2 слайд

Государственный орган по надзору в сфере персональных данных – Роскомнадзор – не перестает уделять большое внимание безопасности несовершеннолетних в сети «Интернет». Скорее всего то, что вы сегодня услышите о безопасности в Интернете и о безопасности своих персональных данных, для одних является известными истинами, а для других отчасти новостью. Вы –представители поколения, для которого Интернет-привычная среда обитания, которая сопровождает вас с самого малолетнего возраста. Большинство из вас разбирается в информационных технологиях намного лучше взрослых людей. Тем не менее, необходимо снова и снова говорить о безопасности в сети Интернет и обеспечении безопасности своих персональных данных в сети Интернет и не только.

3 слайд

Виртуальные риски в сети Интернет можно условно разделить на следующие группы:

1. **Нарушение безопасности:** вирусы, трояны, нежелательная почта (спам), он-лайн мошенничества.

2.Риски, связанные с содержанием информации (**контентные риски**): нецензурные тексты, пропаганда экстремизма, нарушение авторских прав, пропаганда наркотиков и др.

3.**Коммуникационные риски**: незаконный контакт, киберпреследование (угрозы, домогательства с использованием информационных технологий, получение информации о пользователе и др.).

Как правило именно третья группа рисков связана с добровольным распространением самим пользователем сети Интернет личной информации о себе.

4 слайд

Говоря о первой категории виртуальных рисков, следует отметить, что часто в Интернете источником опасности являются поддельные сайты, на которые мы можем случайно перейти. С помощью сайтов-подделок злоумышленники крадут пароли, распространяют вредоносное программное обеспечение, навязывают платные услуги. Чтобы этого не произошло, нужно внимательно проверять настоящий адрес сайта, и далее использовать такой функционал браузера как «избранное», «закладки».

5 слайд

Другая беда, которая знакома каждому пользователю Интернета, это спам – массовая рассылка незапрашиваемых получателем электронных сообщений коммерческого содержания. Интересно, что само слово возникло в прошлом столетии задолго до появления Интернета и имело отношение, как ни странно, к мясным консервам. На первый взгляд, получение безобидной «лишней» информации может обернуться непроизвольной оплатой каких-либо услуг, оформление платной подписки на ненужную информацию, потерей учетных данных и прочих неприятностей. Существует множество защитных систем от спама и от пользователя требуется только не пренебрегать сервисами браузера, нацеленными защитить вас от подобных виртуальных угроз.

6 слайд

Вторая категория виртуальных рисков связана с запрещенной информацией в сети интернет.

В целях ограничения доступа к сайтам в сети "Интернет", содержащим информацию, распространение которой в Российской Федерации запрещено, в соответствии с требованиями (приготовьтесь сейчас услышать длинное название закона) статьи 15.1 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" с 01 ноября 2012 года создана и ведется единая автоматизированная

информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено».

В соответствии с Правилами ведения Единого реестра, в электронном виде создана форма для приема обращений о наличии на страницах сайтов в сети «Интернет» запрещенной информации. Эта форма размещена по адресу: указанному на слайде http://eais.rkn.gov.ru.

Роскомнадзор является уполномоченным органом на принятие решений в отношении материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера; информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами, а также является уполномоченным органом по введению в единый реестр сведений о судебных решениях, вступивших в законную силу о признании информация запрещенной к распространению на территории Российской Федерации.

При выявлении случаев размещения неправомерной информации в сети «Интернет», подтвержденной документально (скриншотами), можно воспользоваться открытой формой для приема обращений граждан по указанному адресу в отношении видов информации, по которым уполномоченные органы правомочны принимать решения о признании информации запрещенной.

7 слайд

Находясь на бескрайних просторах виртуального пространства, необходимо помнить, что все, что делаете Вы и что делают другие пользователи, имеет непосредственное отношение к реальной жизни. В том числе, и ответственность за виртуальные правонарушения тоже вполне реальна. На слайде представлен неполный перечень незаконных действий,

возможных в сети Интернет, за которые предусмотрено весьма существенная мера ответственности.

8 слайд

И, наконец, третья категория виртуальных угроз, о которой было сказано ранее, непосредственно связана с одним из направлений деятельности Роскомнадзора, а именно с защитой прав субъектов персональных данных.

9 слайд

Необходимо рассказать о существовании портала «Персональные данные. Дети», на котором доступно и понятно раскрыты многие понятия, связанные с персональными данными, размещены игры и тесты на данную тему. Если вы еще не были на этом портале, рекомендуем его посетить.

