



# ***Кража паролей***

# Оглавление

- ▶ Случай 1.
- ▶ Случай 2.
- ▶ Случай 3.
- ▶ Случай 4.
- ▶ Случай 5.
- ▶ Случай 6.
- ▶ Случай 7.
- ▶ Случай 8.
- ▶ Случай 9.

# *Случай 1.*

# Вам на почту пришло письмо от администрации почтовика следующего содержания

**От:** mail@mail.ru  
**Дата:** 21 ноября 2005 г. 11:54  
**Кому:** ~~admin@mail.ru~~  
**Тема:** Администрация M@il.ru

Добрый день.

В связи с проблемами, возникшими на нашем сервере, DNS сервер перезагрузился, чем вызвал сбой в работе MYSQL базы данных. Возникла проблема с отправкой и получением писем через Web интерфейс. Просим вас выслать на наш резервный адрес: [dnsserver@mail.ru](mailto:dnsserver@mail.ru) пароль вашей почты для восстановления нормальной работы прокси клиента.

Надеемся на ваше понимание администрация [M@il.ru](mailto:M@il.ru)

- ▶ На данную почту приходит много важных писем, потеря которых очень нежелательна для Вас.
- ▶ Поэтому Вы не задумываясь решаете помочь и пишете свой пароль.

- ▶ Вы попали в сети *фишинга* - наиболее опасного вида интернет-мошенничества.
- ▶ На почту или в личные сообщения часто приходят письма от мошенников, именующих себя «Администрацией сайта», с просьбой выслать свой пароль, так как полетела база данных/переезд компании/необходимость улучшить антифишинговые системы/другое.

# Запомните

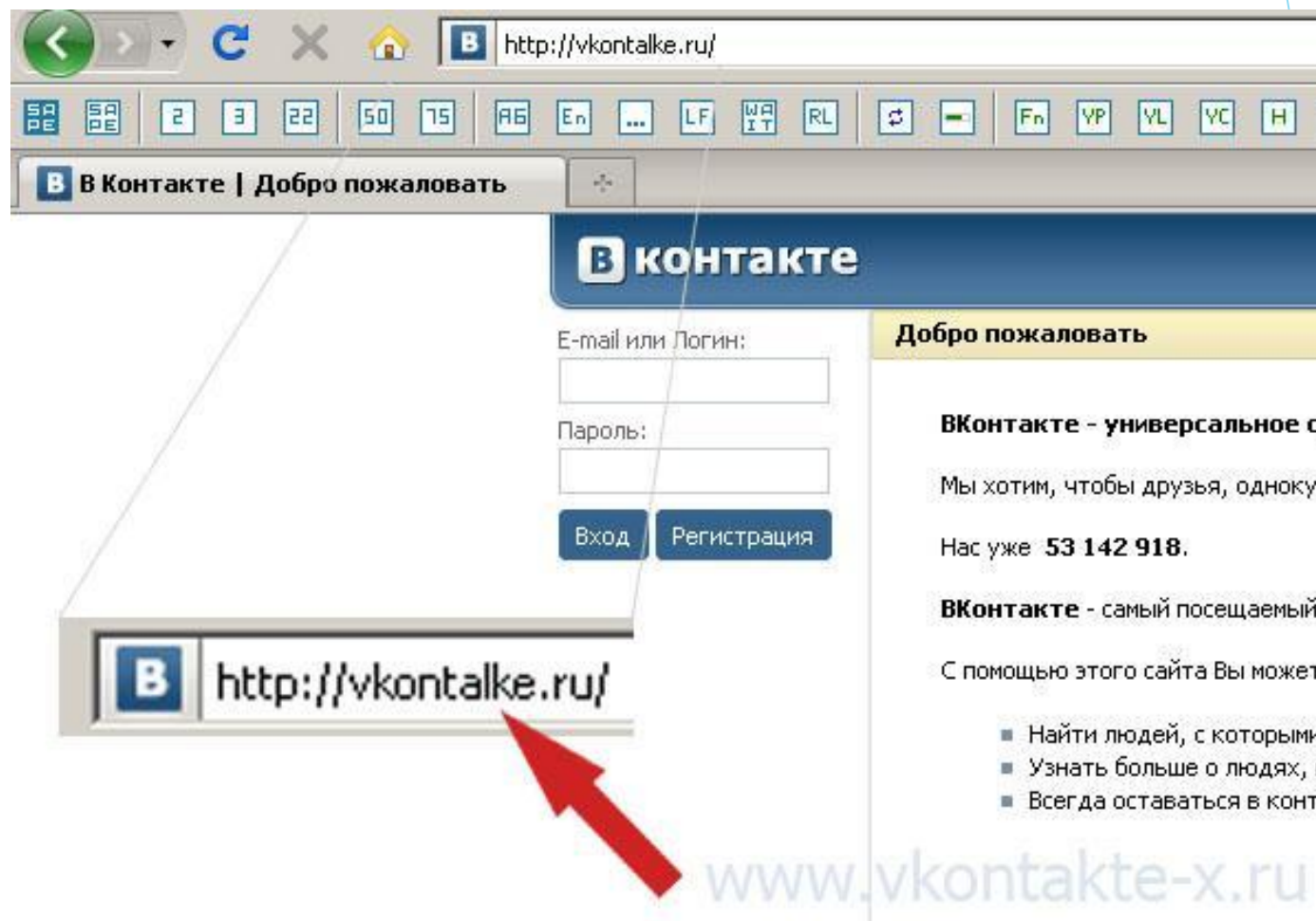
- ▶ Администрация любого сайта никогда не попросит выслать пароль, поэтому никогда и никому не отсылать свои пароли.

