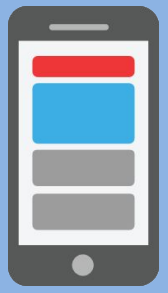
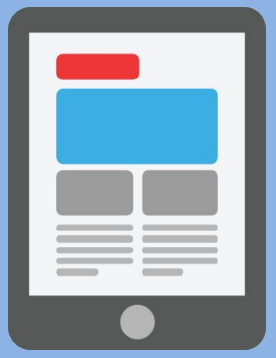
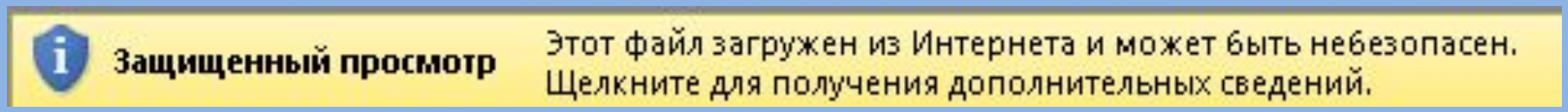
лига безопасного интернета

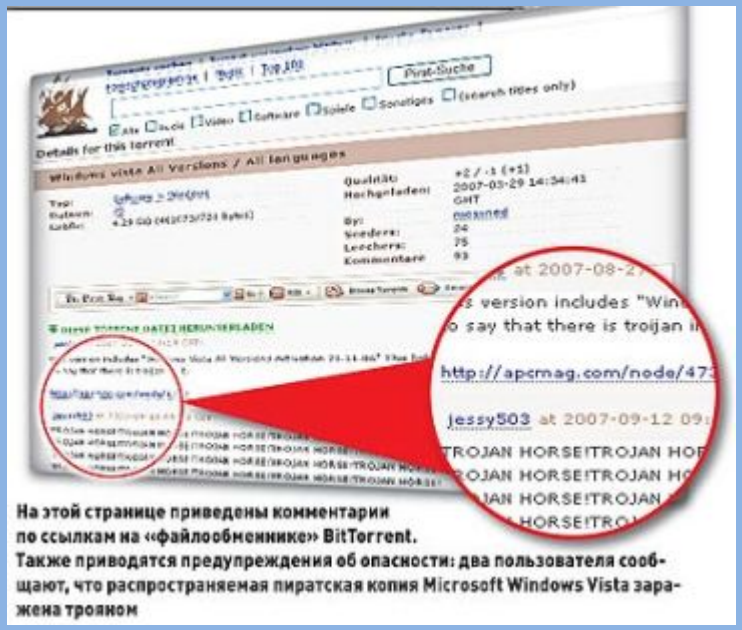
ЕДИНЫЙ УРОК БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ





ВРЕДОНОСНЫЕ ПРОГРАММЫ

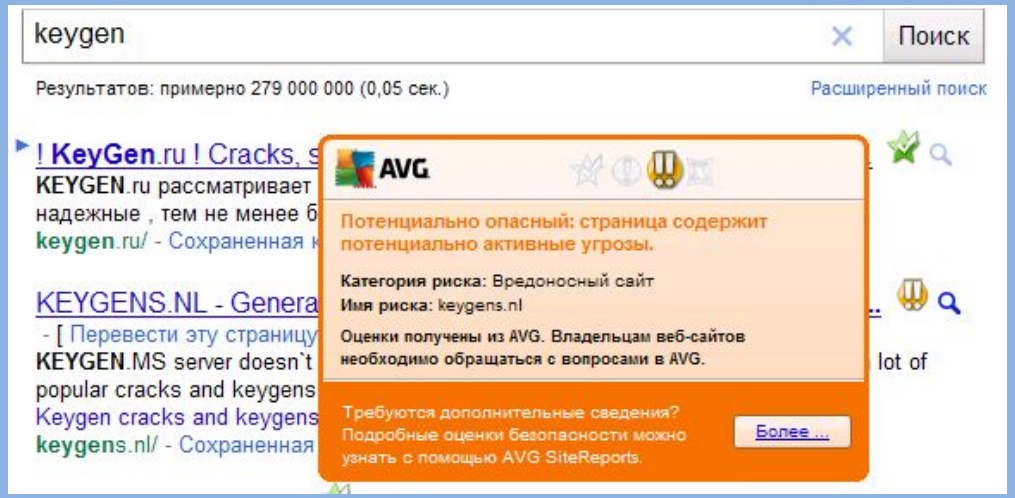




Внимание!

В пиратских версиях троян отключает проверку лицензии…

Что он делает еще?



Вредоносные программы часто маскируются:

- Картинки
- Музыка
- Видео
- Кряки
- Другие программы

Троян в пиратке… Вор у вора крадет?

Компьютерный вирус – это специальная компьютерная программа обычно малая по размеру, которая способна «размножаться» и «заражать» другие программы. Другими словами она многократно копирует свой код и присоединяет его к кодам других программ.

Программа, внутри которой находится вирус, называется **«зараженной».**

Основные признаки проявления вирусов:

1. прекращение работы или неправильная работа ранее успешно функционировавших программ;
2. медленная работа компьютера;
3. исчезновение файлов и папок или искажение содержимого;
4. изменение размеров файла;
5. неожиданное значительное увеличение файлов на диске;
6. уменьшение размера оперативной памяти;
7. частые зависания и сбои в работе компьютера.

Каналы распространения:

- **Дискеты, диски**
- **Флеш-накопители** (флешки — основной источник заражения для компьютеров, не подключённых к сети Интернет)
- **Электронная почта** (обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты)
- ***Системы обмена мгновенными сообщениями.***
- Так же распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.
- ***Веб-страницы.***
- Возможно также заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого.
- ***Интернет и локальные сети (черви)***
- Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер.

Червь (сетевой червь)- это вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом.

- **Особенностью червей**, отличающих их от других вирусов, является то, что они не несут в себе ни какой вредоносной нагрузки, кроме саморазмножения, целью которого является замусоривание памяти, и как следствие, затормаживание работы операционной системы.