10 слайд

Итак, что же такое персональные данные? Если не использовать сухой текст закона «О персональных данных» (№ 152-ФЗ), то можно сказать, что персональные данные- это твоя частная собственность, как записная книжка, ключи от квартиры и прочее. Прежде чем делать персональную информацию общедоступной, следует подумать, а стОит ли.

Представляется важным донести до пользователей сети «Интернет» следующие основные «правила» пользования Интернет - платформами (социальными сетями):

- ознакомление с правилами пользования (пользовательскими соглашениями), а также политикой администратора ресурса в отношении обработки персональных данных и обеспечения их сохранности;

- использование настроек приватности профилей в социальных сетях («только для друзей») и взвешенного подхода к объему размещаемой в сети Интернет личной информации;

- исключение указания при регистрации на различных Интернет - сервисах избыточных, не являющихся обязательными сведений, носящих персональный характер (принцип «не больше, чем достаточно»).

Как общаться в сети

1. Старайтесь не выкладывать в Интернет личную информацию (фотографии, видео, ФИО, дату рождения, адрес дома, номер школы, телефоны и иные данные) или существенно сократите объем данных, которые публикуете в «Интернете».
2. Не выкладывайте личную информацию (совместные фотографии, видео, иные данные) о ваших друзьях в «Интернет» без их разрешения. Прежде чем разместить информацию о друзьях в Сети, узнайте, не возражают ли они, чтобы вы выложили данные.
3. Не отправляйте свои персональные данные, а также свои видео и фото людям, с которыми вы познакомились в «Интернете», тем более если вы не знаете их в реальной жизни.
4. При общении с другими пользователями старайтесь быть вежливыми, деликатными, тактичными и дружелюбными. Не пишите грубостей, оскорблений – читать такие высказывания так же неприятно, как и слышать.
5. Старайтесь не реагировать на обидные комментарии, хамство и грубость других пользователей. Всегда пытайтесь уладить конфликты с пользователями мирным путем, переведите все в шутку или прекратите общение с агрессивными пользователями. Ни в коем случае не отвечайте на агрессию тем же способом.
6. Если решить проблему мирным путем не удалось, напишите жалобу администратору сайта, потребуйте заблокировать обидчика.

7. Если администратор сайта отказался вам помочь, прекратите пользоваться таким ресурсом и удалите оттуда свои данные.
8. Не используйте Сеть для распространения сплетен, угроз или хулиганства.

11 слайд

Данные статистики показывают, что чуть менее половины опрошенных понимают, что их личные данные при размещении в сети Интернет могут быть использованы другими людьми в собственных целях. 34% опрошенных это беспокоит, но и достаточно тех, кто относится к этому вопросу крайне беспечно.

12 слайд

По данным той же статистики, больше половины опрошенных все-таки осознают, что защита ПД – это в первую очередь их обязанность, 34% разделяют эту обязанность с государством и другими лицами, и пусть совсем небольшой процент, но есть и такие пользователи, которые не считают своей обязанностью защищать свои ПД.

13 слайд

На следующем слайде приведена интересная информация о самых популярных паролях среди пользователей интернет. Это говорит о том, что чтобы защитить свою личную информацию с помощью пароля, необходимо проявить оригинальность в его выборе, чтобы не быть предсказуемым для злоумышленников.

14 слайд

Не стоит забывать, что огромное количество личной информации содержится в ваших мобильных устройствах: и контакты, и личные фото/видео, данные доступа к электронной почте и аккаунтам в социальных сетях. Могут быть также данные о банковских картах и платежах.

Поскольку телефон теперь не просто средство связи или красивая игрушка, а полноценное коммуникационное устройство, не уступающее по производительности и функционалу персональному компьютеру, нужно соблюдать все необходимые меры предосторожности, например, при установке мобильных приложений, использовании доступа к Интернету посредством Wi-Fi.

Простые правила помогут вам избежать больших неприятностей:

- установи мобильную версию антивируса на своё мобильное устройство;
- установи приложения, шифрующие твои данные - они защитят личные файлы;
- устанавливай приложения только из проверенных источников;
- отключи функцию автоподключения к открытым Wi-Fi сетям;
- используй только защищённые Wi-Fi сети;
- обязательно правильно завершай работу с публичным Wi-Fi;
- внимательно изучай права, запрашиваемые мобильными приложениями;
- используй только проверенные мобильные сервисы.

16 слайд

И в заключении хотелось бы сказать - Будьте внимательны! Будьте бдительны! Будьте ответственны! Ведь во многом от этого зависит возможность реализации безопасности в сети Интернет. Без вашего участия ни один государственный орган не обеспечит в полной мере вашу защиту в Интернете. Только совместными усилиями в этом вопросе можно достигнуть успеха!