Добрый день, уважаемые родители!

По данным одной из крупнейших колсантинговых компаний «PricewaterhouseCoopers» ежегодная прибыль от продажи этого товара достигает 300млрд долларов. О каком товаре идёт речь?

Да, речь идёт о персональных данных, которые были определены законодательно ещё в 2006 году. Они подразделяются на три основные группы основные, специальные и биометрические. И очень важно помнить, что любая обезличенная информация может стать личной, как только мы сами или кто-то другой устанавливает отношение между этой информацией и собой. Как это происходит я предлагаю показать в ходе небольшой разминки.

Я привожу пример безличной информации, а вы превращаете её в личную. Например:

**Брянск-город партизанской славы. Я живу в Брянске**

**Луна искусственный спутник Земли Я мечтаю побывать на луне.**

Попробуем?

**Великая Китайская стена-самая длинная постройка в мире.**

**Египетские пирамиды –одно из семи чудес света**

**В японском языке сотни иероглифов.**

**Лабрадоры- удивительно послушные собаки**

Спасибо. А сегодня мы продолжим наш разговор о практических способах кражи персональных данных жертвами которых чаще всего становятся наши дети.

Для начала напомню, что целями завладения данными могут быть:

1. Создание и последующее навязывание рекламного контента, интересного именно Вам;

2. Урон Вашей репутации, компроментирование, публичные оскорбления.

3.Хищение принадлежащих Вам денежных средств

4. Психологическое манипулирование и шантаж

5. Более выгодная перепродажа полученных данных и другие причины

Каждый из нас ежедневно оставляет цифровые следы, которые собираются в нашу персональную базу – профайл А все цифровые следы за последние 10 лет создают так называемую базу «Big Data»(Большие данные) появление которых предсказывали многие писатели фантасты в том числе и Джон Толкин в своём «властелине колец», называя его Саурон или Всевидящее око

В нашей же реальной жизни его функции с успехом выполняют всевозможные социальные сети и мессенджеры. Именно о их роли в сборе персональных данных наших детей и пойдёт речь в дальнейшем.

Создавая учебные материалы по защите персональных данных для педагогов, лаборатория Касперского привела пример того, как пользователи игровых платформ рискуют своими данными на примере игровой интернет-площадки Steam. Этими предостережениями я поделилась со старшеклассниками – соведущими игровой программы «Школа безопасного интернета» .В дополнение к нашему разговору они подготовили целый ряд примеров того, какими способами именно дети могут стать жертвами похитителей персональных данных. Эта информация наиболее актуальна, т.к. получена от непосредственных участников и потенциальных жертв киберпреступников.

Итак, даже если у вашего ребенка и нет аккаунта в социальных сетях, то, почти наверняка он играет в онлайн игры. А значит на рабочем столе его компьютера вы скорее всего увидите как минимум один из таких ярлыков. Это не просто крупнейшие интернет-магазины игр, но и площадки для общения геймеров со всего мира. И широчайшее поле деятельности для интернет мошенников. Маскируясь под официальный сайт игровой площадки они используют максимально похожий на настоящий адрес электронной почты, отличающийся одним-двумя символами. Затем на форумах геймеров предлагаю заманчивые акции (бесплатная раздача игровых бонусов, выгодный обмен ) и оставляют ссылку. Пройдя по ней пользователь думает, что он на официальной платформе и без опасений оставляет логин и пароль. И всё-он не хозяин своему аккаунту. Его могут перепродать, если на нём много купленных игр и заработанных игровых достижений. Могут дискредитировать игрока, зайдя в игру от его имени. А если тот оставил и более личную информацию, могут начать его шантажировать. И, простите за каламбур, это уже не игры.

Но это речь идёт о мошенниках, маскирующихся под легальные платформы. Но и сами они часто занимаются недопустимым . Так , недавно было вынуждено оправдываться руководство компании Epic Games Grop., которую пользователи уличили в тайном сборе персональных данных с компьютера клиента, независимо от его желания, а также в несанкционированном доступе к данным, хранящимся на компьютере и слежкой за цифровыми следами клиента. Руководство извинилось и объяснило всё ошибками при создании программного обеспечения в спешке. Объяснение, конечно, так себе. Но лучше чем ничего.

А чем объяснить существующую долгие годы системную ошибку в самой популярной у школьников социальной сети Вконтакте. Её я позволю себе наглядно продемонстрировать, потому что её жертвой может стать каждый из нас. Отправляя личное сообщение другому пользователю сети, мы логично рассчитываем на конфиденциальность послания. И , если прикрепляем к такому сообщению фото или скан документа, мы надеемся , что ознакомится с этим содержимым только наш адресат. Но как бы не так. Это вложение доступно абсолютно любому пользователю сети, как и данные о том, кто его отправил.