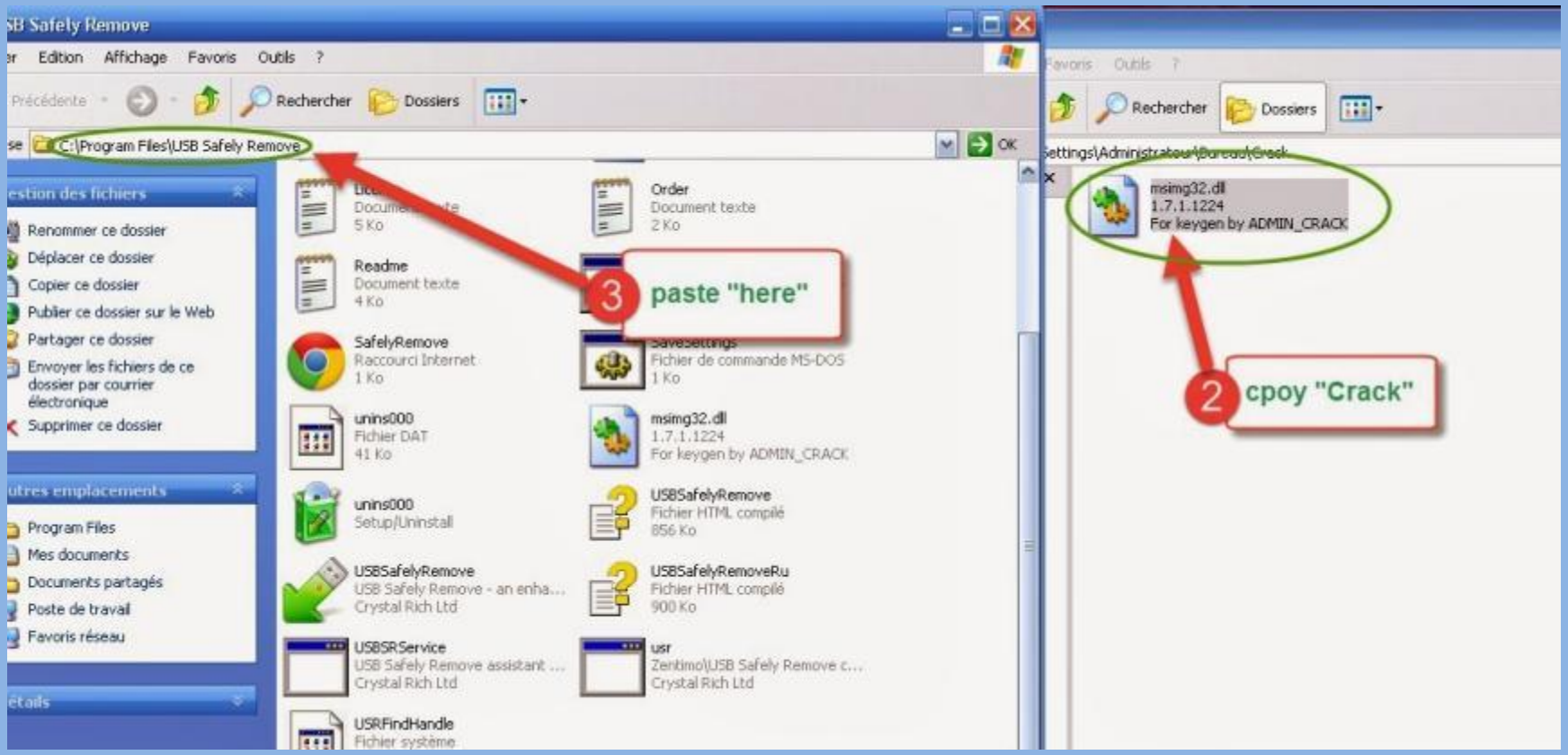
Троян (троянский конь) – программа, основной целью которой является вредоносное воздействие по отношению к компьютерной системе.

- Некоторые трояны способны к самостоятельному преодолению систем защиты компьютерной системы, с целью проникновения в нее. Однако в большинстве случаев они проникают на компьютеры вместе с вирусом либо червем - то есть такие трояны можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу. Нередко пользователи сами загружают троянские программы из Интернет.

Целью троянской программы может быть:

- закачивание и скачивание файлов;
- копирование ложных ссылок, ведущих на поддельные вебсайты, чаты или другие сайты с регистрацией;
- создание помех работе пользователя;
- кража данных, представляющих ценность или тайну, в том числе информации для аутентификиции, для несанкционированного доступа к ресурсам, выуживание деталей касательно банковских счетов, которые могут быть использованы в преступных целях;
- распространение других вредоносных программ, таких как вирусы;
- уничтожение данных (стирание или переписывание данных на диске, труднозамечаемые повреждения файлов) и оборудования, выведения из строя или отказа обслуживания компьютерных систем, сетей;
- сбор адресов электронной почты и использование их для рассылки спама;
- слежка за пользователем и тайное сообщение третьим лицам сведений, таких как, например, привычка посещать конкретные сайты;
- регистрация нажатий клавиш с целью кражи информации такого рода как пароли и номера кредитных карточек;
- дезактивация или создание помех работе антивирусных программ и файервола;

«Кряк»


SB Safely Remove
Edition Affichage Favoris Outils ?
Précédente
Rechercher
Dossiers
C:\Program Files\USB Safely Remove
OK
estion des fichiers
Renommer ce dossier
Déplacer ce dossier
Copier ce dossier
Publier ce dossier sur le Web
Partager ce dossier
Envoyer les fichiers de ce dossier par courrier électronique
Supprimer ce dossier
utres emplacements
Program Files
Mes documents
Documents partagés
Poste de travail
Favoris réseau
etails
Order
Document texte
2 Ko
Readme
Document texte
4 Ko
3 paste "here"
SafelyRemove
Raccourci Internet
1 Ko
Fichier de commande MS-DOS
1 Ko
unins000
Fichier DAT
41 Ko
msimg32.dll
1.7.1.1224
For keygen by ADMIN_CRACK
unins000
Setup/Uninstall
USBSafelyRemove
Fichier HTML compilé
856 Ko
USBSafelyRemove
USB Safely Remove - an enha...
Crystal Rich Ltd
USBSafelyRemoveRu
Fichier HTML compilé
900 Ko
USBSRService
USB Safely Remove assistant ...
Crystal Rich Ltd
usr
Zentimo\USB Safely Remove c...
Crystal Rich Ltd
USRFindHandle
Fichier système
Favoris Outils ?
Rechercher
Dossiers
msimg32.dll
1.7.1.1224
For keygen by ADMIN_CRACK
2 cpoy "Crack"

Профилактика

- 1. пользуйтесь только лицензионными программами и операционными системами

- 2. постоянно обновляйте операционную систему
- 3. не забывайте и специальных средствах защиты — антивирусах и файерволлах.

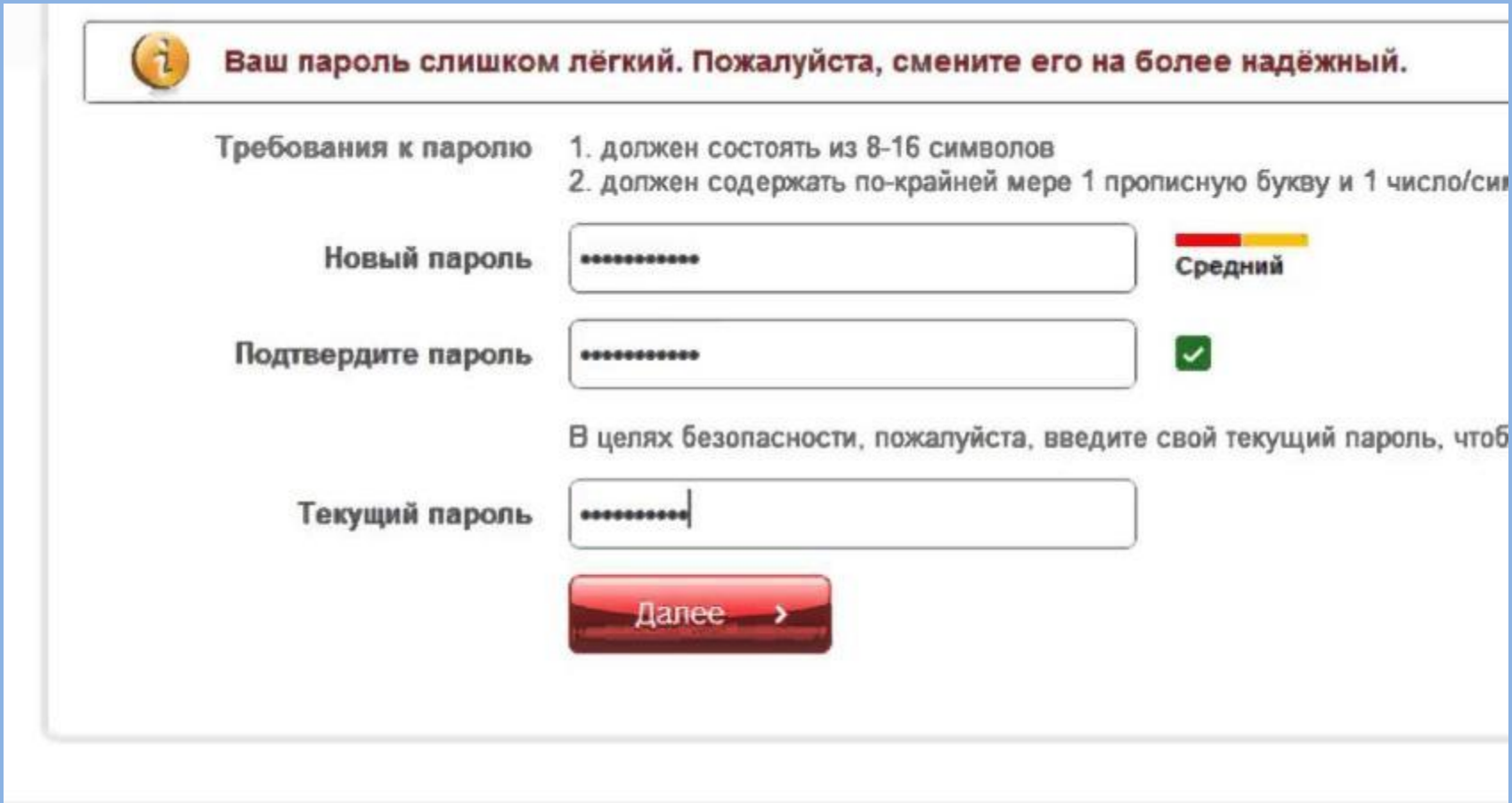
- **Антиви́русная програ́мма (антиви́рус)** — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Файервол (брандмауэр) - это специальный тип программ, который устанавливается на ваш ПК и служит межсетевым фильтром между компьютером и сетью Интернет.

