# Personal Security Online:
## Protecting Yourself

Ladue Chapel Presbyterian Church

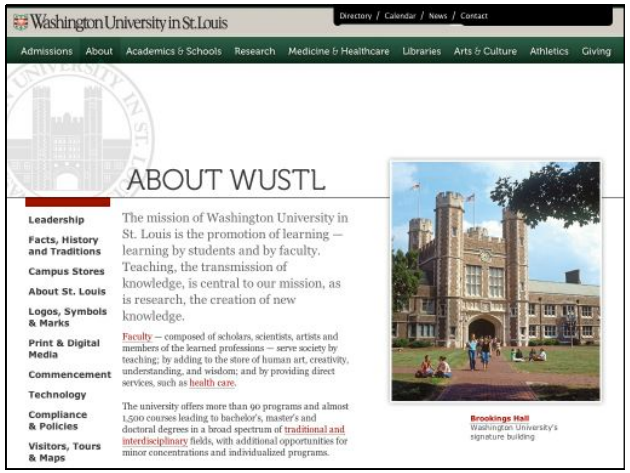
R. Scott Granneman

© 2006-2012 R. Scott Granneman
Last updated 20120505
You are free to use this work, with certain restrictions.
For full licensing information, please see the last slide/page.

1

?

2




3

Washington University in St. Louis

Technology in Our Changing Society

Technology for Managers

Web Site Management

Web Design & Advanced Web Design

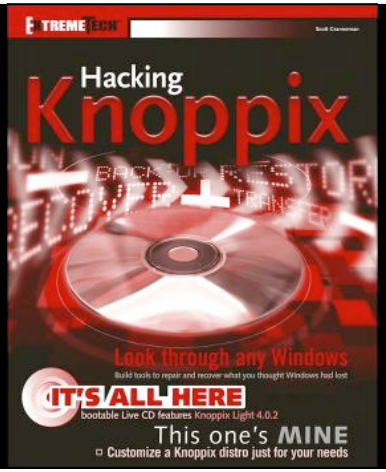
From Blogs to Wikis:
Building Community
in a Virtual Environment

Technology & the Law

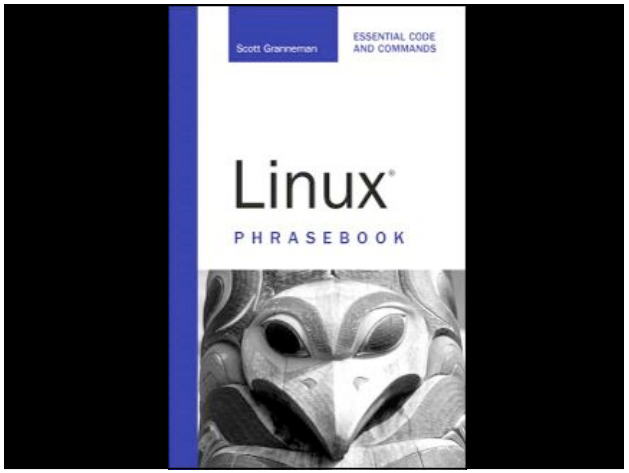
Practical Security

4

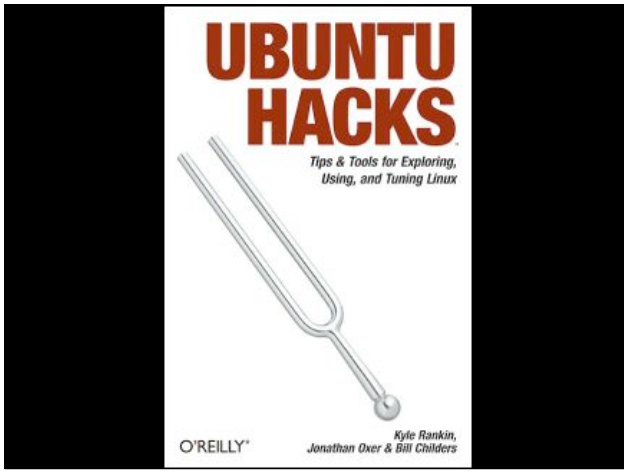
5



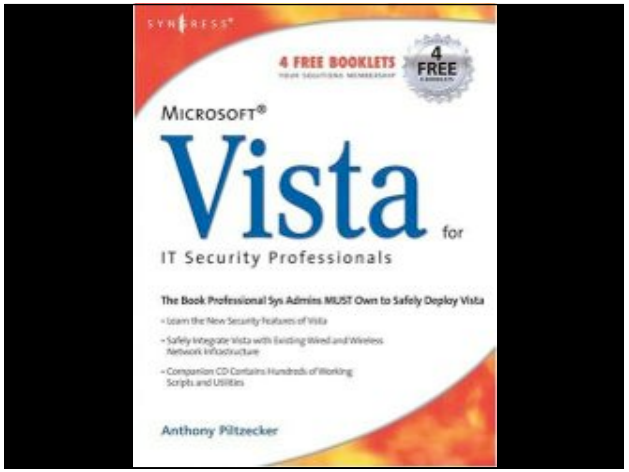

6


Scott Granneman
ESSENTIAL CODE AND COMMANDS
Linux
PHRASEBOOK

7


UBUNTU HACKS
Tips & Tools for Exploring, Using, and Tuning Linux
O'REILLY
Kyle Rankin, Jonathan Oxer & Bill Childers

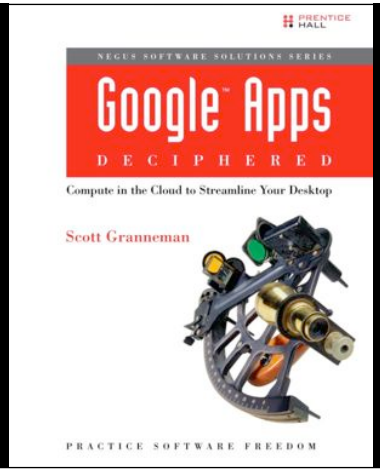
8


4 FREE BOOKLETS
4 FREE
MICROSOFT
Vista for
IT Security Professionals
The Book Professional Sys Admins MUST Own to Safely Deploy Vista
Anthony Piltzecker

