Internet Safety
Evangelism

Kevin Russell, CISSP
Why Should We Care?

- Where do the attacks on our businesses come from?
  - Botnets – Running at homes
- Second Nature to InfoSec Professionals
  - Total Confusion to the average computer user
  - Thus their systems are completely un-protected
- It is our job! Who else is qualified?
The Message

- How to Protect Their Network
- How to Protect Their Family and Privacy
- Internet Do’s and Don’ts
- Where to Get Help
Protect

- How to protect their home network
  - Physically – Firewall
  - Logically
    - Firewall
    - Anti-Malware
    - Additional tools
    - Browser add ons
    - Browser history/cookie/password settings
- Wireless
Protect

- Anti-Virus pop-up scams
- Patching and Updating
- Tools
  - Immunet Project
  - Comodo System Cleaner
  - AVG Linkscanner
  - Threatfire

- Linux and Mac
Securing Your Home

HOW?
- Install firewalls in a layered defense
Protecting Your Family

- Predators
  - The Internet is full of them
    - Talk to your youth about the danger
      - Don’t “Friend” people you don’t know!

- Cyber-bullying
  - It is real – Talk to you kids

- Monitor activity
  - What to watch for?
    - MySpace, uTube, Facebook
    - IM activity
    - File transfers
The Most Common Question from Parents

- Social Media (The Chat Room of web 2.0)
  - Facebook, MySpace, etc are public, everyone can read what you type – UNLESS YOU PROTECT IT
  - Real life rules apply to all social media sites!
  - Don’t talk to strangers, don’t “friend” strangers!
  - Assume that everyone in chat is lying!
    - Most 13 year old girls ARE NOT, some could be creepy old men!
    - Never use your name, your age, your hometown, your school, your……etc
  - Lie – This is where you use your “persona”
    - Don’t post personal information in your profile!
  - Meeting people from the Internet in person
    - Don’t
    - NEVER

Did you know the Facebook min age is 13?

Pay attention to What you put On your wall
Protecting Your Family

- Your Teen’s habits!
  - Does your youth disappear and ONLY work on the computer when you are NOT around
  - Do they turn off the screen
    - Change windows
    - React when you come in or look
    - Pay attention
Internet Safety & Security

Parental Tools

- Control and Blocking Tools
  - OpenDNS
  - www.getk9.com
  - SafeEyes 6
  - Specter Pro 2009

- Specialized Browsers
  - Peanut Butter PC – A safe kids browser
  - KidZui – Safe Internet kids browser/environment
  - Online Family Norton – free if you own Norton AV
Parental Tools

- Get Educated
  - www.getnetwise.org
  - www.software4parents.com
  - www.cyberangels.org

- Parental Advice Sites
  - www.safeisbeautiful.com
  - See next slide!
Parental Tools

Parental Resources on the Internet

Private Sites
- www.childsafe.com
- www.nap.edu/netsafekids
- www.wiredsafety.org
- http://www.netsmartz.org/

Government sites for good information
- www.fbi.gov/publications/pguide/pguidee.htm
- www.ftc.gov/bcp/consumer.shtm
- www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm
- www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.shtm
- www.cybercrime.gov/rules/kidsinternet.htm
- www.onguardonline.gov
- www.ftc.gov/yourarehere
The Internet - Tips

- The Browser
  - Three major players
    - Internet Explorer – Microsoft
      - Set to stop history, passwords, and cookies storage
    - Firefox – Mozilla
      - Set to stop history, passwords, and cookies storage
      - Use many great add-on
        - Noscript, ad block plus, better privacy, WOT
    - Chrome – Google
      - Set to stop history, passwords, and cookies storage
      - Use extensions
        - Ad block plus, WOT
The Internet - Tips

- **Scams**
  - Many scams involve email directing you to a site to “fix” your personal information. These emails look legit and usually inform you that
    - “Due to a security breach we need to validate your information…. Follow this link: ___________”
    - This link takes you to a site that LOOKS like the correct site.
      - You enter your information and they use it against you
  - **What to do if you suspect a scam**
    - If you get any email like this go to the site by keying in the usual one you use. If this is real they will have a splash on the front page with instructions and a pointer.
    - Don’t go there
Digital Information – A Discussion

- Your own website/Facebook/MySpace is cool, & not!
  - Don’t put your real name and information on it
    - Name is ok if you do not use city, school, other traceable info
    - Keep the info to a minimum
    - Everything you post will add to the information a predator can use against you
  - If you must post pictures of yourself
    - Be aware of where it was taken
    - What are you wearing? (this has nothing to do with s**)

- Digital Images
  - They last forever!
  - Be aware of what pictures / video you are in….
How Can You Help?

- Get Involved
- Talk to Groups
- Offer advice
Visit Spike at www.spikedsecurity.com for advice about your Internet safety!

Kevin Russell, CISSP
Director of Information Security at Infogroup
Author of Spiked Security Blog