Зачастую, действие фаервола незаметно, но для безопасности вашего компьютера эта программа крайне необходима. Она препятствует проникновению из интернета всяких вредоносных программ, а также предупреждает вас о выходе какой-либо программы в сеть без Вашего ведома. Брандмауэр Главное отличие от антивирусных программ то, что он не сканирует систему на наличие вирусов и не лечит их, а препятствует их попаданию на Ваш компьютер.

Outpost Network Security,
NOD32 Smart Security,
Norton Internet Security,
Comodo Internet Security,
Windows Brandmauer.

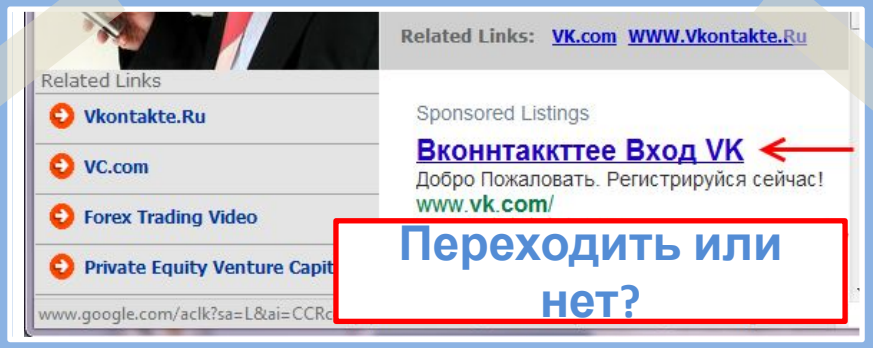
Безопасность аккаунтов

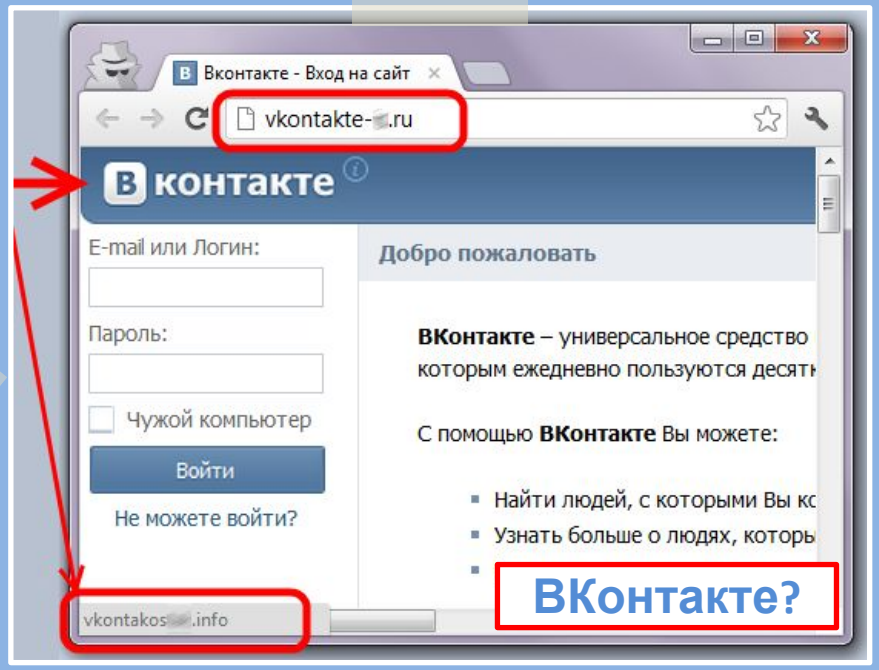


Осторожно, подделка!

Чем опасны сайты-подделки?