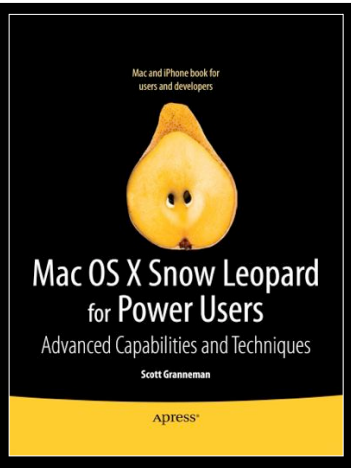
9

shortcut
Your Short Cut to Knowledge
Podcasting with Audacity
Creating a Podcast with Free Audio Software
Mac, Windows, and Linux
Dominic Mazzoni and Scott Granneman
SOURCEFORGE
Community Press
www.prenhallprofessional.com
Audacity

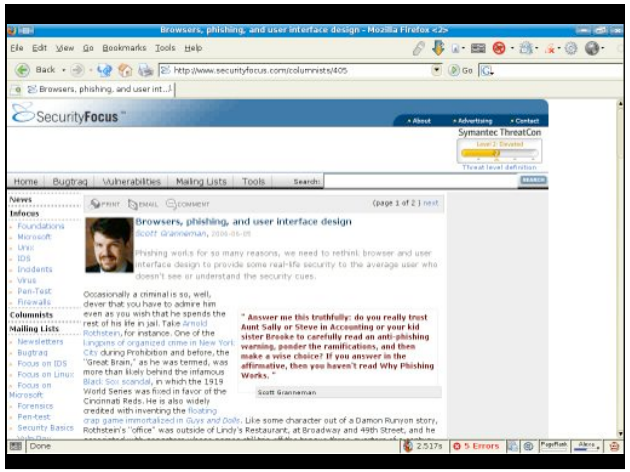
10


PRENTICE HALL
NEGUS SOFTWARE SOLUTIONS SERIES
Google Apps
DECIPHERED
Compute in the Cloud to Streamline Your Desktop
Scott Granneman
PRACTICE SOFTWARE FREEDOM

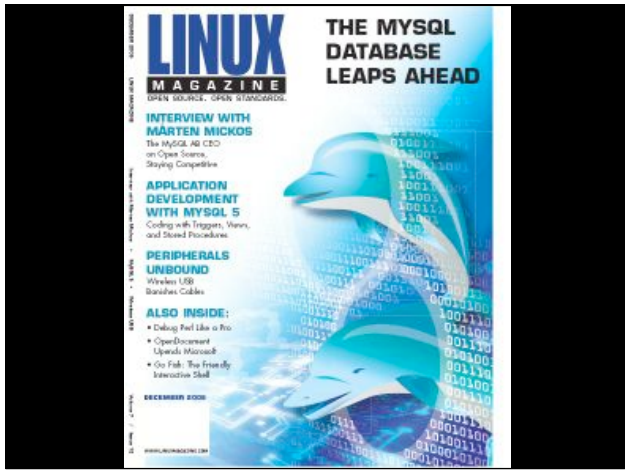
11


Mac and iPhone book for users and developers
Mac OS X Snow Leopard for Power Users
Advanced Capabilities and Techniques
Scott Granneman
Apress

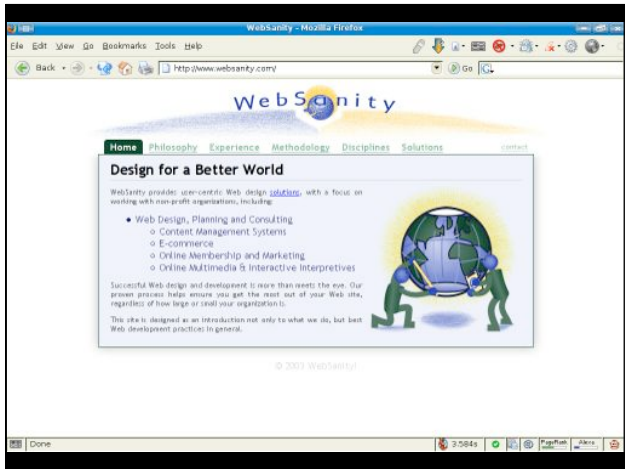
12


Browsers, phishing, and user interface design - Mozilla Firefox
SecurityFocus
Browsers, phishing, and user interface design
Scott Granneman, 2006-05-05
Phishing works for so many reasons, we need to rethink browser and user interface design to provide some real-life security to the average user who doesn't see or understand the security cues.
" Answer me this truthfully: do you really trust Aunt Sally or Steve in Accounting or your kid sister Brooke to carefully read an anti-phishing warning, ponder the ramifications, and then make a wise choice? If you answer in the affirmative, then you haven't read Why Phishing Works. "
Scott Granneman

13


LINUX
MAGAZINE
OPEN SOURCE. OPEN STANDARDS.
THE MYSQL DATABASE LEAPS AHEAD
INTERVIEW WITH MÅRTEN MIKOS
APPLICATION DEVELOPMENT WITH MYSQL 5
PERIPHERALS UNBOUND
ALSO INSIDE:
DECEMBER 2006

14


WebSanity - Mozilla Firefox
WebSanity
Home
Philosophy
Experience
Methodology
Disciplines
Solutions
Design for a Better World
Web Design, Planning and Consulting
Content Management Systems
E-commerce
Online Membership and Marketing
Online Multimedia & Interactive Interpretives

15

16

# 4 Talks

17

Personal Security on the Internet

The Future of Journalism
& the Media

*With Denise Lieberman:*

Voting: Technical & Legal Issues

Technology & the Limits
of Censorship & Free Speech

18

Once a technology
makes something possible,
it gets applied,
whether for good or bad.

