Protecting your Home Environment

From V[illains] Thieves and [Squir]rels

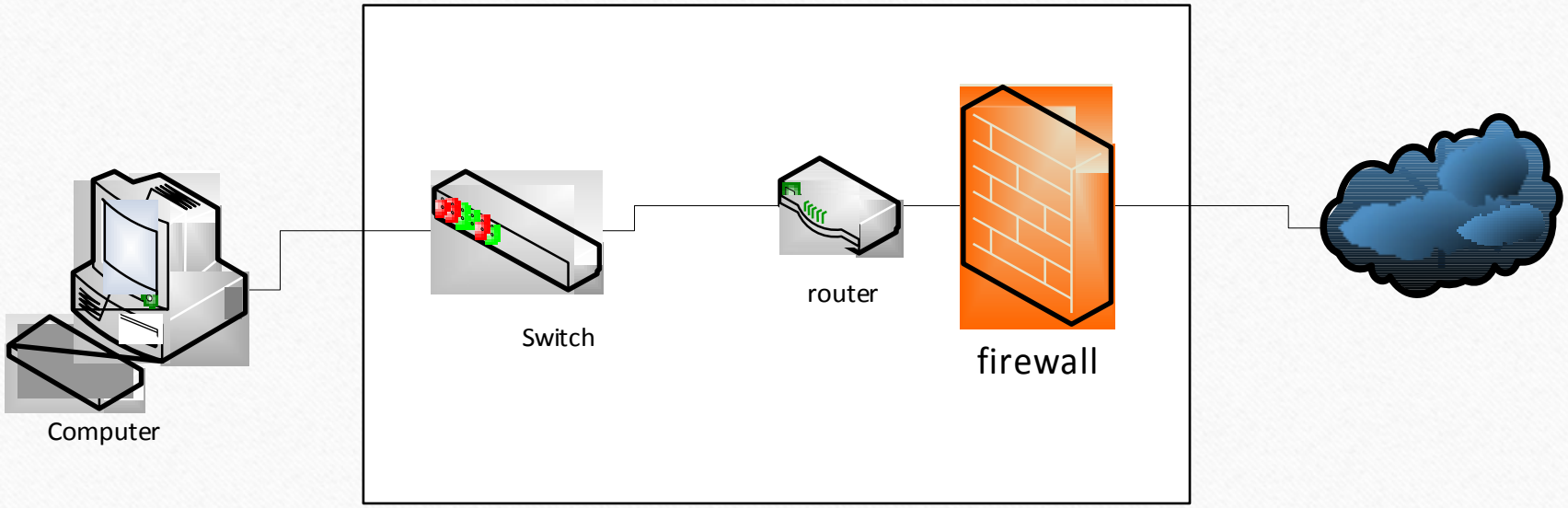
Intro

- Mark Wich
- BS in Computer Science
- MS in Telecommunications Management
- 35 Years of datacenter management experience
- Programming since 1966

Home network basics

- How do we connect to the internet?
  - Dial-up
  - DSL
  - Cable modem
  - FIOS
  - U-verse

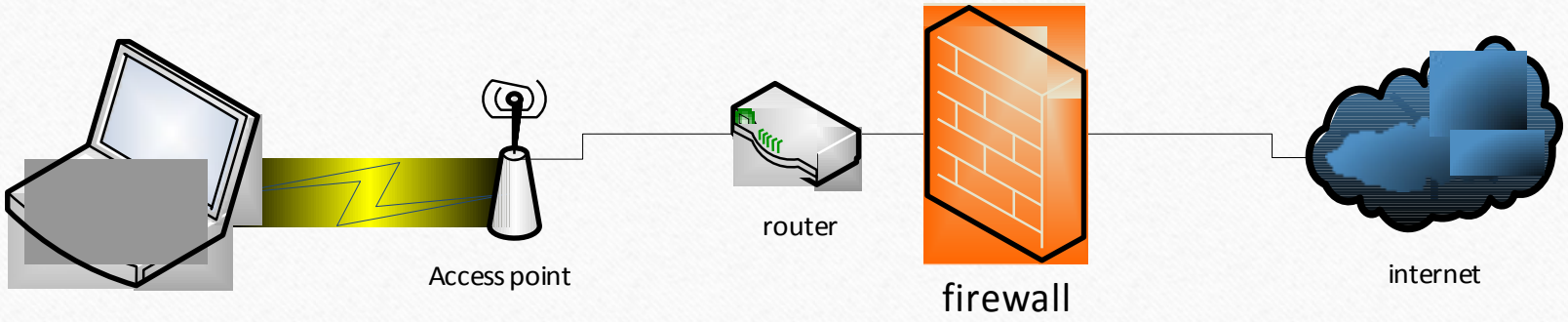
Typical Setup



Things to look for and change

- Password

Wi-Fi



Things to look for and change

- SSID
- WiFi passwords
- MAC filtering

Anti-Virus

- You should always install only **ONE !**
  - Do not think if one is good two is better.
  - Free is good enough
  - Scan weekly

Antivirus Vendors

- Norton
- Trend
- McAfee
- Kaspersky
- Panda
- Avast

Operating system Survey

- Android
- Mac
- Windows
- IOS
- Other

Operating system security

- Computers should ask for password or words when powered up.
- Screen savers should ask for a password
- Change them once in a while

Email

- Vendor Survey
- Webmail
- POP3
- Exchange
- IMAP
- SMTP

Email do's and don’ts

- Do have anti-virus running
- Do scan all downloads before running.
- Notify your service provider about pfishing emails
- Don’t open attachments from people you don’t know
- Don’t click on links inside emails even if you think you know where you are going. Always check.

Surfing 101

- Install ad blocking software
- Install webmail ad blocking software
- Stay away from pirate and porn sites
- Make sure that a pop-up blocker is enabled
- Beware of any popup that says your computer is infected
- If a browser offers incognito mode use it.
- Jealously guard **ANY** personal information

Surfing 101 Part 2

- Do not let web sites store your personal information
  - It may be a pain but you are depending on their security
  - If you don't give it to them they can't lose it.
  - Never store passwords to banks or other financial institutions
- When your browser offers to store a password the answer is **NO**
  - Anyone that has physical access to your computer can then impersonate you.

Surfing 101 Part 2

- Do not let web sites store your personal information
  - It may be a pain but you are depending on their security
  - If you don't give it to them they can't lose it.
  - Never store passwords to banks or other financial institutions
- When your browser offers to store a password the answer is **NO**
  - Anyone that has physical access to your computer can then impersonate you.

Cookies, Trackers , add-ons and other nasties

- Cookies – bits of data stored on your computer by a web site
- Trackers - A program or data that can be used by a third party to identify a user or computer also known as a third party cookie
- Add-ons – Programs that when added to a browser do good/bad things.

Password security

- Get a notepad
- Pick a phrase ie (Tomato4soup)
- In you notepad write 3 things separated by commas
  - Site name
  - Username
  - Tword

Password security (cont.)

- Do this for all your sites/usernames/passwords
- Use variations tword4 = tomato4soup4
  - In the book :
    - Citibank, milominderbinder,tword4
    - Yahoo,milominder25,Tword7
    - Gmail,milo123,Tw0rd35
- **Do not use the same password for more then one site**

Password security (cont.)

- Take a picture or pictures of your notebook with your phone
- Instant password security
- There is no place that the actual password is ever written down.

On-line banking

- Do not use your phone EVER. (personal prejudice)
- Do not store passwords
- Beware of emails from your bank. They may not be from your bank

Q&A

The End