- крадут пароли
- распространяют вредоносное ПО
- навязывают платные услуги



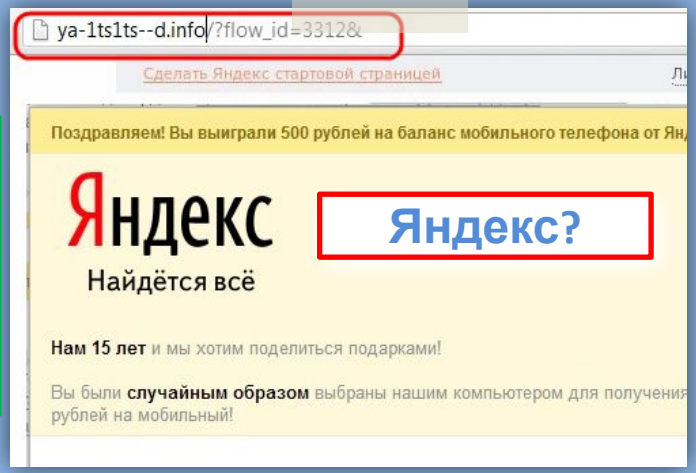


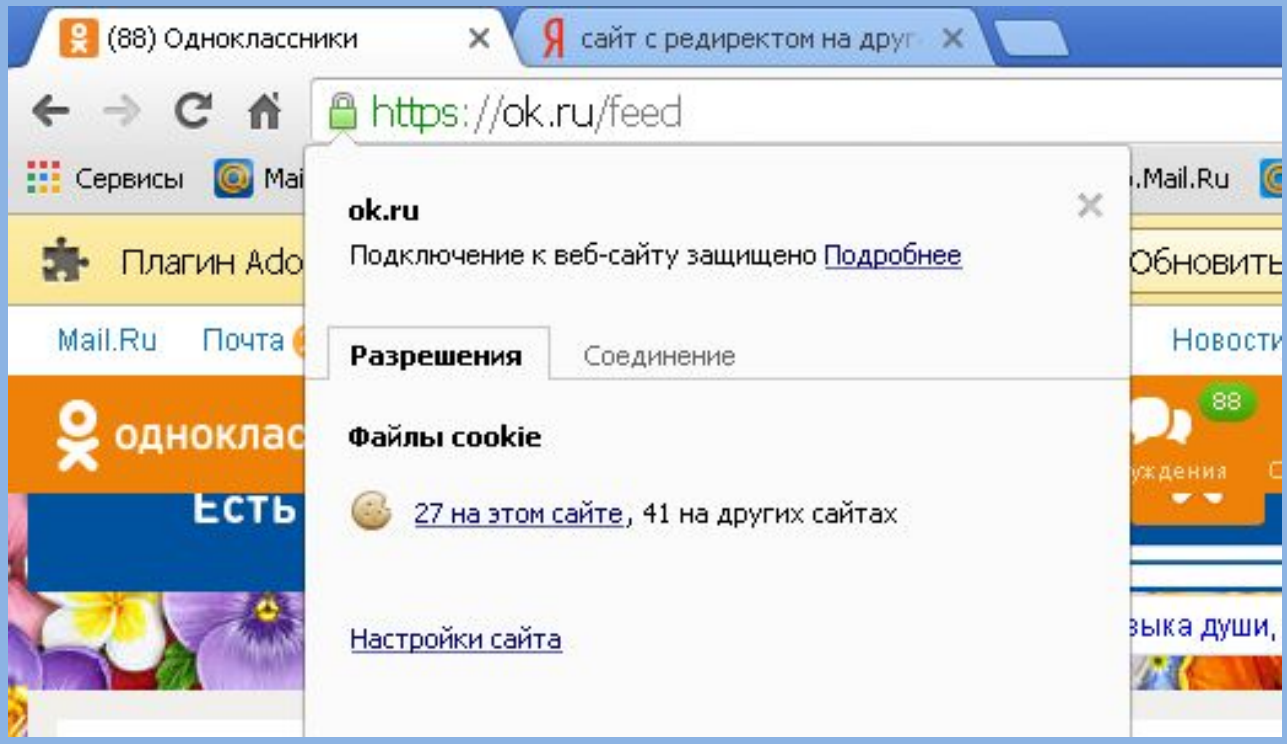
Как не стать жертвой мошенников?
Как определить подделку?
Как обезопаситься?

Используй функционал браузера: «избранное», «закладки»!

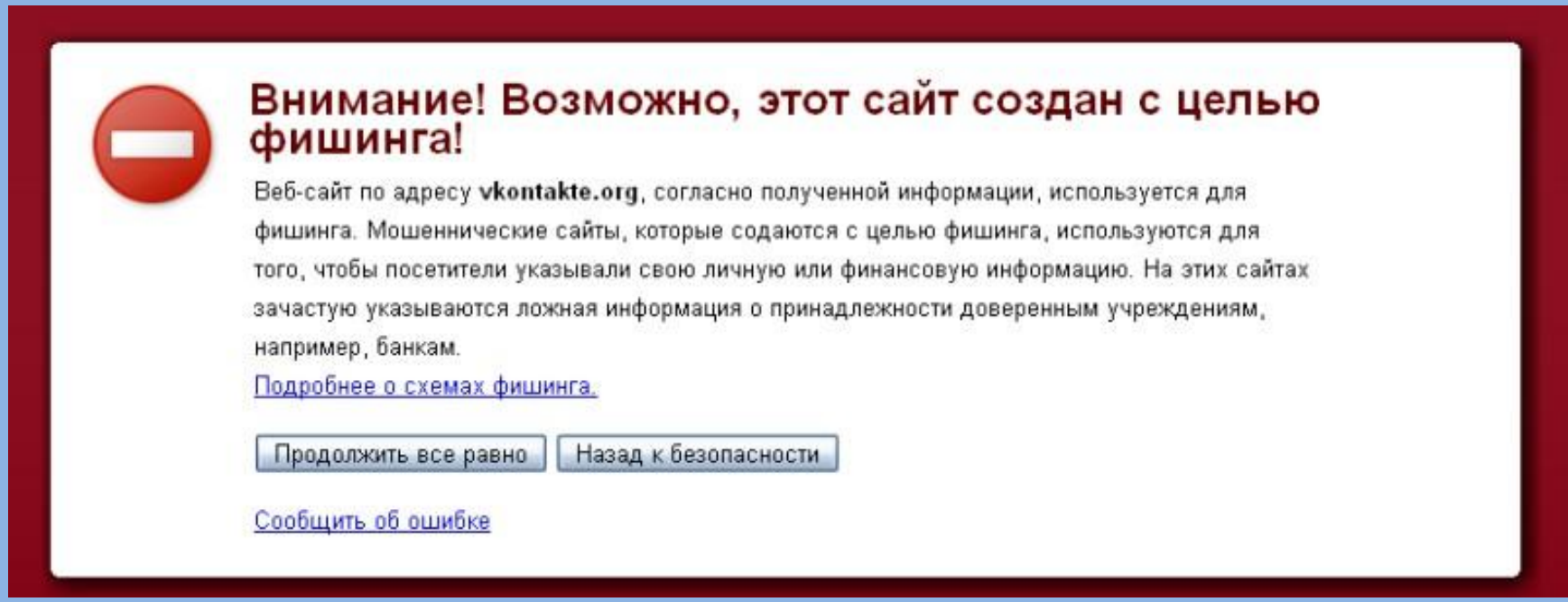
Проверяй адрес сайта!

Обрати внимание на настоящий адрес сайта! При наведении мыши реальный адрес отображается во всплывающей подсказке.




(88) Одноклассники
сайт с редиректом на друг
https://ok.ru/feed
Сервисы
Mail.Ru
Плагин Ado
Обновить
Mail.Ru
Почта
Новости
88
ok.ru
Подключение к веб-сайту защищено Подробнее
Разрешения
Соединение
Файлы cookie
27 на этом сайте, 41 на других сайтах
Настройки сайта

Сайты - подделки



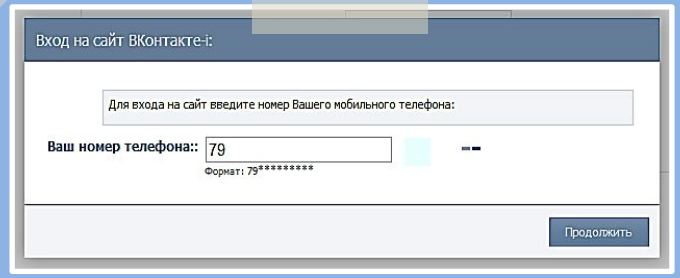
Осторожно, подделка!

Как обманывают в Интернете?

- **Просят подтвердить логин/пароль.**
- **Предлагают бесплатный антивирус. а устанавливают вредоносное ПО, вирусы.**
- **Просят отправить СМС (платное).**

Где правда? Как распознать обман?

Ваш аккаунт заблокирован за рассылку спам-сообщений, на основании многочисленных жалоб от пользователей. Для восстановления анкеты вам необходимо пройти процедуру активации. Активация производится в автоматическом режиме и является абсолютно **бесплатной**. Отправьте смс сообщение с текстом **151178** на номер **8353**. В ответном смс сообщение Вы получите код активации, который необходимо ввести ниже. Если в течение месяца ваш аккаунт не будет активирован, мы оставляем за собой право удалить его.



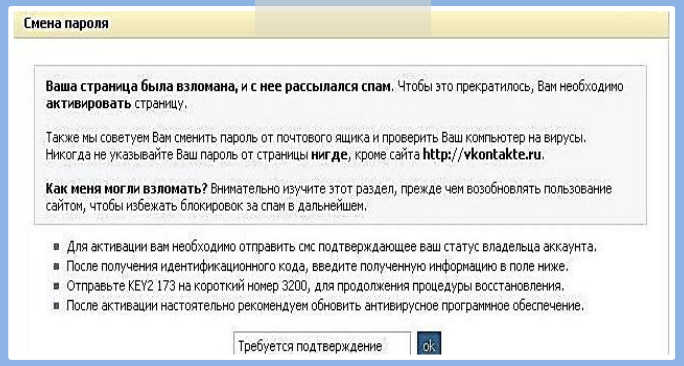
Сомневаешься?

