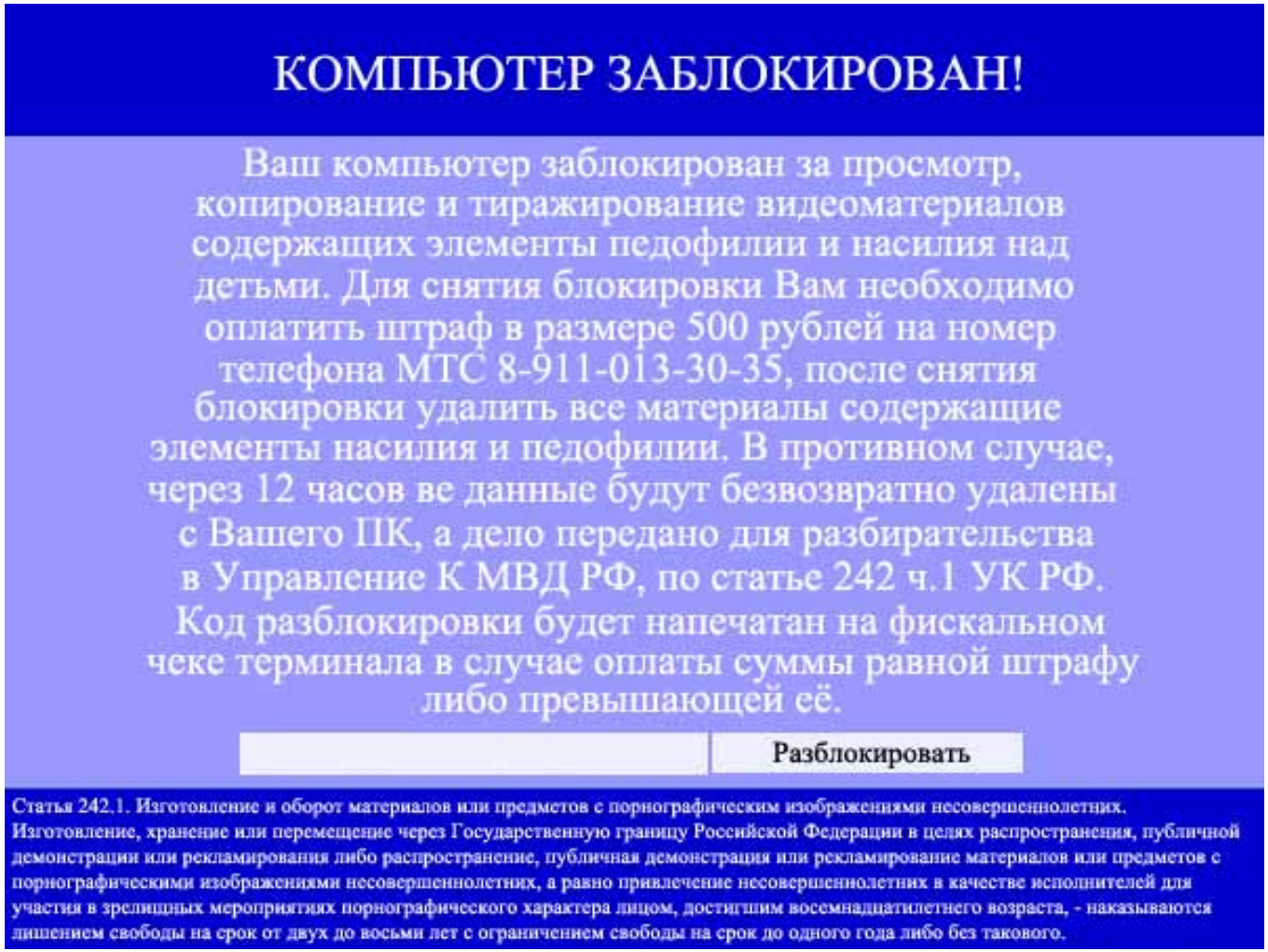
Вирусы и антивирусы

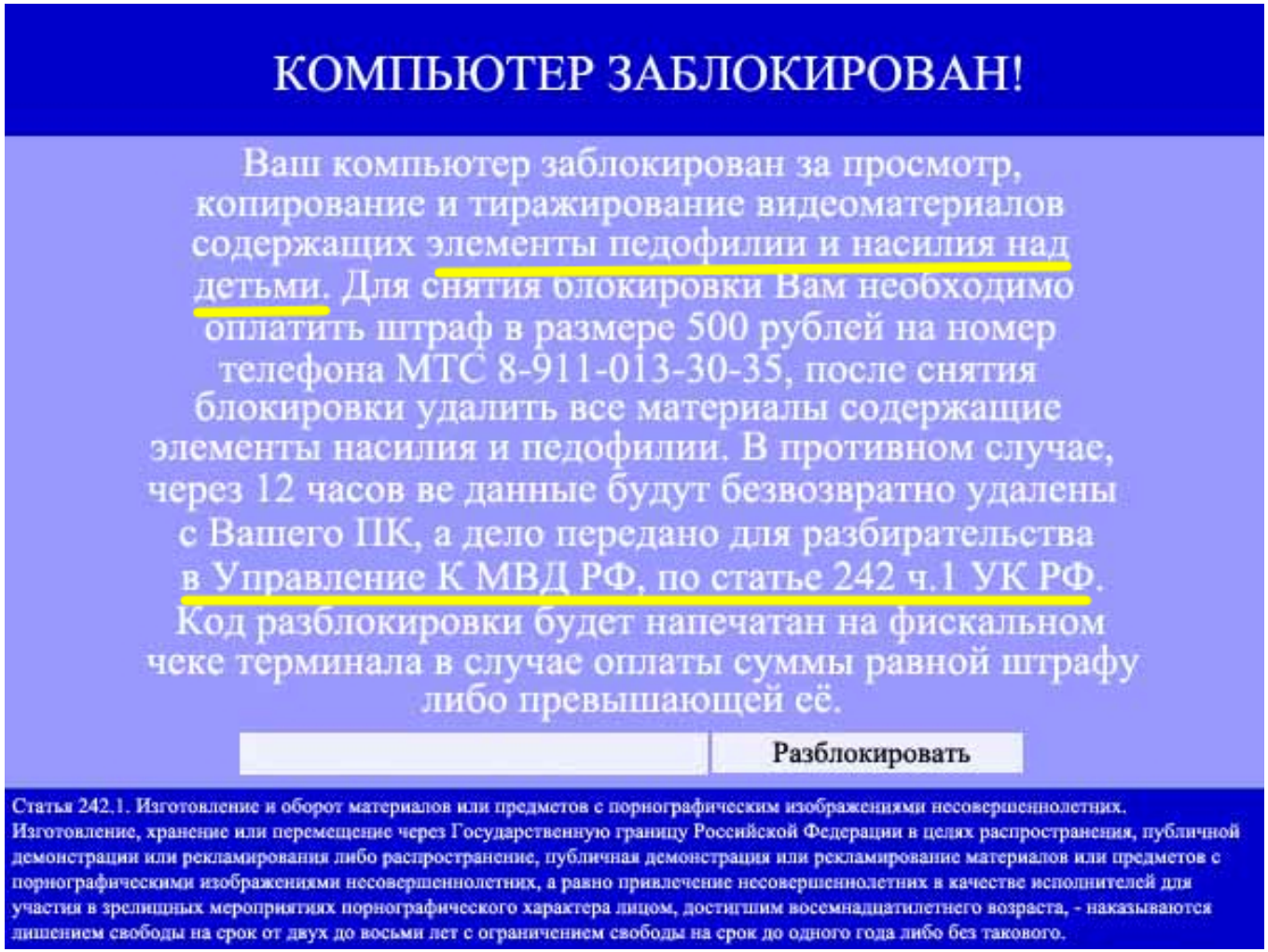
Информатика
10-11 классы

5 октября 2011 г.

Вместо введения



Вместо введения



Что такое *вирус*?

- *Компьютерный вирус* — разновидность вредоносных компьютерных программ, отличительной особенностью которых является способность к размножению и/или самосохранению.

Что такое *вирус*?

- *Компьютерный вирус* — разновидность вредоносных компьютерных программ, отличительной особенностью которых является способность к размножению и/или самосохранению.
- В 1981 году Ричард Скрента написал один из первых загрузочных вирусов для Apple II — ELK CLONER. Он обнаруживал своё присутствие сообщением, содержащим небольшое стихотворение:

ELK CLONER:
THE PROGRAM WITH A PERSONALITY
IT WILL GET ON ALL YOUR DISKS
IT WILL INFILTRATE YOUR CHIPS
YES, IT'S CLONER
IT WILL STICK TO YOU LIKE GLUE
IT WILL MODIFY RAM, TOO
SEND IN THE CLONER!

История вирусов

- Первые вирусы зачастую не влияли глобально на работоспособность компьютера и/или сохранность информации.

История вирусов

- Первые вирусы зачастую не влияли глобально на работоспособность компьютера и/или сохранность информации.
- Первый сетевой червь (*червь Морриса*) появился в 1988 году. Задумывавшийся как безвредный, тем не менее, он причинил ущерба на сумму около 100.000.000$.

История вирусов

- Первые вирусы зачастую не влияли глобально на работоспособность компьютера и/или сохранность информации.
- Первый сетевой червь (*червь Морриса*) появился в 1988 году. Задумывавшийся как безвредный, тем не менее, он причинил ущерба на сумму около 100.000.000$.
- Автор понёс наказание в виде 2 лет условно + 400 часов работ + 10.000$.

