(Теоретическая часть)

СЛАЙД 1

Сеть Интернет в настоящее время представляет собой мировой информационный и коммуникационный ресурс, доступ к которому имеет значительная часть населения планеты и стал неотъемлемой частью нашей жизни. С его помощью мы получаем информацию, общаемся, обмениваемся данными, оплачиваем товары и услуги, отправляем документы для поступления в вузы и делаем многое другое. Вместе с тем интернет таит в себе опасности. В ходе урока мы поговорим о них и научимся их избегать.

Наедине с компьютером или смартфоном легко забыть, что в Сети миллиарды людей и до любого человека всего пара кликов, чтобы связаться с ним. Но не надо забывать, что в Сети кроме доброжелательных собеседников нами могут заинтересоваться мошенники разного рода, а также тролли разной степени небезобидности. Чтобы максимально обезопаситься от подобных угроз, нужно научиться правилам сетевой безопасности. Правила просты, вот основные: во-первых, не стоит никому сообщать о себе излишнюю информацию, например, свои место учебы и проживания, обстоятельства своей жизни (о том, что едем в отпуск, о дорогостоящих приобретениях и т.п.), даже иногда имеет смысл воспользоваться псевдонимом и не раскрывать свое настоящее имя; во-вторых, необходимо сообщать родителям или другим взрослым, которым мы доверяем, о любых разговорах на тревожные темы, которые с нами заводят незнакомцы, в-третьих, обязательно анализировать публикуемый в Сети контент, то есть мы должны осознавать насколько могут быть опасные последствия от публикации, например, фотографий и видео, поскольку по изображениям можно понять, где происходит дело, тем более смартфоны еще и заботливо снабжают фотографии геометками.

Самый большой объем данных о себе, пожалуй, мы распространяем в социальных сетях.

СЛАЙД 2

Социальные сети — большое технологическое достижение, которое сулит много возможностей, но вместе с этими возможностями приходят и неприятности … Нельзя сказать, что социальные сети это один сплошной вред. Во всем должен быть разумный подход, нам необходимо соизмерять вред и пользу нашего нахождения в социальной сети. Польза очевидна - например, можно познакомиться с новыми людьми, которые находятся очень далеко, можно общаться с друзьями, с которыми давно не виделись или они находятся вне зоны непосредственной досягаемости, можно очень оперативно получить новую информацию о чем-либо или о ком-либо. Но стоит отметить и о вреде социальных сетей. Из-за социальных сетей мы утрачиваем навыки межличностного общения. Очень часто бывает, что виртуальное общение иногда заменяет собой Нам реальные взаимоотношения с людьми, оно способно погрузить нас в ирреальный мир, вытеснив желание жить обычной

жизнью, не связанной с компьютером.
Что не позволяет вам социализироваться в обществе, то есть живое человеческое общение сводится к нулю.

СЛАЙД 3

Регистрация в любой социальной сети всегда должна начинаться с прочтения Пользовательского соглашения и Политики конфиденциальности, которые, как правило, размещены в доступном месте на главной странице в любой социальной сети. Но, к сожалению, которые мы никогда не читаем. Прежде чем регистрироваться, именно в соответствующих Правилах следует ознакомиться, как можно установить настройки приватности в сети, а также обратить внимание на предупреждения социальной сети о том, что чем больше информации о себе мы размещаем в Интернете, тем проще другим пользователям установить нашу личность. Поэтому, еще раз говорим о том, что при регистрации в социальных сетях по возможности не указывать набор личной информации о себе, в максимальном объеме. Это же принцип работает и в дальнейшем, когда мы начинаем общение в социальной сети.

Интересный факт:

1 апреля 2010 года британский онлайн продавец компьютерных игр GameStation внес в пользовательское соглашение, которое покупатели должны прочитать, перед совершением оплаты, пункт, согласно которому покупатель также отдает свою душу в вечное пользование магазину. В результате около 7500 согласились с данным пунктом.