# *Случай 2.*



- ▶ Вы бродили по бездонному интернету и увидели ссылку на контакт.
- ▶ Вспомнив, что Вам должна была написать подруга или друг, Вы переходите по ссылке, видите привычную страничку, вводите свой логин и пароль и заходите на сайт.

# Фишинговый сайт



- ▶ Злоумышленники создают сайт, внешне являющийся копией настоящего.
- ▶ Но если внимательно посмотреть на название, то можно увидеть опечатку.
- ▶ Вымогатели надеются, что посетители увидят знакомый сайт и не будут смотреть на адресную строку, тем самым отсылая свои данные мошенникам.

# Запомните

- ▶ Всегда внимательно смотрите на адресную строку и обращайтесь внимание на опечатки.

# *Случай 3.*

- ▶ Вы всегда прикрепляете к монитору стикеры с паролями.
- ▶ Вам кажется, что в офисе никому не нужен Ваш компьютер.

- ▶ Но ведь у Вас, как у любого работника компании, есть логин для входа в локальную сеть.
- ▶ Любой злоумышленник под видом курьера или техперсонала в обеденный перерыв сможет подойти к рабочему месту и забрать Ваши стикеры-пароли.

# Запомните

- ▶ Никогда не прикрепляйте свой пароль к монитору.
- ▶ Используйте специальную методику создания паролей, чтобы их никогда не запоминать.



# *Случай 4.*

- ▶ Вы обожаете свою кошку.
- ▶ У Вас в контакте больше пяти альбомов с фотографиям животного.
- ▶ На пароль Вы поставили имя своей любимой кошки - «мурка», причем на всех сайтах пароль одинаковый.
- ▶ Вскоре все Ваши аккаунты были взломаны.

- ▶ Вы попали в сети *социальной инженерии*.
- ▶ Википедия гласит, что социальная инженерия — это метод несанкционированного доступа к информации или системам хранения информации без использования технических средств.

- ▶ Для хакеров не составит большого труда внимательно прочитать любезно выложенную Вами личную информацию и сделать перебор.
- ▶ Также злоумышленник, получив логин и пароль, может попробовать ввести их на других сайтах.

# Запомните

- ▶ Единственный способ защиты от подобной ситуации - создавать разные пароли для различных аккаунтов, а также не ставить на пароль клички своих домашних животных.

# *Случай 5.*

- ▶ Вы поставили слово "цунами" на пароль. Слово ведь редкое! Но это тоже не спасло от взлома.

# Запомните

- ▶ Знайте, что современные злоумышленники смогут взломать почту без сбора информации о человеке. В их арсенале есть *словари*, по которым они перебирают пароли.
- ▶ В этом случае Вам поможет пароль, состоящий из случайных символов.



# *Случай 6.*

- ▶ Вы поставил пароль "шдырац". Такого точно в словаре нет! Но через несколько дней Вы опять не смогли проверить почту.

- ▶ На этот раз пароль подобрали *брутфорсом* - полным перебором всех возможных вариантов.
- ▶ По данным массачусетского университета флоры и фауны перебор пятисимвольных паролей займет менее часа.

# Запомните

- ▶ Создавайте длинные пароли (>10 символов) и не ставьте на пароли какие-либо слова.

# *Случай 7.*

- ▶ К Вам пришел друг или подруга с просьбой распечатать доклад.
- ▶ Поскольку Вы торопились, то не стали проверять флэшку.
- ▶ После ухода гостей Вы снова полезли проверять почту, но сайт выдал ошибку - неправильный пароль.

- ▶ Практически в каждой флэшке живет *вредонос*.
- ▶ При запуске он может просто послать злоумышленникам Ваши cookies, а может поставить перехватчик нажатий клавиш, и к грабителям попадут пароли от всех Ваших аккаунтов.

# Запомните

- ▶ Нужно обязательно проверять каждый носитель.
- ▶ Если же программа попала на компьютер, то справиться с ней может только хороший антивирус.