Закрой страницу, блокировка пропала? Все в порядке!

Проверь систему антивирусом!

Авторизуйся под своими аккаунтами и убедись, что все в порядке!

Смени пароли к аккаунтам, которые используешь!



Осторожно, спам!

Первоначально слово «SPAM» появилось в 1936 г. Оно расшифровывалось как SPiced hAM (острая ветчина) и было товарным знаком для мясных консервов.

Спам – это массовая рассылка незапрашиваемых получателем электронных сообщений коммерческого и некоммерческого содержания.

ПОМНИ: идя на поводу у СПАМа есть риск:

- Отправить платное СМС, оплатить навязанную услугу.
- Получить платную подписку на ненужную информацию.
- Потерять учётные и (или) иные данные.
- Стать жертвой обмана.

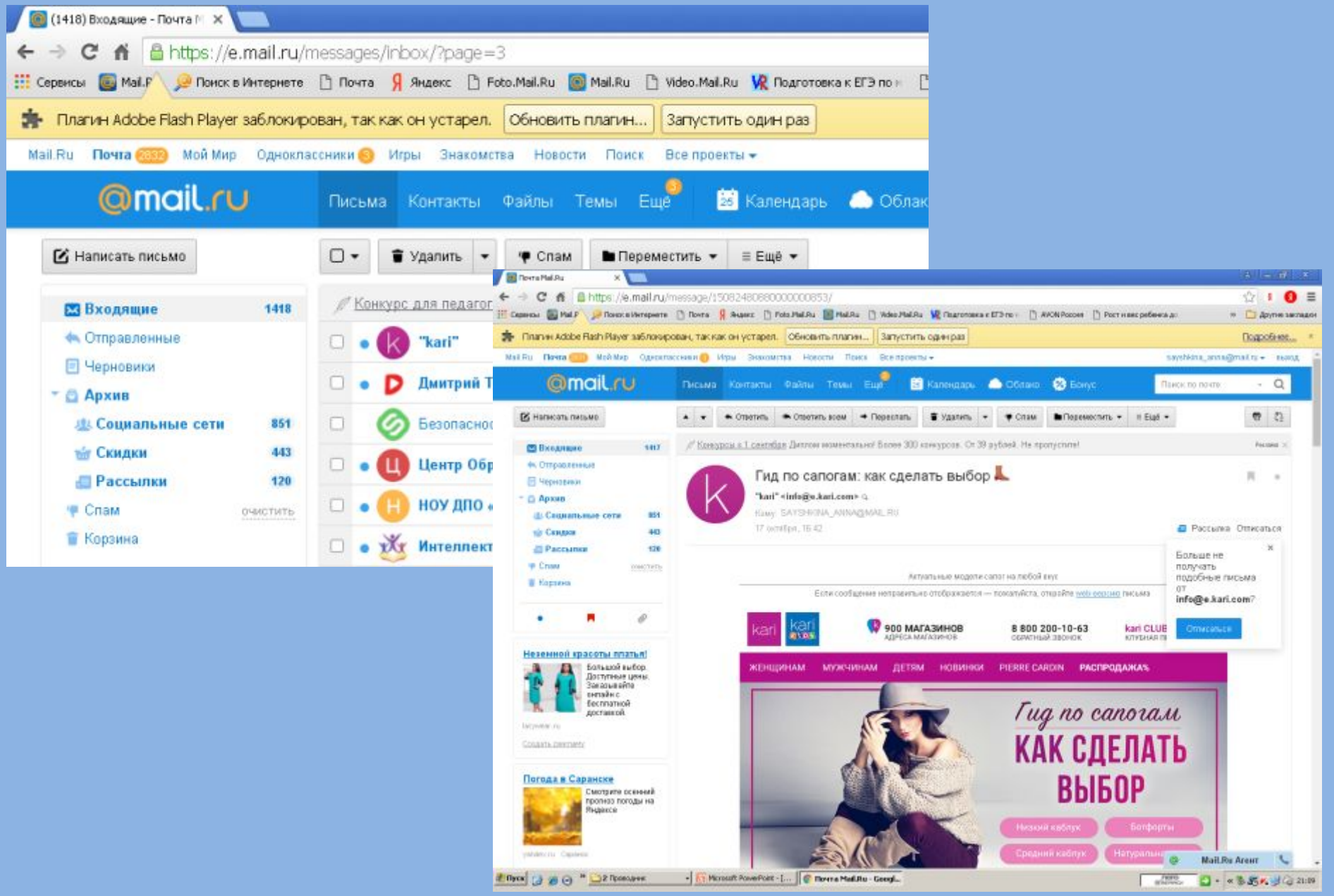
Будь внимателен!

Настрой безопасность браузера и почтовой программы (подключи антифишинг, защиту от спама и др. встроенные средства защиты)!

Используй дополнительные расширения браузеров, например AddBlock (позволяет блокировать СПАМ и рекламные блоки), WOT (показывает рейтинг сайта среди интернет-пользователей)!

Используй Антивирус и файерволл!

Проверяй надёжность поставщика услуг, используй информационные сервисы «who is»!


(1418) Входящие - Почта
https://e.mail.ru/messages/inbox/?page=3
Плагин Adobe Flash Player заблокирован, так как он устарел.
Обновить плагин...
Запустить один раз
Mail.Ru
Почта
Мой Мир
Одноклассники
Игры
Знакомства
Новости
Поиск
Все проекты
@mail.ru
Письма
Контакты
Файлы
Темы
Ещё
Календарь
Написать письмо
Удалить
Спам
Переместить
Ещё
Входящие 1418
Отправленные
Черновики
Архив
Социальные сети 851
Скидки 443
Рассылки 120
Спам
Корзина
"kari"
Гид по сапогам: как сделать выбор
900 МАГАЗИНОВ
8 800 200-10-63
ЖЕНЩИНАМ
МУЖЧИНАМ
ДЕТЯМ
НОВИНКИ
PIERRE CARDIN
РАСПРОДАЖА%
Гид по сапогам
КАК СДЕЛАТЬ ВЫБОР
Погода в Саранске

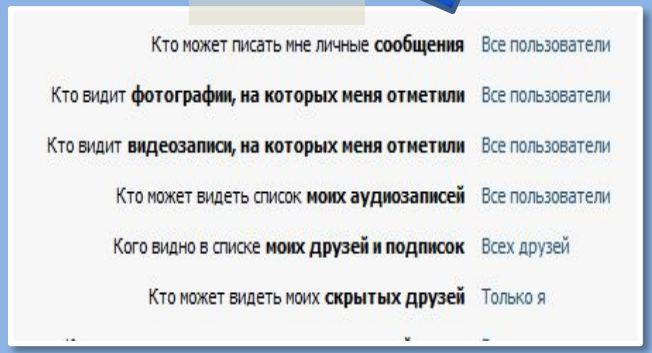
Персональные данные и личная информация в Интернете

Персональные данные – твоя частная собственность, прежде чем публиковать их и (или) передавать третьим лицам, подумай, стоит ли?

Персональные данные охраняет Федеральный Закон № 152 – ФЗ «О персональных данных»

Кому и зачем нужна твоя персональная информация?

- 80% преступников берут информацию в соц. сетях.
- Личная информация используется для кражи паролей.
- Личная информация используется для совершения таких преступлений как: шантаж, вымогательство, оскорбление, клевета, киднеппинг , хищение!