Для этого мы открываем поле для личного сообщения и нажимаем на скрепку.

Открывается перечень типов вложение и мы выбираем слово ДОКУМЕНТ

И вводим , например, слово СПИСОК и нам открывается огромный список приложенных к чужим письмам разнообразных документов, содержащих это слово в названии. Выбираем любой документ и можем прочитать, хотя нам его никто не отправлял, и видим в одном только документе огромное количество нарушений закона о персональных данных.

Но это ещё не всё – у каждого документа есть свой уникальный идентификационный номер, первой частью которого является идентификационный номер владельца аккаунта (странички). Оставив его в адресной строке мы спокойно переходим на страницу отправителя. Как поступят киберпреступники, зная кто и что именно отправил можно только предполагать.

Тот же эффект мы получим, вводя слова Свидетельство, Протокол и т.д. И эту ошибку никто не устраняет и не извиняется за неё.

Помните, что разместить в Интернете персональную информацию гораздо проще, чем её удалить. Конечно, вы можете возразить , что уже с 2006 года в мире активно внедряется идея «права на забвение», которая предполагает удаление персональной информации относящейся к устаревшим, не соответствующим действительности или неуместным персональным данным.

Но как эта идея реализуется? Наиболее показателен пример, вошедший в практику работы по защите персональных данных, как «***История Марио Гонсалеса»***

***В мае 2014года Высший суд евросоюза поддержал иск гражданина Испании Марио гонсалеса, который обратился с требованием удалить электронную версию статьи 1998 года в архиве испанской газеты о продаже своего дома на аукционе в счёт уплаты долга. Этот долг был погашен и Гонсалес не хотел, чтобы компроментирующие его данные были доступны пользователям интернета. Но изначально его жалобу отклонили, т.к. информация была достоверна. Но позже суд обязвл Google удалить ссылку на архив, поскольку Гонсалес больше должником не является. При этом информация из архива газеты не удалена и доступна на сайте, но не показывается при поиске Google. По итогам этого разбирательства была разработана форма заявления для желающих стереть свой цифровой след, воспользовавшись правом на забвение. Но из 240 тысяч заявлений за год было удовлетворено только 40% с 1 января подобный закон вступил в силу и у нас в стране. А что касается Марио Гонсалеса, то благодаря его работе та информация, которую он так хотел скрыть, стала известна на весь интернет. И , я надеюсь, послужит всем нам хорошим уроком.***

А наши временные рамки позволяют рассказать ещё об одном способе сбора персональных данных, раскрывающем один из механизмов манипулирования нашими детьми. Он предельно прост. Им хочется сделать свои сообщения более красочными и интересными, используя уникальные стикеры. Иногда их раздают в рекламных целях. А иногда просят выполнить вроде бы безобидные задания: Опубликуй историю с маской главного поклонника твоих историй. Только, как правило это либо самые близкие друзья, либо мама и история публикуется с геолокацией. А теперь представьте, как можно манипулировать ребенком , угрожая ему или близким , находящимся по реальному адресу. Это взрослый человек в состоянии оценить реальность угроз. А ребёнок? Какие задания идут дальше. Эти скрины прислали дети, которые не выполняли задания до конца. Единственная цель таких раздач – сбор персональных данных.

Это всего три примера утечки персональных данных. Мы обязательно продолжим работу по их изучению дальше. А пока, позвольте напомнить, что мы находимся в школе и задать вам домашнее задание.

1.Донесите до своих детей полученную сегодня информацию и сами постарайтесь не использовать социальные сети для пересылки конфиденциальный информации.

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.

Используйте только сложные пароли, разные для разных учетных записей и сервисов и регулярно меняйте их

Не ставьте геолокации на снимках. Не указывайте места частого времяпрепровождения ребенка (школа, спортивный зал, кружок).

Не выкладывайте фотографии и информацию, раскрывающие увлечения ребенка.

Не выкладывайте фото рядом с машиной

Обязательно корректируйте все изображения, которые могут предоставить официальные данные ребенка. (грамоты, дипломы)Имея в руках полное имя или важный номер документа, легко можно вычислить, где учится и живет ребенок.

Избегайте публикаций фотографий вашего ребенка с другими детьми. Перед тем как выкладывать фото вашего ребенка с друзьями и одноклассниками, подумайте, не будут ли против их родители.

Но самое главное средство обезопасить персональные данные вашего ребёнка в сети остаётся неизменным на протяжении десятков, а то и сотен лет, несмотря на технический прогресс – установите с ребенком доверительные отношения. Говорите с ним , когда он только захочет и на любые темы. Ребёнок должен знать, что при любой непонятной или неприятной ситуации в интернете ему есть к кому обратиться И этот кто-то его самый близкий человек.

Спасибо за внимание!