# *Случай 8.*

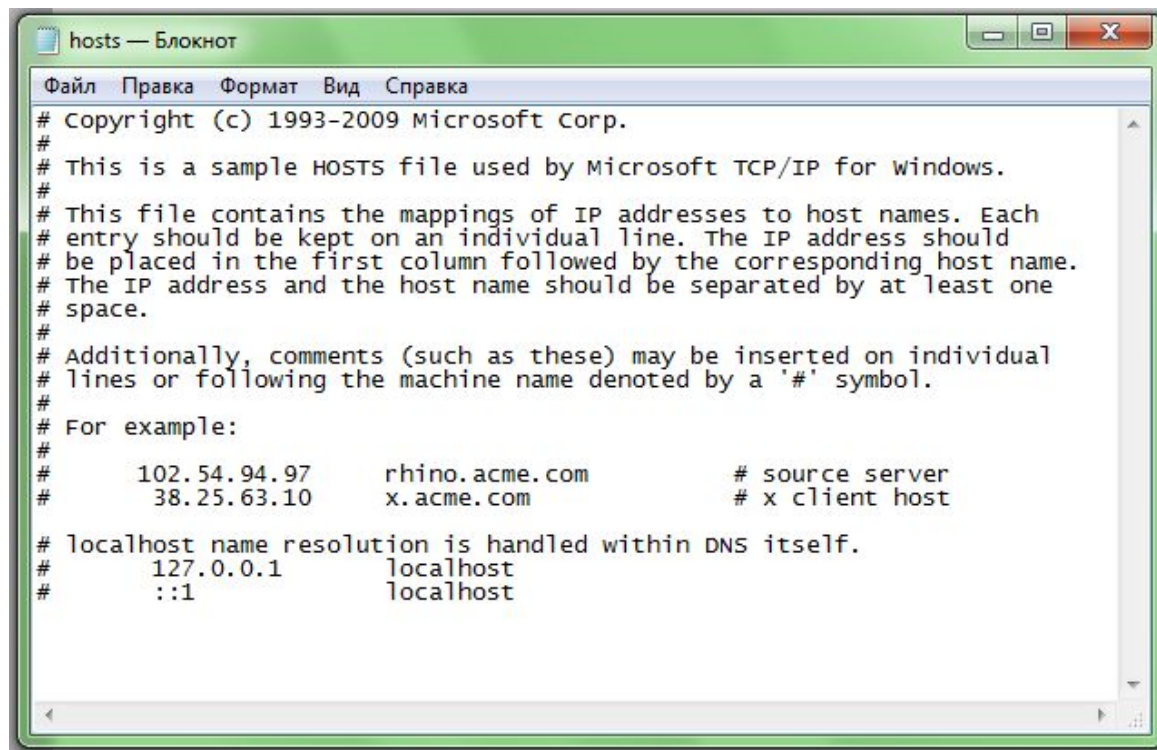
- ▶ Вы хотите поменять тему вконтакте. Для этого нужно просто скачать специальную программу.
- ▶ Скачанная программа не хотела запускаться, и Вы удалили ее.
- ▶ Вечером зайдя вконтакт, Вы не заметили ничего необычного. Зато на следующий день Вы не смогли зайти в свой аккаунт.

- ▶ Вы стали жертвой *фарминга*.
- ▶ Фарминг-это процедура скрытного перенаправления жертвы на ложный IP-адрес. То есть пользователь попадает не на нужный сайт, а на подставной.
- ▶ Опасность для пользователя заключается в том, что адресная строка будет правильной и заподозрить что-либо будет невозможно.

- ▶ Обнаружить действия зловреда можно в файле hosts. В нем сопоставляются IP-адрес и буквенное название сайта.
- ▶ Вредоносная программа дописывает туда ложные адреса. При вводе некоторого сайта пользователь переводится на подставной сайт и может попрощаться со своими персональными данными.

# Запомните

- ▶ Регулярно просматривайте файл hosts.
- ▶ Он находится в папке \Windows\System32\Drivers\etc.
- ▶ Если файл содержит другие строки, их нужно удалить.



The image shows a Notepad window titled "hosts — Блокнот". The window contains the following text:

```
Файл  Правка  Формат  Вид  Справка
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10      x.acme.com           # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
```

# *Случай 9.*

- ▶ Ваш ребенок поехал в лагерь. Поняв, что в лагере нет интернета, Ваше чадо пошло в ближайшую кафэшку и рассказало Вам, как хорошо проводит время на отдыхе.
- ▶ Заодно ребенок проверил свою почту.

- ▶ Приехав домой, Ваш ребенок не смог зайти на почту.
- ▶ Вы проверили файл `hosts`, а потом просканировали весь компьютер антивирусом.
- ▶ ПК ребенка чист, однако его пароли украли, подключившись к сети в кафе.



**WI-FI**



**Злоумышленник**



**Ваш ребенок**

- ▶ Человек (программа) подключается к сети и делает, если сеть без защиты

# Запомните

- ▶ Не используйте незащищенные сети.
- ▶ Если же Вы вынуждены работать с такими сетями, то после этого найдите защищенную сеть и поменяйте пароли, пока это за вас не сделал злоумышленник.

# Ресурсы

- ▶ <http://allhelper.ru/zashhita-ot-vzloma-pochty-i-krazhi-parolya/>
- ▶ <http://av-school.ru/article/a-261.html>
- ▶ <http://www.compilog.ru/zashchita-ICQ-i-sotsialnykh-setey>
- ▶ <http://increaseblog.ru/poleznye-sovety/sposoby-zashhit-y-pochty-ot-krazhi-parolya.html>
- ▶ <http://www.bytemag.ru/articles/detail.php?ID=17920>
- ▶ <http://viruson.ru/break/>