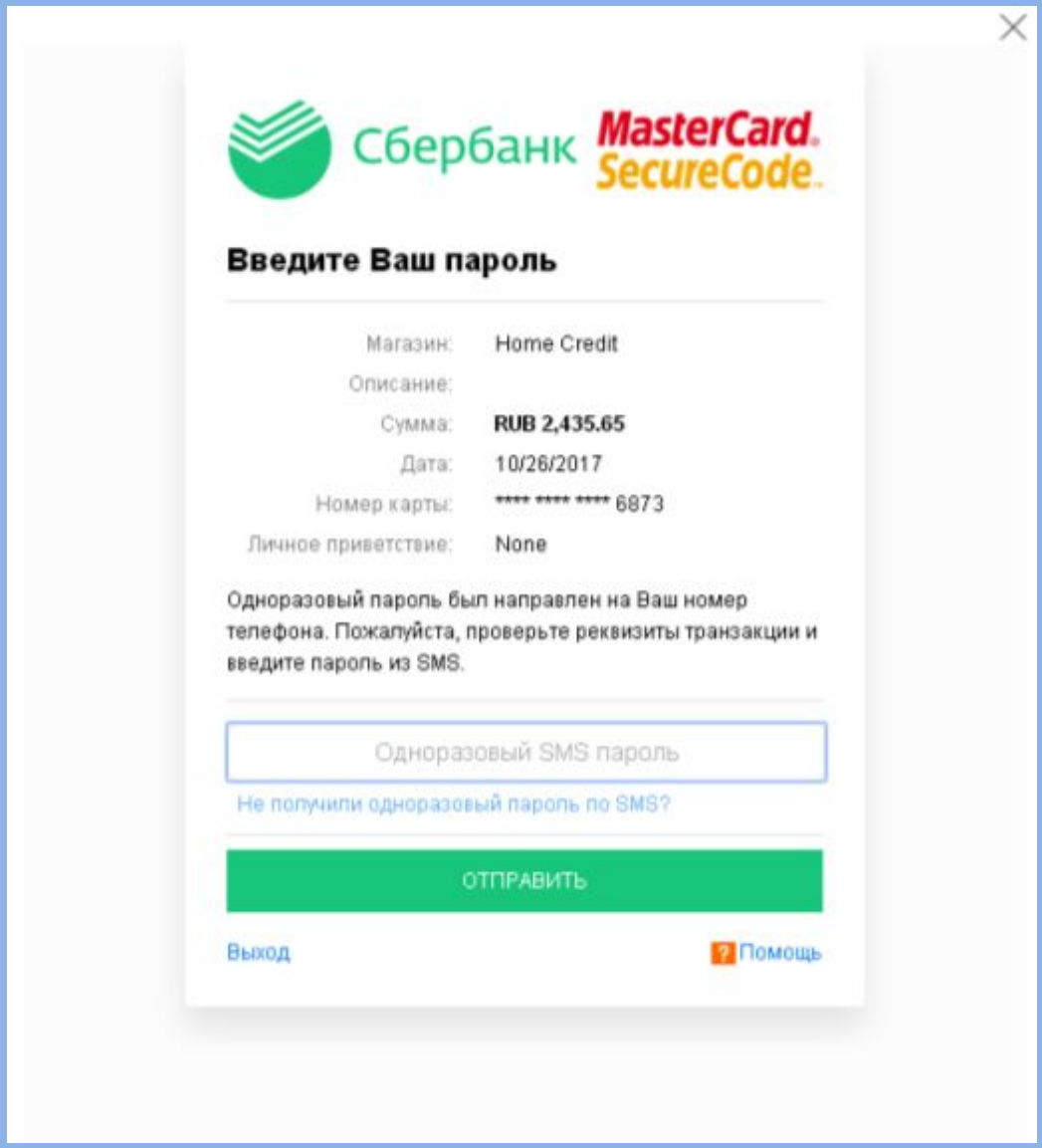
При регистрации в социальных сетях следует использовать только Имя или Псевдоним (ник)!

Настрой приватность в соц. сетях и других сервисах

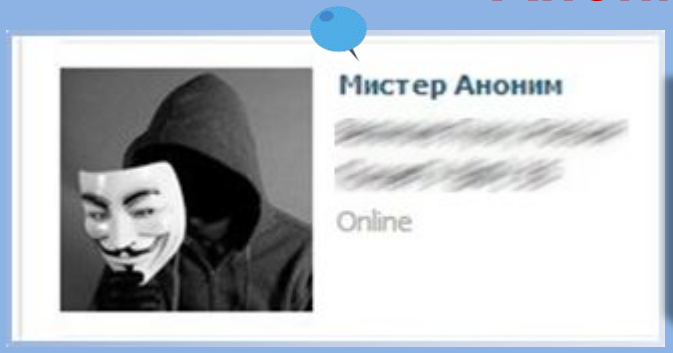
Не публикуй информацию о своём местонахождении и (или) материальных ценностях!

Хорошо подумай, какую информацию можно публиковать в Интернете!

Не доверяй свои секреты незнакомцам из Интернета!


Сбербанк
MasterCard SecureCode
Введите Ваш пароль
Магазин: Home Credit
Описание:
Сумма: RUB 2,435.65
Дата: 10/26/2017
Номер карты: **** **** **** 6873
Личное приветствие: None
Одноразовый пароль был направлен на Ваш номер телефона. Пожалуйста, проверьте реквизиты транзакции и введите пароль из SMS.
Одноразовый SMS пароль
Не получили одноразовый пароль по SMS?
ОТПРАВИТЬ
Выход
Помощь

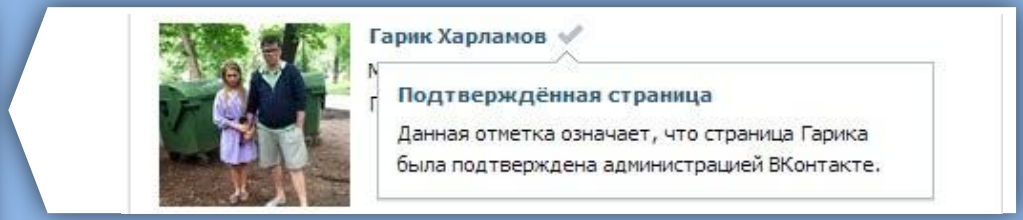
Анонимность в сети



ЗАПОМНИ!
АНОНИМНОСТЬ В ИНТЕРНЕТЕ - ЭТО МИФ!
Следы пребывания в Интернете хранятся долго,
даже прокси и анонимайзеры не помогут скрыться!

Веди себя в интернете вежливо, как в реальной жизни

Задумайся, с кем ты общаешься в интернете, кто скрывается под ником?



Официальные аккаунты знаменитостей всегда проходят процедуру верификации

ВНИМАНИЕ: Будь осторожен при общении с незнакомцами в сети!

Ими могут оказаться:

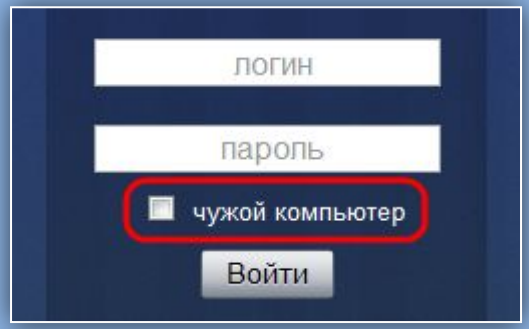
- Маньяки, педофилы, извращенцы. Завлекают в свои сети, склоняют к совершению развратных действий! Такое общение может быть опасным для жизни!
- Интернет-ХАМЫ (Тролли) провоцируют на необдуманные поступки и необоснованную агрессию!
- Киберпреступники зачастую обманом похищают чужое имущество!
- Хакеры используют анонимность для распространения вредоносного программного обеспечения, завладения учётными данными, платёжными реквизитами, персональной информацией!