История вирусов

- Первые вирусы зачастую не влияли глобально на работоспособность компьютера и/или сохранность информации.
- Первый сетевой червь (*червь Морриса*) появился в 1988 году. Задумывавшийся как безвредный, тем не менее, он причинил ущерба на сумму около 100.000.000$.
- Автор понёс наказание в виде 2 лет условно + 400 часов работ + 10.000$.
- Начиная с 1990 года вирусы приобрели характер глобальной эпидемии.

Источник

1. Накопители (USB флэшки, карты памяти, DVD/CD диски),

Источник

1. Накопители (USB флэшки, карты памяти, DVD/CD диски),
2. e-mail (картинки, объекты, архивы),

Источник

1. Накопители (USB флэшки, карты памяти, DVD/CD диски),
2. e-mail (картинки, объекты, архивы),
3. фишинг и социальный инжениринг,

Источник

1. Накопители (USB флэшки, карты памяти, DVD/CD диски),
2. e-mail (картинки, объекты, архивы),
3. фишинг и социальный инжениринг,
4. Интернет (устаревшие браузеры, уязвимости в плагинах типа Flash, уязвимости в ОС, установка заражённых программ)

Пару слов о фишинге

Yndex деньги

Уважаемый пользователь,

Согласно пункту 4.4.3.6. Соглашения об использовании Системы "Яндекс.Деньги", Ваш аккаунт должен пройти реактивацию счета в системе.

Для выполнения реактивации проследуйте по ссылке:

https://money.yandex.ru/login.php?passport=OWELB&idkey=324389205282404&ncmd=627958

Либо свяжитесь с одним из наших операторов:

ООО "ПС Яндекс.Деньги". 101049, г. Москва, ул. Вавилова, дом 40
тел.: +7 (495) 739-03-60

ООО "ПС Яндекс.Деньги", Петербургский филиал. 191190, г. Санкт-Петербург, ул. Радищева, д. 36,
тел.: +7 (812) 334-30-46

Письмо сгенерировано автоматически, пожалуйста, не отвечайте на него.

С уважением, ООО "ПС Яндекс.Деньги"

Дизайн ≈
Студия Артемия Лебедева

Copyright 2002 - 2006
"Яндекс", "PayCash"
Мобильная версия

2007 "ПС Яндекс.Деньги"
О проекте
Статистика
Реклама
Обратная связь

Пару слов о фишинге

1. Пользователям отправляется информация с просьбой зайти на определённый сайт и ввести данные.

Пару слов о фишинге

1. Пользователям отправляется информация с просьбой зайти на определённый сайт и ввести данные.
2. Сайт может быть очень похож на реальный, включая дизайн и доменное имя (google.com vs gooogle.com).

Пару слов о фишинге

1. Пользователям отправляется информация с просьбой зайти на определённый сайт и ввести данные.
2. Сайт может быть очень похож на реальный, включая дизайн и доменное имя (google.com vs gooogle.com).
3. Как вариант: злоумышленник может требовать отправить SMS / некоторую сумму $ для активации / разблокировки и пр.

Пару слов о фишинге

1. Пользователям отправляется информация с просьбой зайти на определённый сайт и ввести данные.
2. Сайт может быть очень похож на реальный, включая дизайн и доменное имя (google.com vs gooogle.com).
3. Как вариант: злоумышленник может требовать отправить SMS / некоторую сумму $ для активации / разблокировки и пр.
4. Рассылки могут быть направленными!

Пару слов о фишинге

1. Пользователям отправляется информация с просьбой зайти на определённый сайт и ввести данные.
2. Сайт может быть очень похож на реальный, включая дизайн и доменное имя (google.com vs gooogle.com).
3. Как вариант: злоумышленник может требовать отправить SMS / некоторую сумму $ для активации / разблокировки и пр.
4. Рассылки могут быть направленными!
5. Вкупе с червями эффект увеличивается в разы.

Необходимое условие

Советы народных целителей

КОМПЬЮТЕРЫ

ЗАЩИТА ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

Включите компьютер и запустите дефрагментацию жесткого диска. Пока ваша машина занята переразмещением файлов, аккуратно протрите корпус процессора, монитор, дисководы и клавиатуру от пыли. При этом произносите:

Зевс, Меркурий, Аполлон,
Сохрани компьютер мой!
Вирус будет побежден,
Он не встретится со мной!

ОБЩАЯ ЗАЩИТА КОМПЬЮТЕРА

Предлагаю вам отличное заклинание, прекрасно подходящее для любого компьютера, но особенно для только что приобретенного.

Кардинальный метод

Реальный метод

1. Делать только то, что понимаешь.

