

# Internet Security for home users

CPAC Seminar : 2016-05-07

# Note

- This PowerPoint presentation has been modified
  - To include information discussed during the seminar
  - To help those who did not attend the seminar in person better understand the topics discussed
- Title has been changed
  - from “Cyber Security” to “Internet Security for Home Users”
- Additional slide has been added
  - Added a slide to cover Ransomware
    - This topic was not in the initial topic list, however was discussed during the seminar
    - It was intensely discussed by questions raised from the audience
  - Added a slide to cover SandboxIE
    - Audience show great interest to this powerful browser protection software

# Jin Cao (j-cao@live.com)

- Over 30 years of IT
  - Programming
  - Application development
  - System integration
  - Network management
  - Tech support
- 18 years in information risk & security
  - Information system risk assessment
  - Security technology implementation
  - Project consulting
  - Incident response and investigation
  - Computer forensics
  - Etc., etc., etc.
- CISSP, ISSAP, CISA, PMP, GCFA, CIPP/C
- (ISC)<sup>2</sup> and ISACA
  - Exam development
- IAPP
  - Board of exam development
- Sr. Information Security Analyst
- Security Architect
- Program Lead

# Topics

- Attacks via Email
- Securing Your PC
- Securing Your Data
- Ransomware
- Cloud Storage
- Web Browsing
- Home Firewall
- Free Stuff

# Attacks via Email

- Spoofing
  - Message sent from your old friend
  - Message sent to you by yourself
  - Message with subject line Re:
- Spear Phishing
  - Urgent
    - From your boss
    - Friend hit by a truck needs money
  - Attractive
    - Too good to be true
  - Fear
    - Bank account being hacked, need you to rest password
- Random Stuff
  - Body part enhancement
  - Failed delivery
- **How to handle them – before opening it**
  - Do NOT click on the links
  - Do move it to spam / junk folder
  - If you really want to open the message, open it inside the junk folder
  - Type the link to browser instead of clicking it

# Securing Your PC

- User accounts
  - Root / administrator
    - Use a strong password
      - Upper / lower case; Letter; Numerical; Special character
      - **Never browse the internet when log on as administrator**
  - User account
    - Always create a separate user account for daily activities
  - Child account
    - Create a separate child account if you share the PC with your kids
- Anti-Virus
  - You must install anti-virus software to your PC – before installing anything
  - Buy / Free (see Sophos)
  - Make sure auto update is on

# Securing Your PC

- Sophos Free Tools
  - Sophos Home for PC and Mac
    - Anti-Virus
    - Anti-malware
    - Web filtering
  - Mobile Security for Android
  - XG Firewall Home Edition
    - Anti-Virus
    - VPN
    - Email filtering
    - Web security and URL filtering
    - Monitoring and reporting
  - Virus Removal Tool
  - Anti-Virus for Linux Free Edition

## SOPHOS



# Securing Your PC

- Patching
  - Enable system auto update
- Create recovery disk
- Webcam
  - Block webcam when not in use
- Enable Windows Firewall
- Be careful when using Free Public WiFi
  - Be afraid, be very afraid
    - Turn off auto connect
  - Do not connect when you see “certificate does not match”
  - Check if google.com site has certificate error



# Securing Your Data

- Encrypt your most important data
  - Master password list
  - Bank account information (i.e. ID and password; statement)
  - Tax return files
- Back up your data
  - External hard drive – if you have large amount of data (photos, design files, etc.)
  - USB stick – quick and easy for small files
  - Daily / weekly back up schedule – set up regular back when use external hard drives
  - Password Safe – keep your important accounts and passwords
  - Back up files to the cloud (subscription fee may apply)

# Ransomware

- You may get hit by ransomware if you
  - Clicked a link from spam email
  - Visited a malware affected website
- When you got hit by ransomware
  - Your files are encrypted and the attacker has the key
    - Photos, family documents, business data, etc., etc.
  - You are asked to pay to get the key
  - Files may be deleted if you delay payment
  - After you made the payment and get the decryption key, you maybe able to decrypt the files
- What can you do?
  - Not much luck – a number of police department had to pay to get their files back
    - Are you more capable than police?
  - Do Not click links in emails
  - Do Back up your data – so you can wipe the system and restore from back up

# Cloud Storage

- Dropbox
- OneDrive
- Google Drive
- iCloud
- 百度云
- Mi Cloud



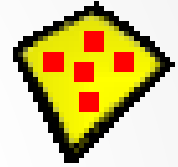
OneDrive



- Always Encrypt Important Data before upload
- Keep ID and password to a safe place
- Avoid connecting to the cloud when using free WiFi

