

ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ЦЕНИМ И УМЕЕМ СОХРАНЯТЬ!

Что надо знать о персональных данных

Персональные данные – все данные о человеке, своего рода «паспорт его личности». Их следует тщательно беречь и не раскрывать в Интернете без необходимости. В противном случае это может привести к очень неприятным последствиям: нежелательным звонкам, спаму, краже денег и документов, аккаунтов, различным мошенническим действиям. Безопасность – это наша непререкаемая ценность для детей и взрослых!

Что относится к персональным данным?

1. Фамилия, имя, отчество;
2. Номера и реквизиты всех документов (паспорт, СНИЛС, ИНН, свидетельство о рождении, аттестат об образовании, медицинский полис и т.п.);
3. Банковские данные (номер счета, карты, пин-код, CVV-код и т.п.);
4. Ваша контактная информация (номера телефонов, адреса электронной почты, адреса жительства, работы или учебы);
5. Фотографии и видеозаписи с вашим изображением;
6. Данные о ваших родственниках;
7. Ваши логины и пароли.



Ключевой вопрос:

Насколько реально и как сохранить персональные данные вашей семьи?

Внимание!

Более трети россиян (37%) не знают, для чего и как могут быть использованы персональные данные (по данным ВЦИОМ)!

Соцсети, мессенджеры и видеохостинги ежедневно собирают о нас огромное количество данных. Делается это, в первую очередь, для заработка денег. Большинство крупных платформ – бесплатны, ведь их владельцы зарабатывают на своих пользователях. Точнее – на их персональных данных, при перепродаже или использовании в рекламе. Соцсети и мессенджеры берут эти данные не только из профиля пользователя, но и из его переписки. Обратите внимание: вся переписка постоянно хранится на серверах социальной сети или мессенджера, поэтому в результате утечки, кражи или хакерской атаки ваша частная жизнь может стать достоянием общественности.

Источники беды

Не стоит надеяться на «приватные» публикации, просматривать которые может только ограниченный круг лиц, которых настраивает сам пользователь. Ведь утечка может произойти через любого из этих людей. Иногда происходят крупные утечки, в результате чего данные тысяч пользователей попадают в открытый доступ. Но чаще всего пользователи сами выкладывают информацию о себе в Интернет. Защитите себя и свою семью! 80% информации о жертвах преступники находят в социальных сетях (по данным Роскомнадзора).

Кроме персональных данных о каждом человеке собираются также его фото- и видеоизображения. Современного человека ежедневно снимают сотни видеокамер, расположенных в публичных местах. Эта информация собирается, в первую очередь, государственными органами с целью обеспечения безопасности, раскрытия преступлений и т.п. Однако следует помнить, что такие видеозаписи могут попасть и в руки к шантажистам или иным злоумышленникам. Будьте осторожны! Не помогайте мошенникам, добровольно передавая им персональные данные.

В текущей ситуации большинство порталов органов власти и коммерческих компаний становятся объектами хакерских атак в ежедневном режиме.

Так, за последнее время в публичный доступ утекли базы данных пользователей компании «Яндекс.Еда» и клиентов медицинской лаборатории «Гемотест». Все это происходит из-за того, что в России до сих пор нет существенной административной и уголовной ответственности для операторов подобных баз. Так, «Яндекс.Еда» «отделалась» штрафом всего лишь в 60 тысяч рублей.

Важно помнить, что из-за халатности или экономии компании на хранении данных, которые мы оставляем, оформляя карточку в магазине, на заправке или любом другом месте могут стать достоянием общественности.

Надо помнить!

Активный пользователь Интернета оставляет цифровой след – иногда свой полный портрет: состояние здоровья, внешность и физические данные, привычки, места пребывания, уровень дохода, данные о личной и интимной жизни и многое другое. Приложения на телефоне могут получить доступ микрофону, камере, акселерометру (используется для измерения движений устройства) и следить за своим пользователем круглосуточно. Всё это может представлять интерес для преступников! Мошенничество, шантаж, травля – вот неполный список того, для чего злоумышленники могут использовать информацию о пользователях. Следите за культурой поведения в сети, сохраняйте свою частную жизнь и конфиденциальность!

В соответствии с действующим законодательством любой гражданин вправе отказаться от предоставления своих персональных данных. Согласие на обработку персональных данных может быть отозвано гражданином у организации в любой момент.

Если вас принуждают к подписанию согласия на обработку персональных данных и отказывают в предоставлении услуги, смело обращайтесь в прокуратуру.

Полезные советы

1. Посоветуйте своему ребенку при регистрации в социальных сетях использовать только имя или псевдоним (никнейм).
2. Следите за тем, чтобы ребенок не размещал в интернете лишнюю информацию: где он живет, где учится, какой дорогой ходит на уроки и т.п.
3. В настройках камеры на телефоне следует отключить геотеги (геолокацию, место съемки). Эта функция показывает, где именно делалась фотография. В таком случае любой желающий по фото может отследить пользователя.
4. Полезно будет настроить приватность в аккаунте своего ребенка. Таким образом его профиль смогут смотреть только его друзья.
5. Объясните ребенку, что нельзя выкладывать в Интернет фото или скан-копии его документов или банковских карт.
6. Расскажите ребёнку, что персональными данными стоит делиться только с ограниченным кругом лиц – самыми близкими. Не стоит передавать такие данные друзьям, а особенно незнакомым людям из соцсетей.
7. Ребёнку надо знать, что злоумышленники могут пытаться выведать информацию и персональные данные через личные сообщения в социальных сетях. Особенно внимательно стоит реагировать на ссылки, которые незнакомцы присылают ребёнку в личных сообщениях. Лучше по ним не переходить, а неизвестные файлы – не открывать.
8. Расскажите ребенку, что нельзя подключаться к первому попавшемуся бесплатному Wi-Fi в публичном месте. Через такую бесплатную сеть злоумышленники могут получать доступ к персональным данным пользователей.