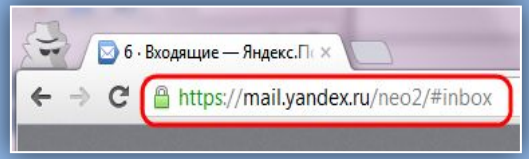
Открытые сети, чужая техника

Небрежное отношение к личной информации может привести к её утере!

ПОМНИ:

1. Будь осторожен в открытых и небезопасных сетях. Подключение к ложной сети может моментально лишить тебя всей персональной информации, хранящейся в твоем электронном устройстве: преступнику станут доступны пароли, и другая информация.
2. Опасно оставлять свои учётные данные на устройстве, которое тебе не принадлежит, этими данными могут воспользоваться в преступных целях.





Несколько простых правил, которые следует соблюдать при работе в открытых сетях или с использованием «чужой» техники:

1. *При работе с публичным устройством используй пункт «чужой компьютер».*
2. *Используй режим «приватного просмотра» в браузере.*
3. *Всегда используй кнопку «выйти» при завершении работы с ресурсом.*
4. *Отказывайся от сохранения пароля при работе на «чужом компьютере».*

1. *Используй безопасное соединение с почтой и сервисами (безопасное соединение обозначено замком с зелёным текстом).*
2. *Не оставляй без присмотра устройства доступа в сеть (телефон, планшет, ноутбук).*

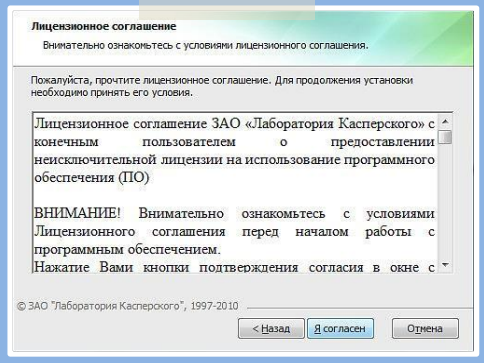
1. *Используй шифрованные хранилища данных, которые помогут защитить твои личные файлы.*
2. *Используй сложные пароли, состоящие из прописных и заглавных латинских букв и цифр, а также символов.*
3. *Используй только открытые сети в надежности которых ты уверен.*

Условия использования программного продукта

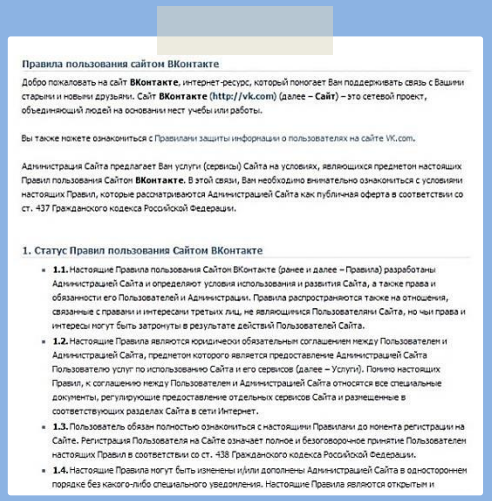
Любая услуга в Интернете имеет лицензионное соглашения и (или) условия использования. При установке программных продуктов (особенно от неизвестных производителей) следует внимательно читать тексты соглашений, ведь после принятия соглашения вся ответственность и последствия использования программного продукта ложатся на тебя!

Подтверждая соглашение «вслепую» ты можешь:

1. Оформить платные подписки/услуги;
2. Предоставить приложению/программе обширные права;
3. Лишиться персональных данных, хранящихся на электронном устройстве;
4. Стать звеном ботнета и (или) СПАМ сети;
5. Стать жертвой мошенников.



ПОМНИ: любые соглашения об использовании программных продуктов и услуг, даже от проверенного производителя, требуют внимательного изучения!



Чтобы не стать жертвой злоумышленников :

Использовать лицензионные продукты проверенного производителя;

Внимательно знакомиться с лицензионным соглашением;

Не использовать подозрительное ПО.

МОБИЛЬНЫЙ ИНТЕРНЕТ

В мобильном телефоне много важной информации!

- Список контактов;
- Личные фотографии/видеозаписи;
- Данные доступа к электронной почте и иным аккаунтам в сети;
- Данные о банковских картах и платежах;
- Привязка к балансу сим-карты.

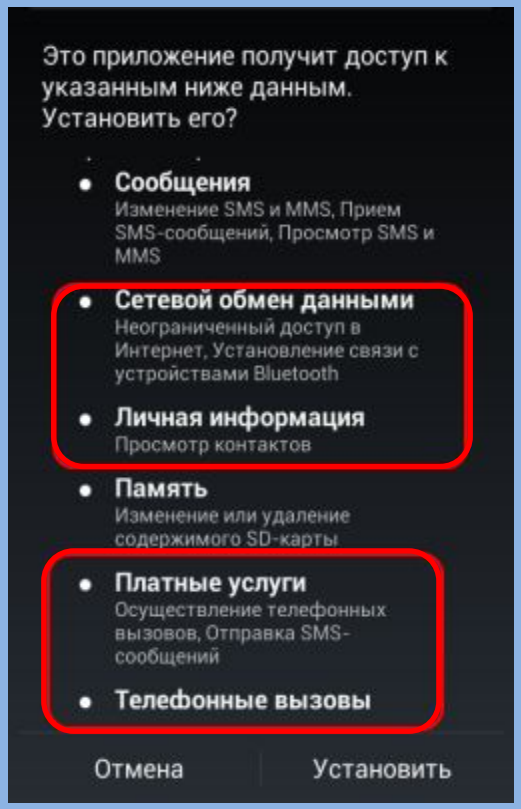
Следи за своим мобильным телефоном или планшетом!

Установи пароль на включение мобильного телефона!

Установи мобильный антивирус!

Игнорируй звонки и СМС с незнакомых номеров!

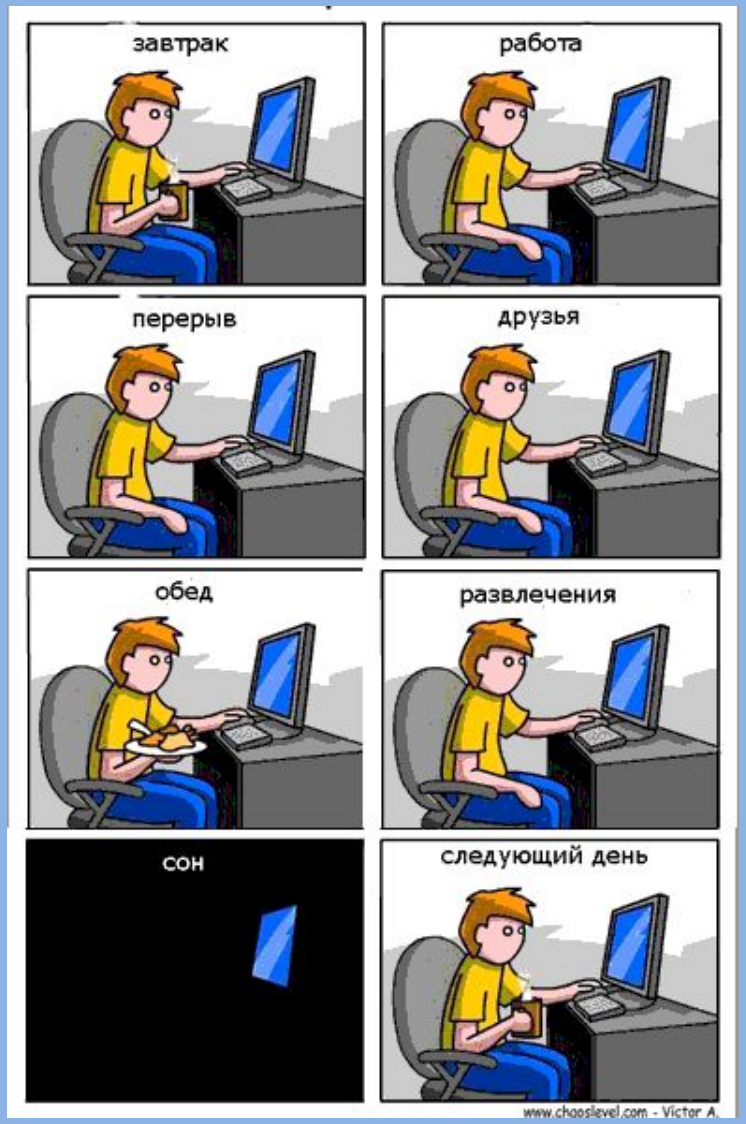
Проверяй, какие права просит мобильное приложение!