Donald A. Norman

19

Security is a *process*,
not a product

20

# What to Believe?

21

22

23

24

25

Yesterday a lot of you
alerted me to a picture
of a Taliban propaganda poster
with Bert!
Reality is imitating the Web!
I am honestly freaked out!

"Bert Is Evil"
Webmaster

26

27

28

# Malware

29

Virus
Worm
Trojan Horse
Spyware

30

*Virus*

Self-replicating

Infects another program
& uses that to spread

Alters the way a computer operates

31

*Worm*

Self-replicating

Uses a network
to send copies of itself
to other computers

Spreads without human intervention

32

*Trojan Horse*

Malicious program
that disguises itself as
legitimate software

Looks harmless or useful,
but hides something harmful

33

*Spyware*

Gathers information
about you & your computer use

Transmits information
to an external entity
without your knowledge
or informed consent

34

# Wireless

35

36

What's a *packet sniffer*?

A program and/or device that monitors the data passing through a network

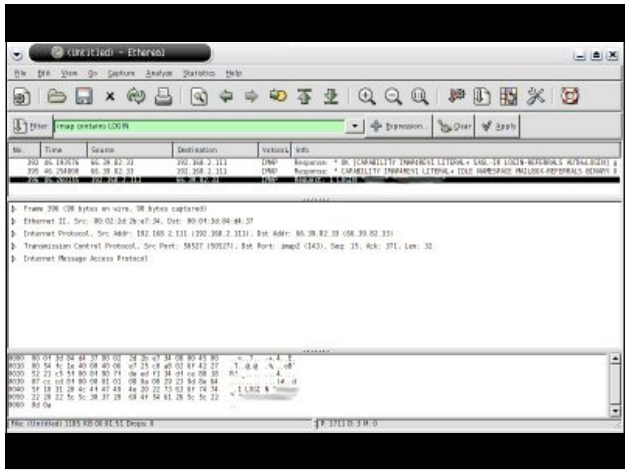
It can tell the user where data is coming from, where data is going, and what the data is

