БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ЛИЧНЫХ ДАННЫХ

См. ролик про защиту персональных данных.

Слайд 2

Используя электронное пространство, мы полагаем, что это безопасно, потому что мы делимся всего лишь информацией о себе и к нашей обычной жизни, вроде бы, это не относится.

Но на самом деле границы между абстрактной категорией «информация» и реальным человеком носителем этой информации стираются.

Слайд 3

Информация о человеке, его персональные данные сегодня превратились в дорогой товар, который используется по-разному:

кто-то использует эти данные для того, чтобы при помощи рекламы продать вам какую-то вещь;

кому-то вы просто не нравитесь, и в Интернете вас могут пытаться оскорбить, очернить, выставить вас в дурном свете, создать плохую репутацию и сделать изгоем в обществе;

с помощью ваших персональных данных мошенники, воры, могут украсть ваши деньги, шантажировать вас и заставлять совершать какие-то действия;

и многое другое.

Поэтому защита личной информации может приравниваться к защите реальной личности. И важно в первую очередь научиться правильно, безопасно обращаться со своими персональными данными.

Так что же это такое – персональные данные?

Слайд 4

Персональные данные - ***любая информация***, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Слайд 5

Персональные данные бывают:

- общие;
- специальные;
- биометрические.

Персональные данные, размещенные в сети Интернет самим субъектом персональных данных, становятся общедоступными, и доступ к ним получает неограниченный круг лиц.

Слайд 6

Цифровой след

Каждое наше действие, совершаемое в сети Интернет, оставляет определенный цифровой след. Такие следы оставляет информация, которую мы добровольно размещаем в сети Интернет, например, фотографии в социальных сетях, высказывания на форумах, «лайки» новостей и многое другое.

Кроме того, цифровые следы оставляет та информация, о наличии которой мы можем и не подозревать, например, информация о посещенных сайтах, о совершенных покупках, о вашем географическом месторасположении и пр.

Если обработать всю эту информацию, то получится очень точный портрет («профайл»), который можно использовать для принятия решений в отношении конкретного человека. Например, направить ему адресную рекламу в соответствии с предпочтениями, «лайками» или отказать в поступлении на работу и пр.

Сегодня информационные технологии позволяют обрабатывать и анализировать огромные объемы данных для выявления новой информации, представляющей ценность для принятия различных решений.

Слайд 7

Риски, которые влечёт обмен информацией в Интернете

Как только информация попадает в Сеть, контролировать ее дальнейшее использование уже практически невозможно. Кто, когда и в каких целях может воспользоваться такими данными, прогнозировать невозможно.

Следует всегда знать и понимать, что вы не будете иметь никакого контроля в отношении информации, размещенной на Вашей странице в социальной сети в случае, когда ваши друзья скопировали информацию и распространили ее в дальнейшем, при этом, не спросив вашего мнения или разрешения.

Пользователи смартфонов часто становятся свидетелями различных инцидентов, которые происходят в общественной жизни и моментально публикуют снятое на фото или видео в Интернете. Некоторые Интернет-форумы пользуются популярностью среди своих пользователей благодаря так называемому «мастерству раскрытия личности лиц, размещенных в онлайн-видеороликах». Даже если вы или ваши друзья оставляют в сети неструктурированную и разрозненную информацию о вас на разных сайтах, есть те, кто может находить способы собирать всю имеющуюся о вас информацию без вашего ведома.

То, что вы говорите или то, чем вы делитесь в Интернете, может повлечь за собой критику. Информация, которой вы поделились с другими может стать мишенью для кибер-хулиганов. Они выставят вас на всеобщее обозрение, подвергнут вас «суду» за ваши он-лайн слова или действия и вынесут вам свой «вердикт».

Кибербуллинг также может произойти, когда злоумышленник создает ложную учетную запись жертвы и использует ее для отправления оскорбительных, агрессивных или неуместных сообщений на почту друзей и семьи, а также на их аккаунты в социальных сетях, включая друзей, таким образом, создавая впечатление, что сообщения были отправлены жертвой.

Вы можете быть уверенными, что находитесь в безопасности от кибер-издевательств, если вы никогда не раскрывали ваших личных данных в Интернете. Тем не менее, поскольку Интернет настолько проник в нашу обычную жизнь, любое лицо, Интернет-пользователь или нет, является уязвимым к безответственному онлайн – поведению.

Угрозы:

- вовлечение детей в деструктивные группы («группы смерти», АУЕ, ИГ, секты, азартные игры, детская порнография);

- мошенничество;

- шантаж;

- манипулирование;

- зависимость от компьютерных игр и от социальных сетей.

Слайд 8

Как же можно обезопасить себя?

- не разглашать сведений о себе и своих близких, которые могут быть использованы против вас и вашей семьи;

- не публиковать в сети Интернет снимков на фоне зданий, по которым можно определить место жительства или места, где вы проводите большую часть времени;

- знать какие сведения о вас выдает ваше мобильное устройство, например, указание геолокации;

- приучить своих родных, друзей, знакомых не размещать ваши данные без вашего согласия, и естественно, самим поступать также;

- прежде чем разгласить сведения о себе и своих близких, подумайте, действительно ли это необходимо (например: оформление дисконтных карт; регистрация на каких-либо сайтах для игр, или получения информации; установка приложений на мобильные устройства).

Важно понимать, что информация, попавшая в сеть Интернет, уже не может быть удалена.

Слайд 9

Как защитить персональные данные в Сети

Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.

Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.

Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает.

Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы, класса иные данные, посоветуйтесь с родителями или взрослым человеком, которому вы доверяете.

Слайд 10

Как использовать электронные средства коммуникаций

Используйте только сложные пароли, разные для разных учетных записей и сервисов.

Старайтесь периодически менять пароли.

Заведите себе два адреса электронной почты — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для открытой деятельности (форумов, чатов и так далее).

При использовании мобильных устройств отключайте функции, которые не нужны в данный момент времени (например: геолокация, Wi-Fi).

При установке приложений на мобильные устройства внимательно читайте условия пользовательского соглашения.

В соответствии с Конституцией Российской Федерации достоинство личности охраняется государством и ничто не может быть основанием для его умаления, никто не должен подвергаться унижающему человеческое достоинство обращению или наказанию. Основным законом, определяющим порядок оборота персональных данных, является Федеральный закон «О персональных данных» № 152-ФЗ, который содержит ряд принципов, помнить и знать которые необходимо.

Слайд 11

Эту и другую информацию Вы можете найти на портале