Cyber Security Notes - mlt

On March 18, I heard Mr. David Aucsmith speak in to a cyber security forum. Mr. Aucsmith is Senior Director, Microsoft Institute for Advanced Technology in Governments, Microsoft Corporation. It was one of those rare presentations that turned out much more interesting than it sounded like it was supposed to be.

> http://www.cc.gatech.edu/inside/board/david-w-aucsmith
> FYI – he does have a hobby……
> http://aucsmithphoto.com/photographer.html

I expected the usual warnings about computer security and recommendations to prevent employees from using anything more complex than a manual adding machine. Instead, Mr. Aucsmith provided a fact-filled exploration of the real world of computer hackers versus computer security experts. I was surprised to enjoy the presentation. He changed my opinion about a few personal computer security issues.

Included below are my comments and opinions based on his presentation. *Nothing in this should be attributed as quote of Mr. Aucsmith – I've paraphrased, rewritten and interpreted most of this.*

Speaking about Microsoft specifically:

- ☐ Microsoft software is used in nearly 80% of the world's critical information systems.
- ☐ Microsoft systems get nearly 40,000 cyber attacks per day.
- ☐ Microsoft corporation has over 106,000 users of over 360,000 PCs
- ☐ MS Hotmail processes 1.9 million messages per second
- ☐ MSN search engines crawl the entire web every 3 weeks updating their index

Speaking of the computer industry as a whole:

Most active computer criminals:

- ☐ Are currently located in China and Eastern Europe
- ☐ Are professional criminals interested in extortion or money
- ☐ Buy and sell tools among themselves to help be better criminals
- ☐ Are actively learning new tricks and seeking new victims

Most dangerous web sites for catching a virus or malicious program (in this order):

- ☐ Game cheats – *"how do I win at this stupid video game?" Now we know why a certain teenager's computer always seems to be the one that gets infected.*
- ☐ Pornography – *"hubba hubba baby"*
- ☐ Pop Star fan sites – "*What color socks is Britney wearing today?"*

Most dangerous month for fake web sites and email scams:

- ☐ April – Income-tax-related scams, email phishing, and fake web sites

Most insecure and most often infected computers:

- ☐ The old hand-me-down PC given to kids, teenagers and grandparents. Because it usually has the old operating system and rarely gets upgraded security software.

Most dangerous time for new computer virus infections:

- ☐ About 3 days after the virus or computer vulnerability is announced. Because hackers have used the 3 days to improve their attack and most victims have delayed uploading the security fixes. Accordingly, it is recommended that you install computer security patches as soon as you can after they are released.

Most likely way that someone will steal money from you on the internet:

- ☐ You'll give it to them by providing a bank account number, credit card number or personal information to a fraudulent web site or by responding to a malicious email message

Most common mistakes for novice users:

- ☐ Using the same password for all financial and banking web sites
- ☐ Clicking the button that says "Click here for a free, really spiffy……"
- ☐ Failing to think before responding or clicking the button

Mikey's pet peeve

- ☐ Otherwise good computer users who won't read the help files, learn to use "Google" information to avoid questionable scams and who won't take the time to train themselves to operate this complex (and financially risky) piece of equipment we call the internet.

Most surprising:

- ☐ When Windows crashes and the little dialog box pops up asking if you want to send an error report to Microsoft – **send the report**. Microsoft **does** look at the reports and **does** use them to fix problems.
- ☐ Almost 48% of crashes reported to Microsoft are caused by problems with a video drivers and 51% of crashes are caused by Malware

Mikey's recommended strategy for home PC users:

1- Read the instructions and be sure you understand how to download updates and do routine maintenance. *Remember your parents wouldn't let you drive the car until you knew how to change a flat tire*.
2- Learn common computer terminology and learn how to find answers.
3- Read the darn screen messages and dialog boxes. *I got a thingy that was some sort of error or warning or something but I don't remember what it said I just clicked the buttons – 2 or 3 times.*
4- Get and use an automatic password generator to help create secure passwords. *Write them down at home if you have to and store them in the sock drawer. You can almost be sure that a burglar in your house wouldn't be looking in your sock drawer for computer passwords*
5- Be sure all users of your computer (kids, spouses, in-laws) know what to watch out for, what the most dangerous web sites are and how to respond to threats. *If they don't know how to drive, don't give them the keys to the family car!*
6- Use common sense. *The Nigerian Government doesn't need my help; I can't win the Irish Lottery if I never play it; nor did a 20-year-old hottie suddenly get the urge to date an old fat guy.*
7- Install, update and use a good antivirus program.
8- Perform regular maintenance tasks every few months – depending on how much time you spend connected to the internet: *(note: these are all separate actions and not alternatives. I recommend you do all of them at least every 5,000 miles).*
    a. Verify you have downloaded and installed the latest updates for your computer operating and security systems.
    b. Let your anti-virus do a full system scan
    c. Run the windows Malicious Software removal tool *(link below)*
    d. Run Windows Defender and have it do a full scan *(Since I use a good anti-virus program, I don't normally have Windows Defender running all the time, just when I do the scan)*
    e. Run Ad-Aware and/or Spybot to clean up malicious advertisements *(I normally don't let either one of these run in the background either – preferring to clean up later instead of slowing my system down)*
    f. Run Windows Cleanup and delete temporary files
    g. Run disk defragmenter to clean up the hard drive

More References:

- ☐ Malicious Software Removal Tool
  http://www.microsoft.com/security/malwareremove/default.mspx
- ☐ Windows Defender
  http://www.microsoft.com/athome/security/spyware/software/default.mspx
- ☐ Security at Home
  http://www.microsoft.com/protect/default.mspx
- ☐ Parental supervision and age-based guidance
  http://www.microsoft.com/protect/family/default.mspx