37

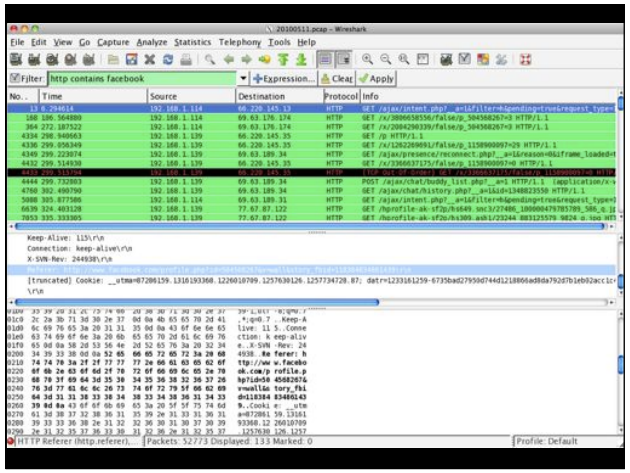
www.wireshark.org

38

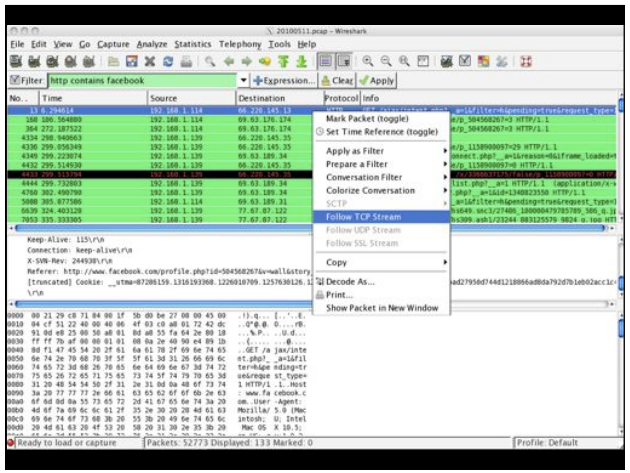
39



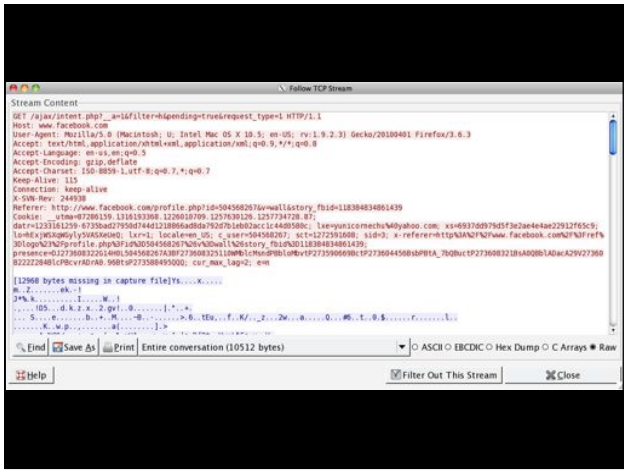
40



41

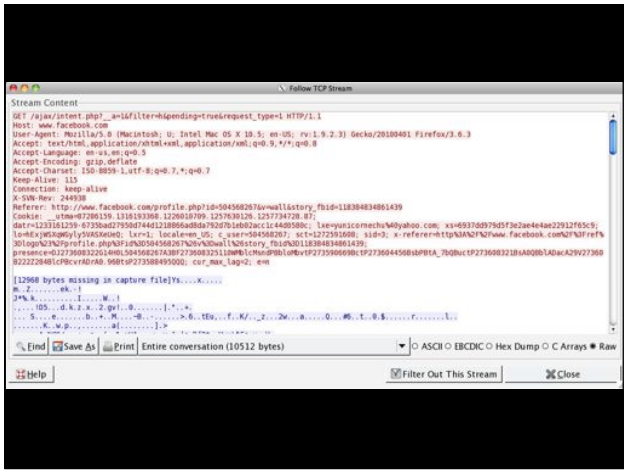


41


Follow TCP Stream
Stream Content
GET /ajax/intent.php?__a=1&filter=h&pending=true&request_type=1 HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
X-SVN-Rev: 244938
Referer: http://www.facebook.com/profile.php?id=504568267&v=wall&story_fbid=118384834861439
Cookie: __utma=87206139.1316193368.1226010709.1257630126.1257734728.87;
datr=1233161259-6735bad27950d744d1218866ad8da792d7b1eb02acc1c44d0580c; lxe=yunicornechu%40yahoo.com; xs=6937dd979d5f3e2ae4e4ae22912f65c9;
lo=HExjW5XqWGyly5VASXeUeQ: lxr=1; locale=en_US; c_user=504568267; sct=1272591608; sid=3; x-referer=http%3A%2F%2Fwww.facebook.com%2Flogin%2Fsession.php%3Flfu%3Dyunicornechu%2540yahoo.com%26next%3Dhttp%253A%252F%252Fwww.facebook.com%252Fhome.php%253Flogin_success%253D1%26lsd%3DHExjW5XqWGyly5VASXeUeQ;
presence=DJ27360832261HDL504568267A3BF27360832511DWMblcMsnDPBbloMbvtP27359066980tP27360445680sbPBtA_7bQBuctP27360832180sA0QBbIADacA29V27360822222848lcPBcvrADrA0.96BtsP27358849500Q; cur_max_lag=2; e=m

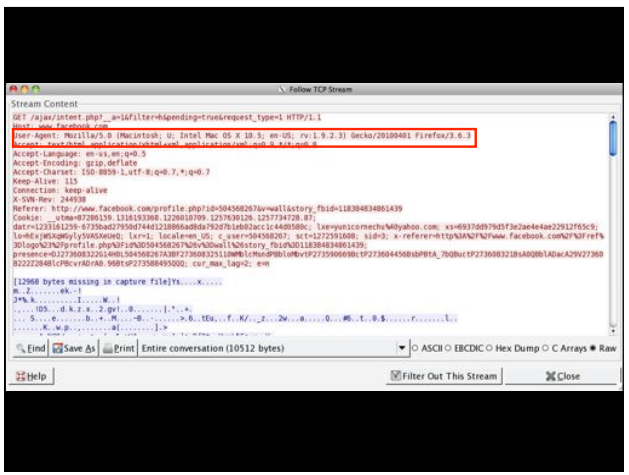
[12968 bytes missing in capture file]Ys....x.....
m..Z.......ek.-!
J*%.k.........I.....W..!
....!D5...d.k.z.x..2.gv!..0.......|.*..+.
...S....e.......b..+..M....~@..-.....>.6..tEu,..f..K/.._.z...2w...a.....Q....#6..t..0.$.....r.....l..
.....K..w.p.....a[.....].>
Find
Save As
Print
Entire conversation (10512 bytes)
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

41


Follow TCP Stream
Stream Content
GET /ajax/intent.php?__a=1&filter=h&pending=true&request_type=1 HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
X-SVN-Rev: 244938
Referer: http://www.facebook.com/profile.php?id=504568267&v=wall&story_fbid=118384834861439
Cookie: __utma=87206139.1316193368.1226010709.1257630126.1257734728.87;
datr=1233161259-6735bad27950d744d1218866ad8da792d7b1eb02acc1c44d0580c; lxe=yunicornechu%40yahoo.com; xs=6937dd979d5f3e2ae4e4ae22912f65c9;
lo=HExjW5XqWGyly5VASXeUeQ: lxr=1; locale=en_US; c_user=504568267; sct=1272591608; sid=3; x-referer=http%3A%2F%2Fwww.facebook.com%2Flogin%2Fsession.php%3Flfu%3Dyunicornechu%2540yahoo.com%26next%3Dhttp%253A%252F%252Fwww.facebook.com%252Fhome.php%253Flogin_success%253D1%26lsd%3DHExjW5XqWGyly5VASXeUeQ;
presence=DJ27360832261HDL504568267A3BF27360832511DWMblcMsnDPBbloMbvtP27359066980tP27360445680sbPBtA_7bQBuctP27360832180sA0QBbIADacA29V27360822222848lcPBcvrADrA0.96BtsP27358849500Q; cur_max_lag=2; e=m

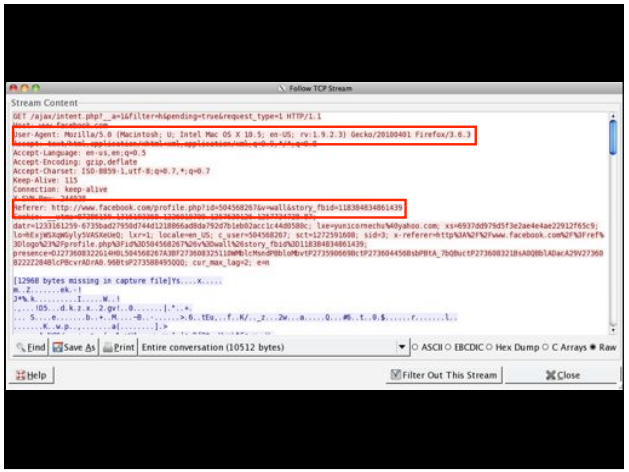
[12968 bytes missing in capture file]Ys....x.....
m..Z.......ek.-!
J*%.k.........I.....W..!
....!D5...d.k.z.x..2.gv!..0.......|.*..+.
...S....e.......b..+..M....~@..-.....>.6..tEu,..f..K/.._.z...2w...a.....Q....#6..t..0.$.....r.....l..
.....K..w.p.....a[.....].>
Find
Save As
Print
Entire conversation (10512 bytes)
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