Это показало, как легко подавляющее число пользователей, которые не читают подобные документы, могут юридически согласиться с самым безумным требованием продавца.

СЛАЙД 4

Так что же такое личная информация, из чего она состоит. Личная информация равнозначна по смыслу с понятием **персональные данные.** Важность особенного отношения к личной информации, персональным данным можно подчеркнуть тем, что принят специальный закон по этой теме, закон, определяющий порядок обращения с персональными данными - Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.2006. В этом законе раскрывается и персональных данных - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту).

Чтоб вам было понятно, приведу примеры персональных данных. К персональным данным можно отнести: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, фотография, группа крови,отпечатки пальцев, ДНК семейное, социальное, имущественное положение, образование, профессия, доходы, паспортные данные и другая информация.

Кстати, отдельно можно поговорить, о пользовании средствами геолокации. Исследования показали, что использование геотегов являются возможными угрозами собственной безопасности и считаются одним из способов распространения личной информации. Нужно понимать, что «чекиниться» (то есть отмечать свое местоположение; от англ. check-in – регистрация) опасно из-за угрозы собственной жизни или имуществу. Например, если мы оставляем свое имущество без присмотра и при этом оставляем в Сети информацию о своем текущем местоположении (уезжая с родителями в путешествие и размещаем на своей страничке в Интернете фотографию с места отдыха с геометкой), то воры могут использовать эту информацию как сигнал для своих действий.

Еще один минус такого раскрытия информации состоит в том, что она позволяет выявить предпочтения и интересы, что может дать мошенникам возможность использовать различные уловки для привлечения внимания к некачественным услугам (например, на своей страничке вы часто размещаете фотографии с тренировок с геотегами, как следствие, к вам может начать поступать навязчивая реклама товаров, связанных с видом спорта, которым вы занимаетесь). Поэтому пользователям не стоит увлекаться использованием новых возможностей социальных сетей и не забывать о том, что информация об их местоположении может быть крайне важной. Во избежание проблем на смартфоне эту функцию лучше вовсе отключить.

Мы уже много говорили об объеме, персональных данных, который следует указывать при регистрации в социальных сетях, поэтому еще раз, обращаем внимание, что предлагаемые формы регистрации в социальных сетях содержат поля, которые вовсе не обязательны для заполнения и не заполняя которые, все равно можно создать свой аккаунт.

Важно !*Ограничьте просмотр профиля и его содержимого с помощью настроек приватности. В друзьях не должно быть случайных и незнакомых людей.*

СЛАЙД 5

Фейковые страницы и фейковые новости

В социальных сетях **фейк** - это “не настоящая” страница пользователя.
Чаще всего фейковые страницы создают под профайлы известных людей.
Как определить, кого ты встретил в Интернет-пространстве: фейк или не фейк!

1. Во-первых, “пустой профайл”. Обычно кроме имени не указаны другие данные, поскольку зачастую создатели таких страниц особо не стараются повторить оригинал.
2. Профиль наполнен “стоковыми” фотографиями, то есть фотографиями, взятыми из других социальных сетей или поисковых сервисов.
3. Как правило, в общении с другими людьми владелец “фейка” пишет общими фразами, и скорее всего, предложит перейти по различным ссылкам, рекламируя товары и услуги. спам - вот что 100% ожидаемо от фейка!
4. Чем старше аккаунт- тем выше вероятность, что перед Вами не фейк.

Фейковыми бывают не только аккаунты,но и новости.

Как оценить достоверность новостной информации:

1. Первое, что может выдать “фейковую новость”- так называемый “кликбейт”- способ построения заголовков, не договаривающихся саму суть информационного повода и часто граничащих с дезинформацией. Они вызывают у читателей любопытство, поэтому стимулируют пользователей перейти на страницу.

Наверняка они вам встречались:

“Ты ни за что не поверишь!” “Шок! В теле женщины обнаружили ЭТО!”

