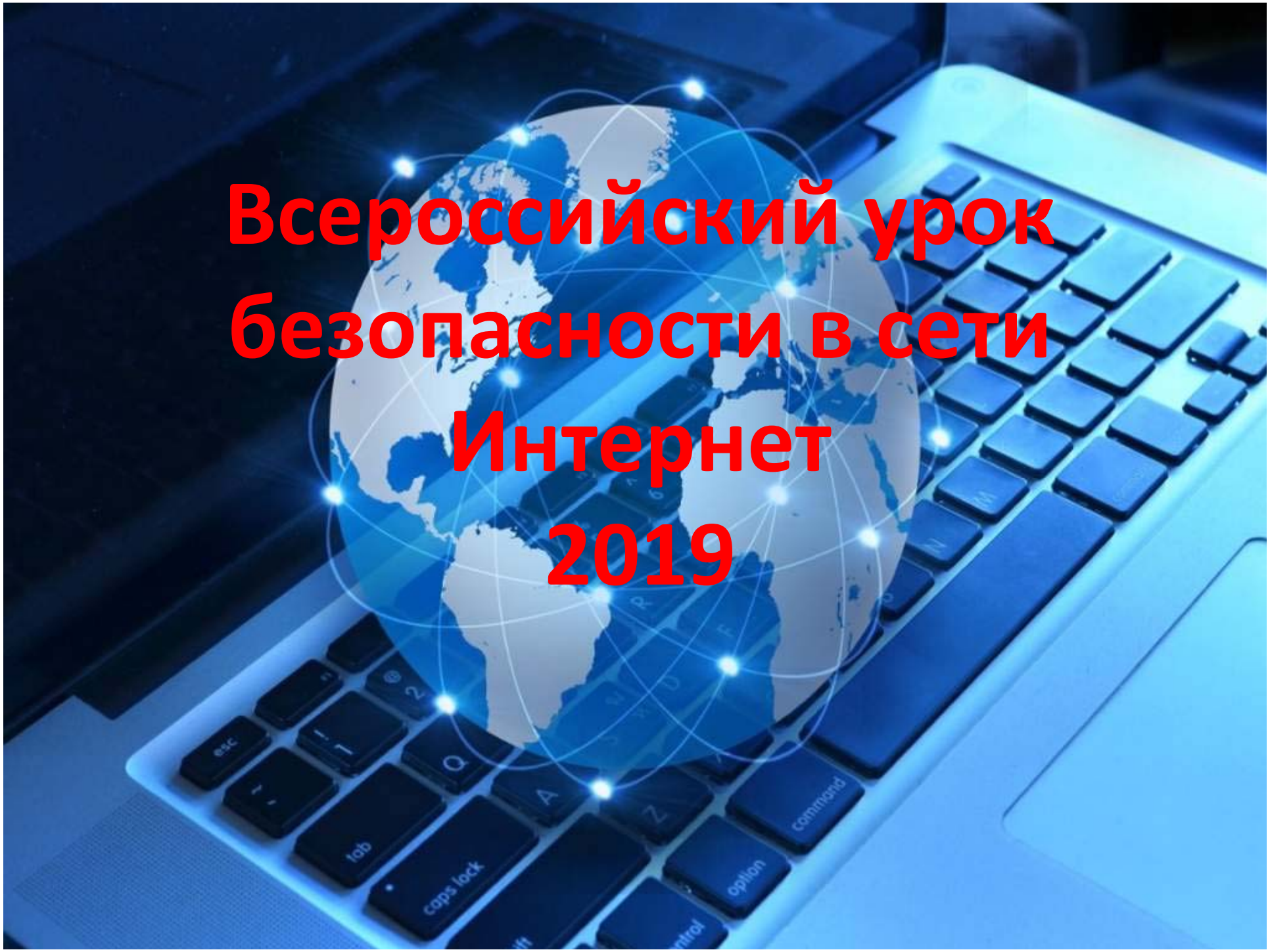


Всероссийский урок безопасности в сети Интернет 2019

Современный мир – это мир компьютерной техники

Наряду с огромными возможностями Интернета как высокотехнологичного источника коммуникации и инструмента поиска и получения информации, проблема безопасности подростков в сети «Интернет» становится очень актуальной.

На главную

Основные угрозы безопасности в Интернете

- Загрузка вредоносных программ
- Опасный контент
- Интернет-травля
- Интернет - хищники
- Интернет - мошенники

Загрузка вредоносных программ

Возможна при загрузке файлов, программ или музыки из случайных источников

На главную

Опасный контент

Опасным можно назвать различные материалы, содержащие:

- сцены насилия
- сцены неоправданной агрессии
- эротика и порнография
- нецензурная лексика
- информация, разжигающая расовую ненависть
- пропаганда нездорового образа жизни, неправильного питания
- пропаганда употребления наркотических веществ
- мошенническая информация
- азартные игры

На главную

Интернет-травля

осуществляется посредством

- электронной почты
- программ для мгновенного обмена сообщениями в социальных сетях,
- через размещения на видеопорталах

непристойных видеоматериалов

- мобильного телефона (с помощью SMS-сообщений или надоедливых звонков).