42

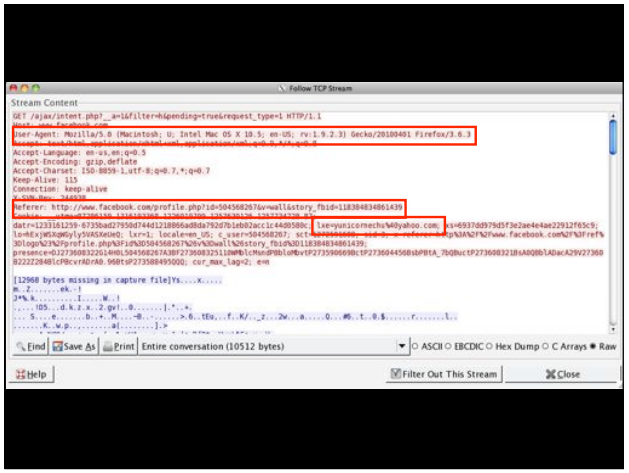

Follow TCP Stream
Stream Content
GET /ajax/intent.php?__a=1&filter=h&pending=true&request_type=1 HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
X-SVN-Rev: 244938
Referer: http://www.facebook.com/profile.php?id=504568267&v=wall&story_fbid=118384834861439
Cookie: __utma=87206139.1316193368.1226010709.1257630126.1257734728.87;
datr=1233161259-6735bad27950d744d1218866ad8da792d7b1eb02acc1c44d0580c; lxe=yunicornechu%40yahoo.com; xs=6937dd979d5f3e2ae4e4ae22912f65c9;
lo=HExjW5XqWGyly5VASXeUeQ: lxr=1; locale=en_US; c_user=504568267; sct=1272591608; sid=3; x-referer=http%3A%2F%2Fwww.facebook.com%2Flogin%2Fsession.php%3Flfu%3Dyunicornechu%2540yahoo.com%26next%3Dhttp%253A%252F%252Fwww.facebook.com%252Fhome.php%253Flogin_success%253D1%26lsd%3DHExjW5XqWGyly5VASXeUeQ;
presence=DJ27360832261HDL504568267A3BF27360832511DWMblcMsnDPBbloMbvtP27359066980tP27360445680sbPBtA_7bQBuctP27360832180sA0QBbIADacA29V27360822222848lcPBcvrADrA0.96BtsP27358849500Q; cur_max_lag=2; e=m

[12968 bytes missing in capture file]Ys....x.....
m..Z.......ek.-!
J*%.k.........I.....W..!
....!D5...d.k.z.x..2.gv!..0.......|.*..+.
...S....e.......b..+..M....~@..-.....>.6..tEu,..f..K/.._.z...2w...a.....Q....#6..t..0.$.....r.....l..
.....K..w.p.....a[.....].>
Find
Save As
Print
Entire conversation (10512 bytes)
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

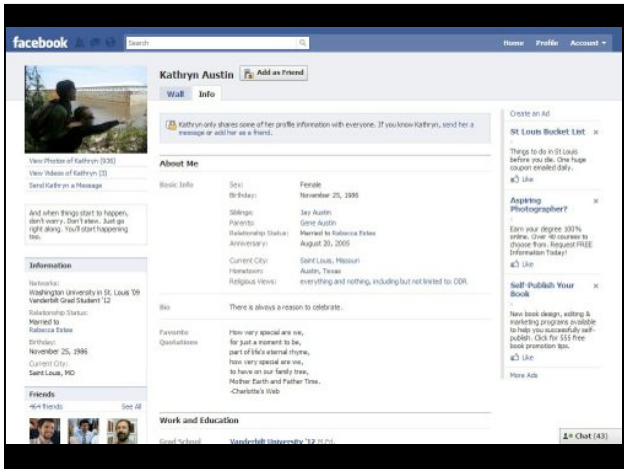
42


Follow TCP Stream
Stream Content
GET /ajax/intent.php?__a=1&filter=h&pending=true&request_type=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.facebook.com/profile.php?id=504568267&v=wall&story_fbid=118384834861439
Find
Save As
Print
Entire conversation (10512 bytes)
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

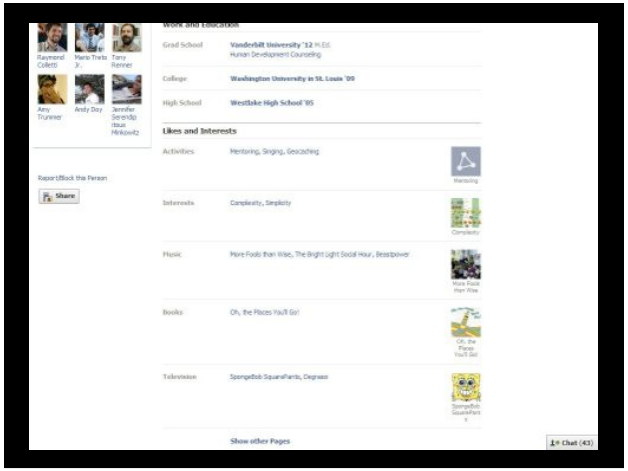
42


Follow TCP Stream
Stream Content
GET /ajax/intent.php?__a=1&filter=h&pending=true&request_type=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.facebook.com/profile.php?id=504568267&v=wall&story_fbid=118384834861439
lxe=yunicornechs%40yahoo.com
Find
Save As
Print
Entire conversation (10512 bytes)
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

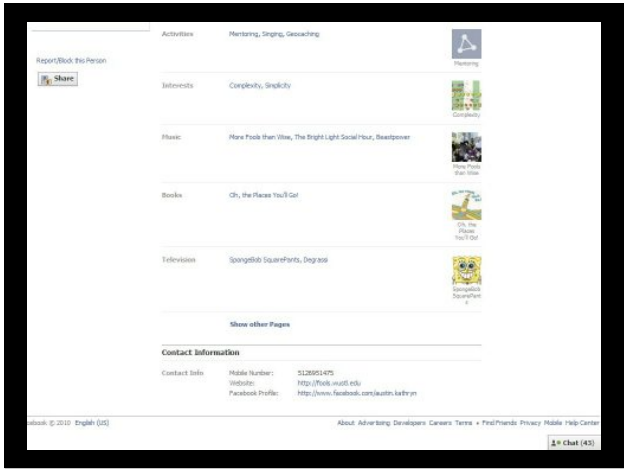
42


facebook
Search
Home
Profile
Account
Kathryn Austin
Add as Friend
Wall
Info
About Me
Work and Education
Chat (43)