2. Источник информации. В реальных новостях обычно есть указанием ссылки на источники информации. Проверьте ссылки. Убедитесь, что об этом пишут и другие новостные порталы.
3. Если в качестве доказательства в новости используются фото, то необходимо убедиться в принадлежности данного фото событию, не взято ли оно из другой новости. В данном случае можно воспользоваться сервисом Google “поиск по картинкам”.

СЛАЙД 6

Фишинг как опасный вид спама

Фишинг - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей.

В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Явные признаки фишинга:

1. ***Нет обращения к Вам по имени***
2. ***Подозрительный адрес отправителя***

СЛАЙД 7

Кибербуллинг, а также кибермоббинг, интернет-моббинг, троллинг, флейм - это провокационные агрессивные сообщения, издевательства, оскорбления, угрозы, сообщение другим лицам компрометирующих данных, с помощью современных средств коммуникации (социальных сетей, почтовых ящиков электронной почты, мессенджеров и т.п.) как правило, в течение продолжительного периода времени. Вот несколько советов, которых стоит придерживаться, чтобы не стать жертвой:

1. Не спеши выбрасывать свой негатив в кибер-пространство.
2. Лучший способ побороть тролля - полное игнорирование
3. Надо помнить, что вся личная информация, которая публикуется в интернете, может быть использована против тебя.
4. Если в сети началась травля, то нужно заблокировать злоумышленника, ужесточить настройки конфиденциальности и задокументировать виртуальное нападение. Если кто-то в интернет угрожает вам физически, то надо сделать снимки сообщений и обратиться в полицию.

СЛАЙД 8

Цифровая репутация и сетевой этикет

Цифровая репутация - это Ваш имидж, который формируется из информации о Вас в интернете. Компрометирующая информация в интернете может серьезно отразиться на реальной жизни. Ваше место жительства, учебы, финансовое положение, особенности характера рассказы о близких – все это накапливается в Сети.

Многие подростки легкомысленно относятся к публикации личной информации в интернете, не понимая возможных последствий. Не задумываясь о том, что фотография размещенная пять лет назад, может стать причиной отказа принять на работу.

Комментарии, фотографии и Ваши действия могут не исчезнуть даже после того как Вы их удалите. Вы не знаете, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она. Найти информацию много лет спустя сможет любой, как из добрых побуждений, так и с намерением причинить вред.

Сетевой этикет - правила поведения, общения в Сети, традиции и культура интернет - сообщества, которых придерживается большинство.

Основные правила сетевого этикета:

1. *Помните, что Вы говорите с человеком.*
2. *Придерживайтесь тех же стандартов поведения, что и в реальной жизни.*
3. *Помните, что Вы находитесь в киберпространстве.*
4. *Уважайте время и возможности других.*
5. *Сохраняйте лицо.*

СЛАЙД 10

Основные правила безопасного поведения в Сети:
1.Необходимо знакомиться с пользовательским соглашением
2. Объем размещаемых персональных данных= Цели обработки
3.Настройка приватности
4. Важно использовать надежные пароли
5. Не забывайте об осторожности в использовании информации, полученный в Сети (фейки, спам, фишинговые сайты)
6. Всегда соблюдайте правила сетевого этикета и формирования цифровой репутации

СЛАЙД 10 !НАПОМИНАЛКА!!!

СЛАЙД 11

(Практическая часть)
Игра: ГДЕ ЛОГИКА? (мини версия)
Цель игры: Закрепить полученные знания ПД.
Задача: С помощью логики и ассоциаций усвоить основные понятия, представленные в теоретической части презентации.
Правила: по Картинкам необходимо определить понятия.
Слайд 12 Социальные сети
Слайд13 Персональные данные.
Слайд 14 Фейковые новости
Слайд 15 Кибербуллинг

СЛАЙД 16 спасибо за Внимание!