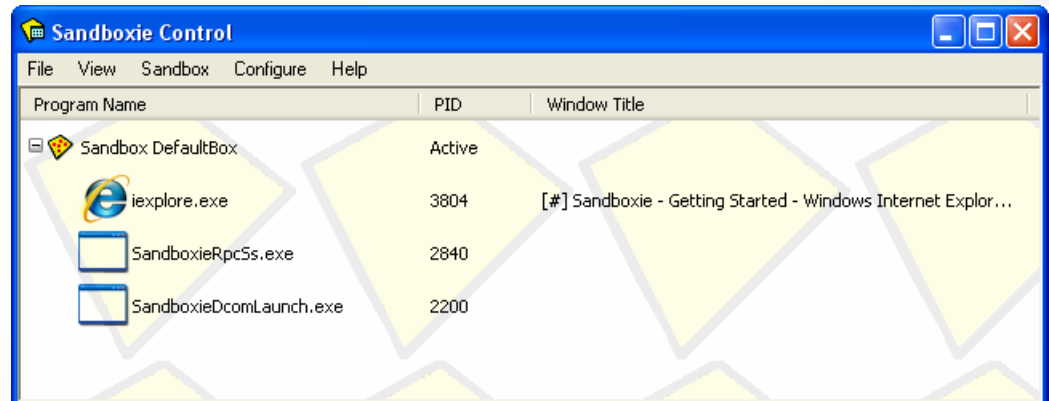
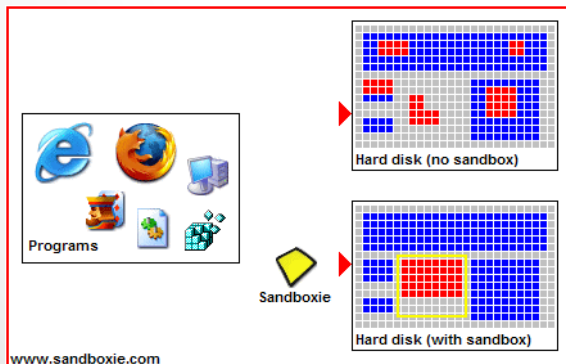
# Web Browsing

- Do use NoScript
- Do use AdBlock
- Do use SandboxIE
- Do use at least two different kinds browsers (IE, Chrome, etc.)
  - General purpose – do not allow JavaScript, block ads, run sandboxed
    - News
    - Novel
    - Forums
    - Everything
    - Do not save passwords
  - Special purpose – allow JavaScript
    - Online banking
    - NetFile Tax return
    - Online shopping
    - Travel agency



# Web Browsing

- Run web browser from the inside the SandboxIE
  - Malware downloaded will be quarantined to Sandbox location
  - System files and user files are protected
- SandboxIE is free to home / personal use
  - After 30 days you will see a pop up reminder to register (to pay)
  - You can still keep using it after the pop up closed
- SandboxIE registration fee is Very Low
  - \$25USD for one PC, \$50USD for 3 PCs and \$75USD for 5 PCs (for life)



# Home Firewall

- Sophos UTM home edition – a perfect DIY project
  - Full Installation or VM appliance
  - Anti-Virus
  - VPN
  - Web security and URL filtering
  - Email filtering
  - Etc., etc., etc.
- pfSense (Community Edition)
- Build your own
  - FreeBSD
  - Linux
- On the Cloud
  - Host business applications to the cloud

# Free Stuff

- Fill the form to enter a prize draw
  - What did you give out?
  - Where will it go?
  - Who is collecting it?
  - How will it be used?
  - How long will it affect you?
- Free USB keys for you (ever got one from a trade show?)
  - What is the content?
  - What will it do if you click it open?
  - What will you use it for?
  - DO YOU REALLY NEED IT?
- Be very careful about the free stuff

# Resources

- Microsoft Safety and Security Center
  - <https://www.microsoft.com/en-us/safety/pc-security/default.aspx>
- Sophos Free Tools
  - Sophos Home for PC and Mac
  - Mobile Security for Android
  - XG Firewall Home Edition
  - Virus Removal Tool
  - Anti-Virus form Linux Free Edition
  - <https://www.sophos.com/en-us/products/free-tools.aspx>





- Password Safe
  - <https://www.schneier.com/cryptography/passsafe/>
- BitLocker (Windows 7, 8, 10 Ultimate & Pro)
- 7-zip
- GnuPG
- SandboxIE
  - <http://www.sandboxie.com/index.php?HomeUse>

# Questions



Send your questions to [j-cao@live.com](mailto:j-cao@live.com)  
Add “CPAC seminar” to the Subject line!