Реальный метод

1. Делать только то, что понимаешь.
2. Скачивать и устанавливать программы / контент с **проверенных** ресурсов.

Реальный метод

1. Делать только то, что понимаешь.
2. Скачивать и устанавливать программы / контент с **проверенных** ресурсов.
3. Постоянно (**каждый день!**) обновлять систему и ПО.

Реальный метод

1. Делать только то, что понимаешь.
2. Скачивать и устанавливать программы / контент с **проверенных** ресурсов.
3. Постоянно (**каждый день!**) обновлять систему и ПО.
4. Использовать антивирусы **И** файерволлы.

Реальный метод

1. Делать только то, что понимаешь.
2. Скачивать и устанавливать программы / контент с **проверенных** ресурсов.
3. Постоянно (**каждый день!**) обновлять систему и ПО.
4. Использовать антивирусы **И** файерволлы.
5. Для сёрфинга использовать Firefox / Safari / Chrome с выключенными плагинами (типа Flash, Java и пр.).

Реальный метод

1. Делать только то, что понимаешь.
2. Скачивать и устанавливать программы / контент с **проверенных** ресурсов.
3. Постоянно (**каждый день!**) обновлять систему и ПО.
4. Использовать антивирусы **И** файерволлы.
5. Для сёрфинга использовать Firefox / Safari / Chrome с выключенными плагинами (типа Flash, Java и пр.).
6. Перейти на Linux / Mac OS X

Защита от фишинга и инженирии

1. Сначала думать, потом делать.

Защита от фишинга и инженирии

1. Сначала думать, потом делать.
2. Использовать сложные пароли, не хранить их в текстовых файлах / открытом виде.

Защита от фишинга и инженирии

1. Сначала думать, потом делать.
2. Использовать сложные пароли, не хранить их в текстовых файлах / открытом виде.
3. **Никогда** не вводить важные логины и пароли на “левых” сайтах. Только на известных.

Защита от фишинга и инженирии

1. Сначала думать, потом делать.
2. Использовать сложные пароли, не хранить их в текстовых файлах / открытом виде.
3. **Никогда** не вводить важные логины и пароли на “левых” сайтах. Только на известных.
4. Понять, что халявы не бывает.

Защита от фишинга и инженирии

1. Сначала думать, потом делать.
2. Использовать сложные пароли, не хранить их в текстовых файлах / открытом виде.
3. **Никогда** не вводить важные логины и пароли на “левых” сайтах. Только на известных.
4. Понять, что халявы не бывает.
5. Понять, что Дуров — не идиот, и не будет вводить платные SMS-ки для школоты.

Защита от фишинга и инженирии

1. Сначала думать, потом делать.
2. Использовать сложные пароли, не хранить их в текстовых файлах / открытом виде.
3. **Никогда** не вводить важные логины и пароли на “левых” сайтах. Только на известных.
4. Понять, что халявы не бывает.
5. Понять, что Дуров — не идиот, и не будет вводить платные SMS-ки для школоты.
6. При проблеме **сначала** посоветоваться с Google.

Защита от фишинга и инженирии

1. Сначала думать, потом делать.
2. Использовать сложные пароли, не хранить их в текстовых файлах / открытом виде.
3. **Никогда** не вводить важные логины и пароли на “левых” сайтах. Только на известных.
4. Понять, что халявы не бывает.
5. Понять, что Дуров — не идиот, и не будет вводить платные SMS-ки для школоты.
6. При проблеме **сначала** посоветоваться с Google.
7. Поднимать свой уровень знаний о компьютере.

Mikko Hypponen

1. Директор антивирусной компании F-Secure.

Mikko Hypponen

1. Директор антивирусной компании F-Secure.
2. Офисы более чем в 100 странах.

Mikko Hypponen

1. Директор антивирусной компании F-Secure.
2. Офисы более чем в 100 странах.
3. Home: mikko.hypponen.com.

Mikko Hypponen

1. Директор антивирусной компании F-Secure.
2. Офисы более чем в 100 странах.
3. Home: mikko.hypponen.com.
4. Twitter: @mikkohypponen.

Mikko Hypponen

1. Директор антивирусной компании F-Secure.
2. Офисы более чем в 100 странах.
3. Home: mikko.hypponen.com.
4. Twitter: @mikkohypponen.
5. Беседа о вирусах.

Mikko Hypponen

1. Директор антивирусной компании F-Secure.
2. Офисы более чем в 100 странах.
3. Home: mikko.hypponen.com.
4. Twitter: @mikkohypponen.
5. Беседа о вирусах.
6. Short link: http://goo.gl/duqGk

Будущее юных хакеров

- Википедия (http://wikipedia.org),
- Google :),
- TED (http://ted.com),
- Множеству сайтов, которые распарсил Google, из которого были взяты замечательные картинки.