На главную

Интернет - хищники

используют социальные сети, чаты, мессенджеры, интернет - форумы и другие социальные средства коммуникации для общения с детьми и подростками с целью склонить их к незаконным действиям различного характера

На главную

Интернет - мошенники

Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким -либо образом использует личную **информацию** пользователя, с целью получить материальную прибыль

На главную

Компьютерные вирусы

- Загрузочные
- Файловые
- Макро – вирусы
- Скрипт – вирусы

На главную

КАКИМ ОБРАЗОМ ЗЛОУМЫШЛЕННИКИ МОГУТ ПОЛУЧИТЬ ДОСТУП К ВАШЕМУ КОМПЬЮТЕРУ?

Первый приём. **Социальная инженерия**.

Это метод управления действиями человека без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным.

Сегодня социальную инженерию зачастую используют в интернете для получения закрытой информации, или информации, которая представляет большую ценность. Благодаря использованию уловок и психологических приемов, вы открываете присланное хакерами письмо, содержащее вирус.

Второй приём. Фишинг («рыбалка»).

В интернете создаются подделки популярных сайтов и пользователи «клюют на эту наживку». Так вместо официальной страницы своего банка вы можете оказаться на его поддельной копии со всеми вытекающими последствиями.

Третий приём. Предложение бесплатного программного обеспечения.
Это как правило уловки, содержащие в себе множество вирусов и троянов.

Троя́нская программа (также — **троя́н**, **троя́нец**, **троя́нский конь**) — это разновидность вредоносной программы, проникающая в компьютер под видом легального программного обеспечения, в отличие от *вирусов* и *червей*, которые распространяются самопроизвольно.

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: *сбор информации и её передачу злоумышленнику, её разрушение или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.*

Четвёртый приём. Блокирование операционной системы.

Еще один простой вариант получить доступ к ПК пользователя и его деньгам – заблокировать операционную систему и потребовать некоторые сведения и некоторую сумму за ее разблокировку.

Советы по безопасной работе в сети Интернет

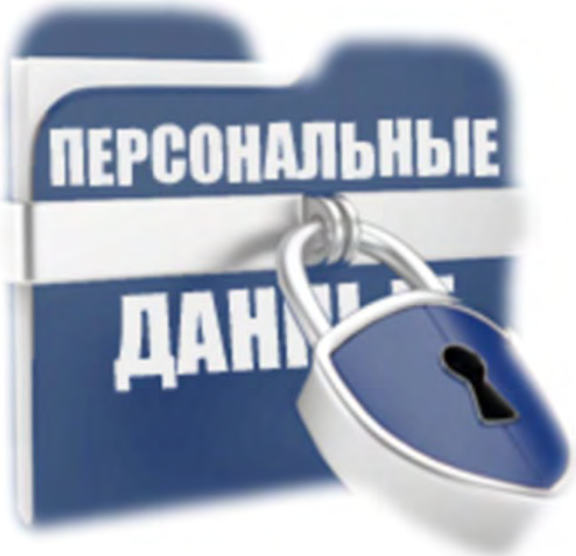
На главную

Сложный пароль

Чем сложнее пароль, тем сложнее взломать твой аккаунт

На главную

Личная информация



Никогда не рассказывай о себе незнакомым людям в Интернете: где ты живешь и учишься, не давай свой номер телефона.

Не говори никому о том, где работают твои родители, не сообщай номера их телефонов

На главную

Самые эффективные антивирусные программы

- Антивирус лаборатории Касперского
- Доктор Web
- NOD 32
- AVAST

На главную

КАК ОБЕСПЕЧИТЬ ЗАЩИТУ ПК

1. Не открывать файлы, скачанные из непроверенных источников.
2. Сразу удалять письма подозрительного содержания.
3. Не обращать внимания на предложения легкого заработка, и уж тем более, не высылать никому своих логинов и паролей.
4. При регистрации использовать сложные пароли из символов, букв и цифр. Назначайте каждый раз новый оригинальный пароль.
5. Соблюдать осторожность, используя интернет в местах общего пользования.
6. С платежными системами безопаснее работать через специальные приложения, а не через официальный сайт.
7. Следить за интернет-трафиком. Резкое увеличение трафика безо всякой причины – серьезный повод для беспокойства.
8. Игнорировать сообщения о крупных выигрышах или получении наследства.
9. Использовать лицензионное ПО.
10. Использовать только проверенные варианты при совершении покупок в интернет – магазинах.

ПЯТЬ ПРАВИЛ БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

1. Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу удалите их.

2. Никогда не отвечайте на спам.

3. Применяйте фильтр спама или программы работы с электронной почтой.