43




43




43

Firesheep

Appeared October 27, 2010

Firefox extension

Makes cookie sidejacking *easy*

44

amazon.com
Prime
Shop All Departments
Search
All Departments
Cart
Your Lists
Books
Movies, Music & Games
Digital Downloads
Kindle
Computers & Office
Electronics
Home, Garden & Pets
Grocery, Health & Beauty
Toys, Kids & Baby
Clothing, Shoes & Jewelry
Sports & Outdoors
Tools & Home Improvement
Automotive & Industrial
Outfit Your Kindle
Colorful new covers and sleeves. Shop now
Fight the Cold
Visit Our Winter Warm-Up Store
Shop now
Something for Everyone
Great Features, Low Prices
HDTVs under $499
Amazon Windowshop for iPad
Explore and shop like never before
Inspired by Your Shopping Trends
Get a Free Gund Bear

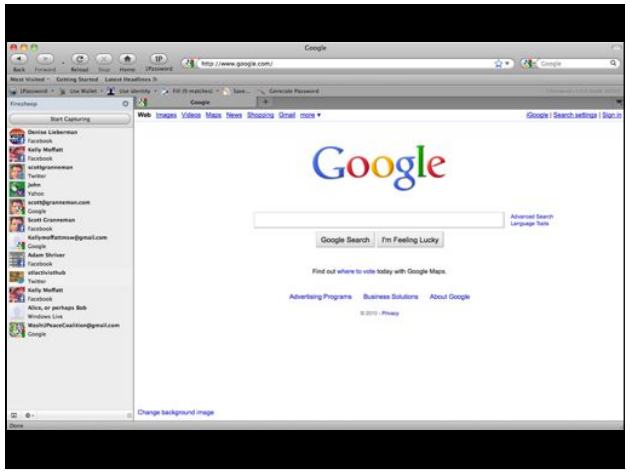
45

Websites
Capture
Websites
Advanced
Amazon.com
Basecamp
bit.ly
Cisco
CNET
Dropbox
Enom
Evernote
Facebook
Flickr
Foursquare
GitHub
Google
Gowalla
Hacker News
Harvest
Add
Edit
Remove
Import
Export

46

Websites
Capture
Websites
Advanced
Foursquare
GitHub
Google
Gowalla
Hacker News
Harvest
Windows Live
New York Times
Pivotal Tracker
ToorCon: San Diego
Slicehost SliceManager
tumblr.com
Twitter
Wordpress
Yahoo
Yelp
Add
Edit
Remove
Import
Export

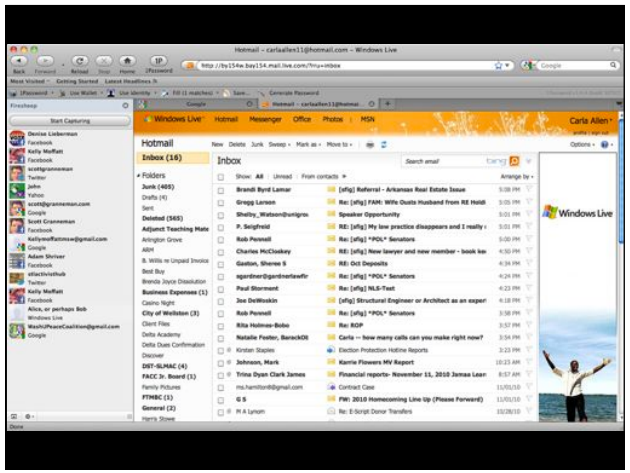
46


Google
Google Search
I'm Feeling Lucky

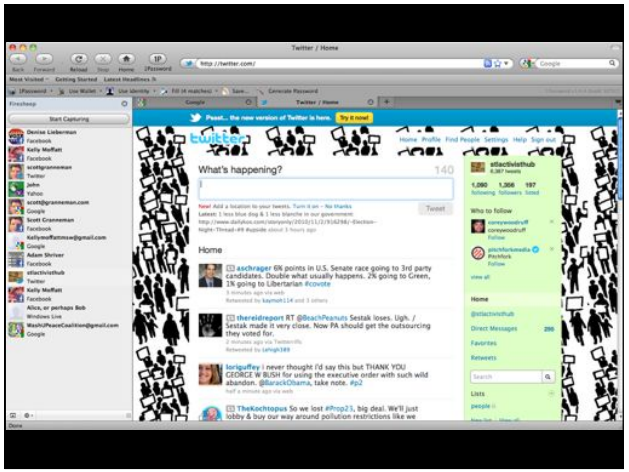
46

facebook
Today is Election Day
News Feed

46


Hotmail
Inbox (16)
Inbox
Windows Live

46




46

The solution: encryption

47

Service providers
(Facebook, Yahoo Mail, Twitter)
need to use HTTPS everywhere

48

Send email using encryption

Read email using encryption

IM using encryption

Conduct e-commerce
using HTTPS

49

VPN
(Virtual Private Network)
encrypts all Internet traffic

StrongVPN
www.strongvpn.com
$7/month

50

Email

✓ Gmail

✓ Hotmail

51

IM

✓ Skype

✓ Google Chat

52

Firefox extensions

✓ HTTPS Everywhere

✓ Force-TLS

53

Google Chrome extensions

✓ Secure Login Helper

✓ KB SSL Enforcer

54

For more info, see my
“Coffee shop WiFi for dummies”

www.securityfocus.com/
columnists/385

55

# Backup

56

# Why?

57

How much data
can you afford to lose?

1 hour?
1 day?
1 week?