ИНТЕРНЕТ–ЗАВИСИМОСТЬ

Признаки :

- сидишь за компьютером больше 1 часа в день;
- не хочешь отрываться от компьютера;
- включаешь компьютер раньше, чем умоешься;
- лучше поиграешь, чем поешь;
- плохо спишь и не высыпаешься;
- удобней общаться в сети, чем в жизни;
- ругаешься с родителями, когда нужно выключить компьютер и помочь по дому, сделать уроки;
- готов солгать, чтобы посидеть за компьютером подольше;
- готов тратить деньги на бонусы в играх.

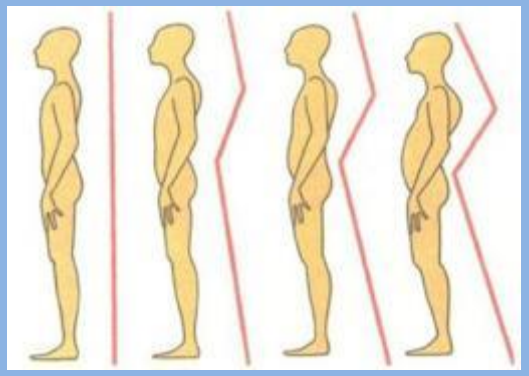


Ограничь пользование интернетом, живи реальной жизнью!

ИНТЕРНЕТ-ЗАВИСИМОСТЬ И ЗДОРОВЬЕ

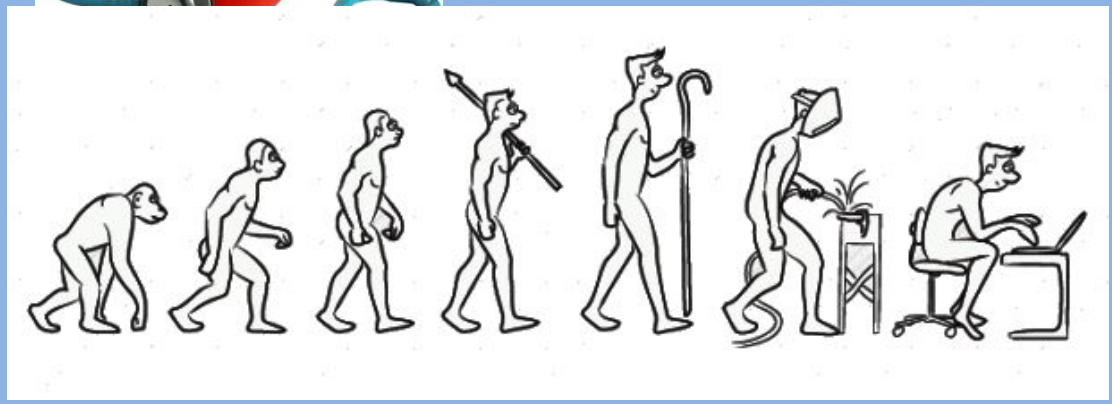
в России до 80% школьников в возрасте 12—13 лет страдают компьютерной зависимостью.

В России полностью здоровы только 14-23% школьников



Каждый третий выпускник имеет близорукость, нарушение осанки

Каждый четвертый выпускник имеет патологию сердечно-сосудистой системы.



75% школьников находятся в условиях гиподинамии

Ограничь пользование интернетом, живи реальной жизнью!


БЕГИ ИЛИ УМРИ


КАК СТАТЬ ФЕЕЙ ОГНЯ ИЗ ВИНКС
ДОМАШНИХ УСЛОВИЯХ?
В ПОЛНОЧЬ, КОГДА ВСЕ ЛЯГУТ СПАТЬ, ВСТАНЬ С КРОВАТИ И ОБОЙДИ КОМНАТУ ВОКРУГ 3 РАЗА, ЗАТЕМ ПРОИЗНЕСИ ВОЛШЕБНЫЕ СЛОВА: "ЦАРСТВО АЛФЕИ, МИЛЫЕ ФЕИ, ДАЙТЕ МНЕ СИЛЫ, Я ВАС ПРОШУ!" ПОСЛЕ ЭТОГО, ТИХО ИДИ НА КУХНЮ, СТАРАЙСЯ, ЧТОБЫ ТЕБЯ НЕ УВИДЕЛИ, ИНАЧЕ МАГИЯ СЛОВ ПРОПАДЁТ!
ВКЛЮЧИ ГАЗОВУЮ ПЛИТУ, ВСЕ 4 КАМФОРКИ НО НЕ ЗАЖИГАЙ ЕЁ! ТЫ ЖЕ НЕ ХОЧЕШЬ ОБЖЕЧЬСЯ?
ЗАТЕМ ТАКЖЕ ТИХО ИДИ СПАТЬ. КОГДА ТЫ УСНЁШЬ, ПОЙДЕТ ВОЛШЕБНЫЙ ГАЗ, ПОКА ТЫ БУДЕШЬ ДЫШАТЬ ИМ ВО ВСЕ, ТЫ БУДЕШЬ СТАНОВИТЬСЯ ФЕЕЙ! А КАК ПРОСНЕШЬСЯ, СКАЖИ: "СПАСИБО АЛФЕЯ, Я СТАЛА ФЕЕЙ!" И ТЫ СТАНЕШЬ НАСТОЯЩЕЙ ФЕЕЙ ОГНЯ!

Вопросы для обсуждения

- Чем опасны сайты подделки?
- Как распознать подделку?

- Что такое Спам? Как бороться со Спамом?
- Какие существуют методы блокировки Спам рекламы?

- Что относится к персональным данным, а что к личной (конфиденциальной) информации?
- Какую информацию можно публиковать в сети?
- Почему не стоит публиковать свои полные данные?

- Анонимность в сети: правда или вымысел?
- Какие правила поведения в сети нужно соблюдать?

- Какие опасности подстерегают нас в открытых сетях?
- Как не стать жертвой преступника при использовании открытых сетей?
- Какие правила пользования чужой техникой нужно помнить?

- Лицензионное соглашение/правила пользования: читать или нет?
- Почему важно знать правила использования программного продукта/интернет-ресурса?

- Виды Интернет-мошенничества (объекты мошенничества)?
- Какие виды преступлений распространены в Интернете?
- Как не стать жертвой киберпреступника?