреблять информацией, чтобы издеваться над другими, унижать их или распространять слухи в Интернете.

Кроме того, ваши персональные данные могут использоваться злоумышленниками, чтобы взломать аккаунты в социальных сетях или приложениях и ”украсть“ вашу личность, чтобы, например, заполучить ваш игровой счет, выманить деньги у вас или ваших близких.

Хорошая новость заключается в том, что мы можем избежать отрицательных последствий, если будем контролировать свои цифровые следы“, то есть то, что мы делаем в Интернете“.

*(Слайд 5)* ”Цифровой след – это данные, которые вы оставляете при каждом действии в интернете. Когда вы посещаете веб-сайты, отправляете сообщения в мессенджерах или пользуетесь социальными сетями, вы создаете цифровые следы. Они похожи на следы на песке, которые остаются после того, как вы прошлись по пляжу. Но цифровой след о себе можете оставлять не только вы. Ваши друзья и семья, когда они публикуют фотографии с вами или упоминают вас в своих постах, тоже создают цифровые следы о вас.

Как же защитить свою личную информацию в социальных сетях? Существует множество способов сделать это. О них мы сейчас и поговорим“.

*(Слайд 6)* ”Прежде чем размещать фотографии, видео и иную информацию в Интернете, спросите себя: ”Хочу ли я, чтобы их увидели все?”

Один из способов сохранить что-то в тайне – никогда не публиковать это в сети. Если вы не хотите, чтобы что-то было отправлено другим людям, не размещайте это в Интернете.

Помните, что независимо от того, какую аудиторию вы выбираете для своих публикаций, Интернет собирает все, что вы когда-либо разместили в сети. Вы можете удалить информацию из своего профиля, но данные, размещенные в Интернете, могут храниться в разных местах“.

*(Слайд 7) ”*Относитесь внимательно к сообщениям и комментариям, которые вы пишете.

Общаться в Интернете может быть весело и забавно, но иногда люди специально оставляют обидные или злые комментарии. Некоторым кажется, что такие действия не несут серьезных последствий. Но важно помнить, что люди, которым вы пишете сообщения и комментарии в Интернете, могут поделиться ими со своими знакомыми.

Неприятные сообщения могут повлиять не только на чувства человека, которому вы их пишете, но и на отношение других людей к вам. Поэтому старайтесь всегда вежливо общаться с людьми в Интернете“.

*(Слайд 8) ”*Создавайте надежные пароли.

Пароли – это способ сохранить личную информацию в безопасности в Интернете.

Выбрав пароль, не делитесь им с друзьями. Пароль – это секрет, который должны знать только вы. Ведь если кто-то узнает ваш пароль, он может получить доступ к вашему аккаунту и использовать полученную информацию против вас.

Помните, что не стоит использовать один пароль для разных аккаунтов в социальных сетях, потому что, узнав один пароль, злоумышленник сможет завладеть доступом к другим вашим аккаунтам.

Более подробно о правилах создания надежного пароля мы поговорим позже (вариант: говорили на предыдущем занятии)[[1]](#footnote-1)“.

*(Слайд 9) ”*Не принимайте запросы в друзья от людей, которых вы не знаете.

Принятие запроса в друзья означает нечто большее, чем нажатие на сенсорную кнопку. Поэтому, прежде чем добавить нового человека в друзья, подумайте о возможных последствиях. Если вы не разграничили настройки доступа для разных списков друзей, вы предоставите новому ”другу“ возможность ознакомиться со всей вашей личной информации.

Помните также, что если кто-то в Интернете просит вас предоставить личную информацию (домашний адрес, номер телефона, фотографии и т.д.), расскажите об этом взрослому, которому вы доверяете, например, родителям, старшему брату или сестре, учителю.

Вам может показаться, что это дружеская просьба или искреннее желание помочь, но нельзя быть на 100 % уверенным, что вы действительно переписываетесь с тем человеком, о котором думаете, или что у вашего собеседника добрые намерения“.

*(Слайд 10) ”*Уважайте цифровые следы своих друзей.

Вы можете размещать в Интернете фотографии и видео своих друзей, но спрашиваете ли вы при этом их согласие на совершение таких действий?

Фотографии и видео, на которых запечатлены ваши друзья, – это их цифровые следы. И они могут стать общедоступными, если вы поделитесь ими в Интернете. Поэтому перед публикацией фотографии или видео, на которых изображен кто-то другой, обязательно спросите его или ее, можете ли вы это сделать. Помните, что поступать по-иному вы просто не имеете права“.

**3. Интерактивная часть**

*(Слайд 11)* Следует объединить учеников в группы и раздать каждой группе одну из ситуаций, указанных в приложении, с предложением обсудить, в чем состоит опасность такого поведения в Интернете.

Каждой группе следует оформить по итогам обсуждения свою позицию, используя формулу ПОПС.

В качестве ожидаемого от учеников результата можно использовать следующий пример:

*Ситуация. Иван заметил, что неприятный комментарий, который он написал в Инстаграме под постом Виктора, опубликован в аккаунте ”Грубые люди Инстаграма“.*

*Ответ. Я считаю, что Ивану не следовало писать такой комментарий под постом, потому что он задел Виктора. А еще у Ивана могут появиться проблемы из-за того, что Виктор поделился его комментарием.*

*Например, об Иване может сложится плохое впечатление среди друзей и родственников. Виктор даже может обратиться с заявлением в милицию или суд, чтоб привлечь Ивана к ответственности.*

*Можно сделать вывод, что Ивану необходимо тщательнее выбирать слова, которые он пишет, и думать в следующий раз о последствиях.*

**4. Заключение**

*(Слайд 12)* ”Помните, когда вы начинаете использовать Интернет на своем устройстве, например, телефоне, вы попадаете в пространство, к которому подключены миллионы других устройств по всему миру. Да, это открывает множество возможностей, но также может принести и неприятности. Для того, чтобы обеспечить безопасность и сохранить контроль над своими данными, следует быть осторожным при выкладывании личной информации в сети“.

|  |  |
| --- | --- |
|  | Приложение к занятию”Личное не публичное или правила поведения в соцсетях“ |

**Ситуация 1.** Анна решила поделиться своими фотографиями на публичном форуме. Она не заметила, что ее фото содержали указание на местоположение. Злоумышленники использовали эту информацию, чтобы определить, где она живет.

**Ситуация 2.** Виктор пытается подружиться с вами в ТикТоке, просит вас пообщаться с ним и поделиться данными о ваших родителях.

**Ситуация 3.** Лиза получила электронное письмо о том, что выиграла приз. Чтобы его получить, нужно перечислить 100 рублей с помощью ссылки, указанной в письме. Она сразу же взяла банковскую карту из маминой сумки и ввела данные.

**Ситуация 4.** У Жени есть тайное хобби, о котором он не хотел рассказывать. Когда Женя пел песню, Миша снял его на видео и выложил это в Интернет ради смеха. Вся школа посмотрела это видео.

**Ситуация 5.** Максим поделился с другом своим паролем от социальной сети. Тот воспользовался этой информацией, чтобы зайти в аккаунт Максима, и разместил сообщения от его имени.

1. Обозначенные вопросы рассматриваются в занятии по теме «Кибер-гигиена: как надежный пароль помогает предотвратить утечку персональных данных». [↑](#footnote-ref-1)