Личный пример

Тщательно отбирайте фото и видео, которые вы сами выкладываете в Интернет!



НАЦИОНАЛЬНЫЙ
ЦЕНТР ПОМОЩИ
ОРФАНЩИМ И ПОСТАРАДАВШИМ ДЕТЯМ
KAITPPEBENKA.PO



лига
безопасного
интернета



Сайт
ligainternet.ru



Внимание!

Не только дети, но и взрослые могут проводить в Интернете целый день. Видео, соцсети, игры - на это можно тратить очень много времени. Как показали независимые исследования в 76% случаев дети используют Интернет для игр, в 70% для просмотра видео, в 67% для общения с друзьями и в 53% для подготовки к урокам. 80% опрошенных школьников не могут обойтись без смартфона*. Среднее время, которое подростки проводят в Интернете, составило почти 6 часов в день*. Эта пугающая тенденция приводит к подмене реальных ценностей виртуальными.

Ключевые фигуры IT-отрасли, которые сами занимались разработкой устройств и программ, такие как Билл Гейтс или Стив Джобс, строго ограничивали время использования Интернета и гаджетов в своей семье. До определенного возраста они вообще не разрешали детям пользоваться смартфонами.

Признаки «беды»

1. Ребенок теряет интерес к нахождению на улице, встречам с друзьями или спортивным играм.
2. Ребенок плохо учится в школе, постоянно даже там «сидит» в смартфоне.
3. Ребенок утомляется, плохо спит, жалуется на головные боли и зрительное утомление.
4. У ребенка меняются привычки в еде.
5. Ребенок начинает плохо следить за личной гигиеной.
6. Ребенок заикливается на конкретном сайте или игре.
7. Ребенок крайне агрессивно реагирует на просьбы отвлечься от его виртуальных занятий.
8. Находясь не за компьютером, ребенок ведет себя нервно или раздражительно.
9. Ребенок отдаляется от родителей, перестает разговаривать с ними на личные, волнующие его темы.
10. Ребенок отдаляется от одноклассников и друзей в реальном мире, отдавая предпочтение «виртуальному общению, находит себе лучшего друга «родную душу» в социальных сетях.
11. Ребенок проводит ночное время или часть времени, предназначенного для сна, в социальных сетях или за компьютерными играми.
12. Ребенок резко меняет свое отношение к вопросам, касающимся традиционных духовно-нравственных основ жизни, в частности: патриотизма, милосердия, сострадания, начинает защищать права на нетрадиционные сексуальные отношения, смену пола, гендерную идентичность, идеологию феминизма, чайлдфри и пр.
13. Ребенок проявляет беспричинную агрессию, замкнутость, депрессию, частую смену настроения.
14. На теле ребенка регулярно появляются ссадины, порезы или иные повреждения.

Полезные советы

1. Установите ограничения на то, когда и сколько времени может проводить ваш ребенок в Интернете во внеучебное время.
2. Введите запрет на использование ребенком телефонов, компьютеров и планшетов в ночное время. Общение ребенка через социальные сети и личную переписку в ночное время часто используется преступниками как методика доведения их до самоубийства, вовлечения в опасные квесты, нанесения вреда собственному телу, склонения к разговорам на сексуальные темы и иные виды деструктивного поведения.

* Всероссийский центр изучения общественного мнения

3. Используйте доступные вам технологии – функции родительского контроля! Инструменты для отслеживания времени, проведенного в сети, помогут вам установить рамки допустимого пользования электронными устройствами или Интернетом. Будьте честны с ребенком и объясните, ради чего вы собираетесь использовать эти технологии. Родитель должен знать, чем ребенок занимается в сети! Более подробную пошаговую инструкцию о том, как настроить родительский контроль на разных устройствах можно найти на портале Лиги безопасного Интернета <https://ligainternet.ru/>
4. Отключите уведомления в приложениях социальных сетей, чтобы свести к минимуму отвлекающие факторы.
5. В зависимости от возраста вашего ребенка вы можете составить ежедневный распорядок использования гаджетов для всей семьи, в котором определено время на реальный мир (общение с друзьями и в семье без гаджетов), и время на виртуальный мир. Не противопоставляйте эти два мира, чтобы живое общение не было наказанием! Пусть расписание будет естественно чередовать различные полезные виды деятельности.
6. Не используйте смартфон как средство для освобождения ребенка от вас. Если ребенок слишком рано выйдет в Интернет, это может привести к «цифровой наркомании» и проблемам со здоровьем.
7. Разнообразьте список ваших домашних дел «офлайн» занятиями – например совместными физическими упражнениями, чтением книг или настольными играми.
8. Обсудите возможность запрета использования электронных устройств во время занятий с классным руководителем вашего ребенка, вынесите данный вопрос на рассмотрение родительского собрания для распространения ограничения на всех учеников класса.

Личный пример

Вы можете подать хороший пример независимого поведения ребёнку и сами, сократив свой досуг перед экраном ноутбука или смартфона.