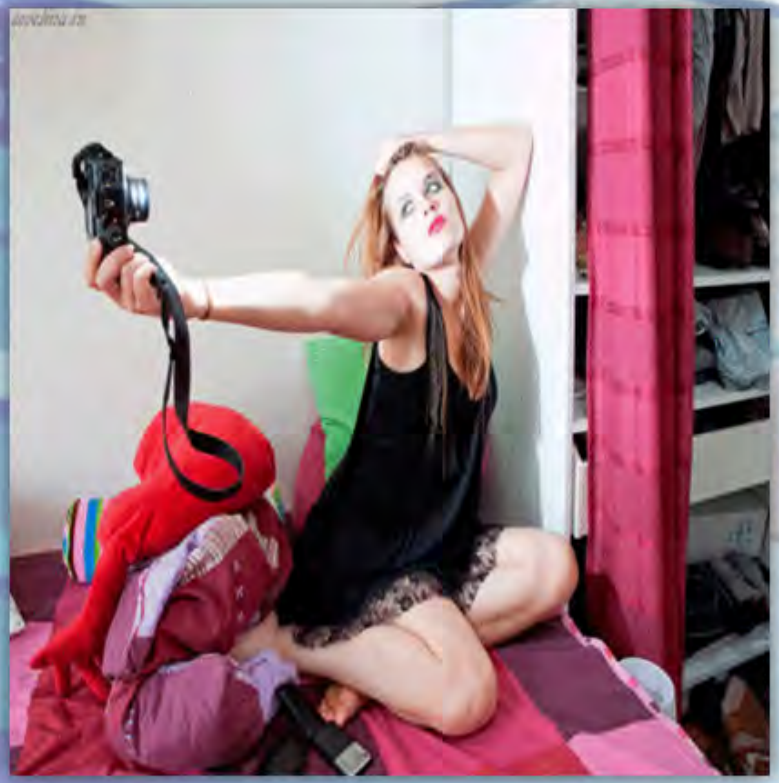
4. Создайте новый или используйте семейный адрес электронной почты для Интернет-запросов, дискуссионных форумов и т.д.

5. Никогда не пересылайте «письма счастья». Вместо этого сразу удаляйте их.

Раньше СМИ отвечали за каждое своё слово, а в Интернете царила свобода. Сегодня по количеству введённых запретов для пользователей Интернета российские законодатели перегнали многие развитые страны.

ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

- Не заполняйте все поля вашего профиля.
- Не нужно выкладывать в социальных сетях откровенные фотографии.



- Не регистрируйтесь под чужими данными. Если хотите сохранить инкогнито – прибегните к вымышленному имени.
- Не используйте чужие изображения без разрешения этих людей.
- Никогда не используйте социальную сеть или иной подобный сервис в качестве основного хранилища информации.

- Не участвуйте в сомнительных акциях.
- НИКОГДА не переходите по длинным ссылкам, это чаще всего путь к зараженному вирусом файлу.
- Соблюдайте культуру общения в сети.

- Не пишите в ленте о своих сомнительных с точки зрения закона «подвигах».
- Не добавляйте в друзья всех подряд.
- Не вступайте в сомнительные сообщества, куда вас приглашают непонятные люди.

ОТВЕТСТВЕННОСТЬ ЗА ИНФОРМАЦИОННЫЕ ПРАВОНАРУШЕНИЯ

Виды ответственности:

- Административная ответственность;
- Уголовная ответственность;
- Дисциплинарная ответственность;
- Гражданско-правовая ответственность.

Ответственность за экстремистские действия в сети

- **Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма**

  От штрафа в размере до 500 тысяч рублей до лишения свободы на срок от 2 до 5 лет.

- **Распространение личной или семейной тайны человека**

  От возмещения морального ущерба до лишения свободы на срок до 2 лет.

- **Реабилитация нацизма**

  От штрафа до 300 тысяч рублей до лишения свободы на срок до 3 лет.

- **Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности России**

  От штрафа в размере от 100 до 300 тысяч рублей до лишения свободы на срок до 5 лет.

Список экстремистских материалов опубликован на сайте Минюста.
http://minjust.ru/ru/extremist-materials.

гл. 28 «Преступления в сфере компьютерной информации» Уголовного Кодекса РФ

Статья 272. Неправомерный доступ к компьютерной информации

Т.е. информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ или их сети, то предусматривается наказание от

штрафа в размере до 200 000 до лишения свободы на срок до 2 лет.

То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, - наказывается:

штрафом в размере от 100 000 до 300 000 р. либо лишением свободы на срок до 5 лет.

или штраф в размере зар. платы или иного дохода осужденного за период от 1 года до 2-х лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

Заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети наказываются:

лишением свободы на срок до 3-х лет со штрафом в размере до 200 000 р.;

Те же деяния, повлекшие по неосторожности тяжкие последствия, наказываются лишением свободы на срок от 3 до 7 лет.

Если соблюдать эти простые правила, то работа в Интернете станет безопасной, полезной и увлекательной.