58

```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer, If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000D1 (0x0000000C,0x00000002,0x00000000,0xF86B5A89)


***       gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

59

Source: Sylvain Pedneault; edited by jjron; http://commons.wikimedia.org/w/index.php?title=File:FirePhotography_edit1.jpg&oldid=26671960

60

Source: Sylvain Pedneault; edited by jjron; http://commons.wikimedia.org/w/index.php?title=File:FirePhotography_edit1.jpg&oldid=26671960

60

Source: Sylvain Pedneault; edited by jjron; http://commons.wikimedia.org/w/index.php?title=File:FirePhotography_edit1.jpg&oldid=26671960

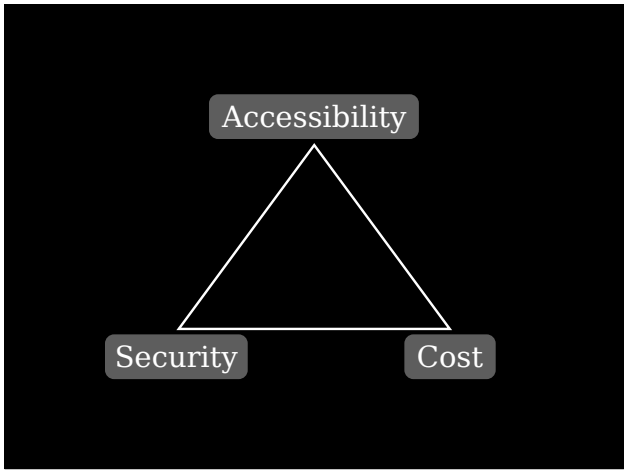
60

Source: Sylvain Pedneault; edited by jjron; http://commons.wikimedia.org/w/index.php?title=File:FirePhotography_edit1.jpg&oldid=26671960

60

Source: Sylvain Pedneault; edited by jjron; http://commons.wikimedia.org/w/index.php?title=File:FirePhotography_edit1.jpg&oldid=26671960

60




61

## Backing Up Online

62

Dropbox
www.dropbox.com

Mozy
www.mozy.com

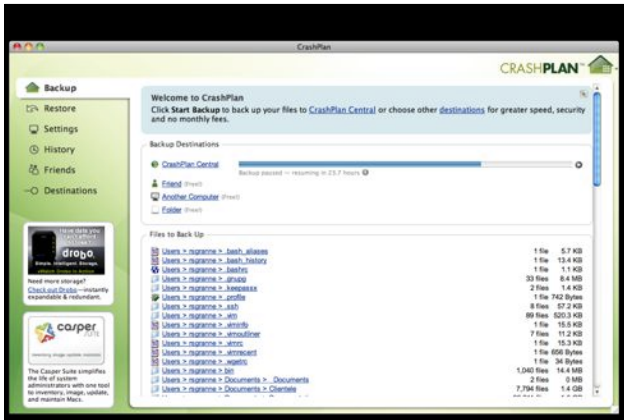
Backblaze
www.backblaze.com

63

CRASHPLAN

CrashPlan
www.crashplan.com

64




65

CRASHPLAN

CrashPlan provides secure unlimited backup to multiple destinations. Add destinations to improve your CrashPlan:

**Friends** — Back up to a friend's computer and pay no monthly fees. Need more room? Attach an external drive to the PC.

**Computers** — Back up between your computers. Laptop to desktop, home to office, Mac to PC... it all works!

**Folders** — Back up directly to an attached drive. Move drive to a remote PC to continue offsite protection.

**Online** — Back up to your favorite third-party provider online.

66

CRASHPLAN

Data encrypted
during transport
& in storage

67

CRASHPLAN

68

CrashPlan+

1 PC/$50/year

2–10 PCs/$120/year

Unlimited data

www.crashplan.com

69

# Backing Up Locally

70

Time Machine

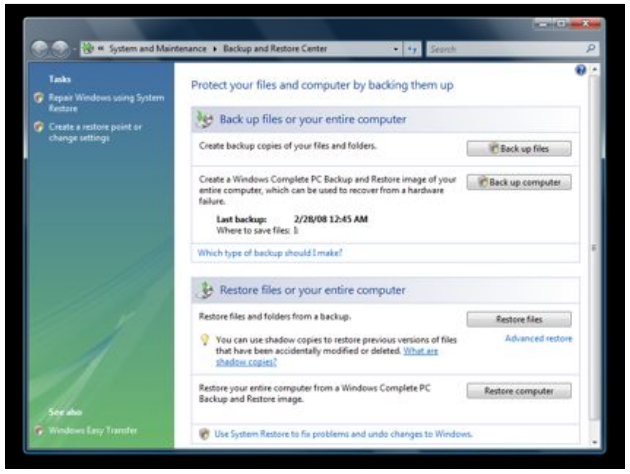
71

72

Backup and Restore Center

73

# Vista only



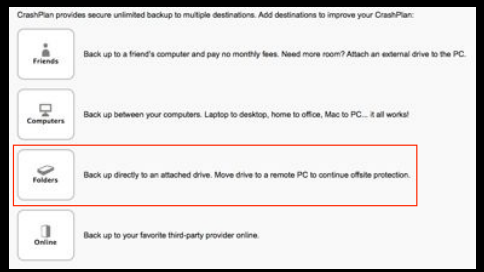

74

| | Backup Personal Files | Backup System Files | Complete PC Backup | Automated Backup |
|---|---|---|---|---|
| Home Basic | ✓ | | | |
| Home Premium | ✓ | | | ✓ |
| Business | ✓ | ✓ | ✓ | ✓ |
| Enterprise | ✓ | ✓ | ✓ | ✓ |
| Ultimate | ✓ | ✓ | ✓ | ✓ |

75

CrashPlan

76




77

# Cloning

78

Carbon Copy Cloner

Free

www.bombich.com

79

Acronis

Acronis True Image

$50 for Home

www.acronis.com

80

Clonezilla

Free

clonezilla.org

81

Backup locally & off-site!

Source: Sylvain Pedneault; edited by jjron; http://commons.wikimedia.org/w/index.php?title=File:FirePhotography_edit1.jpg&oldid=26671960

82

Backup locally & off-site!

Source: Sylvain Pedneault; edited by jjron; http://commons.wikimedia.org/w/index.php?title=File:FirePhotography_edit1.jpg&oldid=26671960

82

Backup locally & off-site!

Source: Sylvain Pedneault; edited by jjron; http://commons.wikimedia.org/w/index.php?title=File:FirePhotography_edit1.jpg&oldid=26671960



Backup locally & off-site!

Source: Sylvain Pedneault; edited by jjron; http://commons.wikimedia.org/w/index.php?title=File:FirePhotography_edit1.jpg&oldid=26671960

82

Backup locally & off-site!

Source: Sylvain Pedneault; edited by jjron; http://commons.wikimedia.org/w/index.php?title=File:FirePhotography_edit1.jpg&oldid=26671960

82

# Passwords

83

Pick a good password

*Password crackers*
will make mincemeat
of poor passwords

84

Guidelines for a good password

1. Don’t use easy passwords
2. Mix of 3 of these 4:

```
A a 1 #
```

3. At least 8 characters
4. Easy to remember
& hard to guess

85

Here's a good method
for picking a good password:

"Where it began,
I can't begin to know when"

Wib,Icbtkw
↓
W16,Ic6tkw
↓
W16,Ic6tkw!



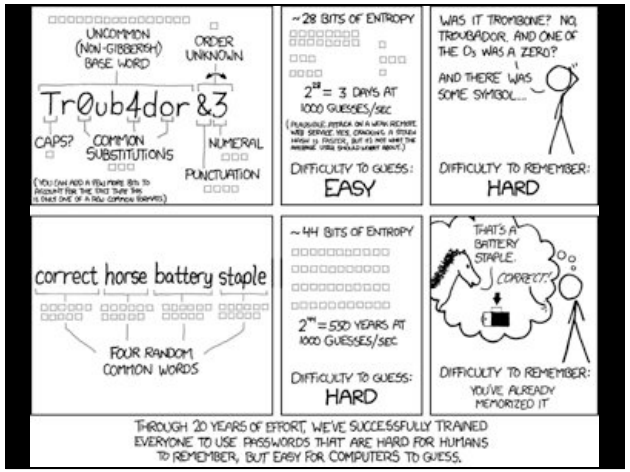
Here's a good method
for picking a good password:

"Where it began,
I can't begin to know when"

Wib,Icbtkw
↓
W16,Ic6tkw
↓
W16,Ic6tkw!



Passphrases are great!




88

robins2006porsche

17 characters

| | |
|---|---|
| number of passwords | $\approx 2^{88} \approx 2.865 \times 10^{26}$ |
| time to enumerate | ≈ 90.85 trillion years (at 100 000 passwords per second) |
| password entropy | 87.89 bits |

89

robins2006porsche911

20 characters

| | |
|---|---|
| number of passwords | $\approx 2^{103} \approx 1.337 \times 10^{31}$ |
| time to enumerate | $\approx 4.239 \times 10^{18}$ years (at 100 000 passwords per second) |
| password entropy | 103.4 bits |

90

4,239,000,000,000,000,000 = 4 quintillion, 239 quadrillion

Use a *password safe*

Generate lengthy, difficult passwords

Securely store passwords

91

92

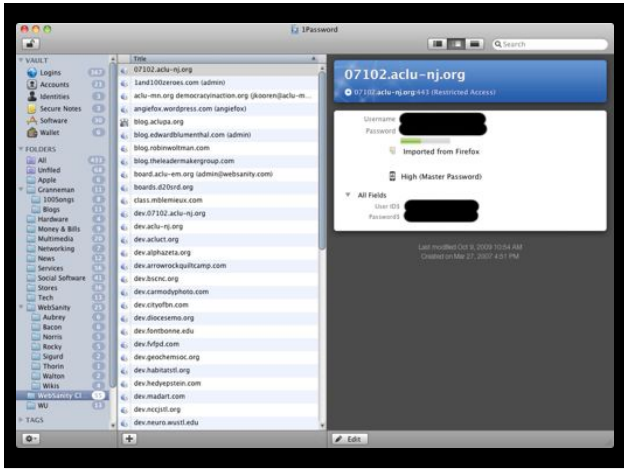
1Password

agilewebsolutions.com/
products/1Password

iPhone/iPad/Android apps too!

$40

93




94

KeePassX
www.keepassx.org

MyPasswordSafe
www.semanticgap.com/myps/

Password Gorilla
www.fpx.de/fp/Software/Gorilla/

All are free & open source

95

Don’t forget to change
the default administrator password
on your firewall!

Default passwords are well known

96

| Maker | Device | Login | Password |
|---|---|---|---|
| Apple | Airport 1.1 | - | public |
| D-Link | DI-704 | - | admin |
| Intel | Wireless 2011 | - | Intel |
| Linksys | Cable/DSL router | - | admin |
| Netgear | RT311 | admin | 1234 |
| SonicWall | Any | admin | password |

www.governmentsecurity.org/articles/DefaultLoginsandPasswordsforNetworkedDevices.php

97

# To Review…

98

What to Believe?

Malware

Wireless

Backup

Passwords

99

You *can* be secure!*

* If you use your head, act carefully,
& understand that security
is a continuous process that never stops

100

101

Thank you!

Email: scott@granneman.com
Web: www.granneman.com
Publications: www.granneman.com/pubs
Blog: www.ChainsawOnATireSwing.com
Twitter: scottgranneman

102

# Personal Security Online:
## Protecting Yourself

Ladue Chapel Presbyterian Church

R. Scott Granneman

© 2006-2012 R. Scott Granneman
Last updated 20120505
You are free to use this work, with certain restrictions.
For full licensing information, please see the last slide/page.



## Licensing of this work

This work is licensed under the Creative Commons Attribution-ShareAlike License.

To view a copy of this license, visit
http://creativecommons.org/licenses/by-sa/1.0
or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

In addition to the rights and restrictions common to all Creative Commons licenses, the Attribution-ShareAlike License features the following key conditions:

**Attribution**. The licensor permits others to copy, distribute, display, and perform the work. In return, licensees must give the original author credit.

**Share Alike**. The licensor permits others to distribute derivative works under a license identical to the one that governs the licensor's work.

Questions? Email scott@granneman.com