Network and Internet Best Security Practices

Hosted By

A Best Practice can be described as:

- Documented and effective procedures and methodologies developed by knowledgeable bodies; which have been shown to provide reasonable assurance of desired outcomes.

Top Five : Best Security Practices in Small Office/Home Office Networks

1. Use Anti-virus and Personal Firewall Software on every personal desktop
2. Use obscure and hard to guess Passwords
3. Keep Operating System and other Software Updated with patches and updates.
4. “Prepare for the Worst and Hope for the Best”
5. Be Aware

Use Virus Protection Software

- Use an activated and updated copy of anti-virus and/or personal firewall (PC-cillin, Norton's, etc...)
  - Your protective software is only as smart as you let it be.
  - Update your virus definitions daily.
  - Be prepared for some configuration and personalization. Protection is a double-edged sword

Use obscure and “hard to guess” Passwords and User Names

- General Rules of Thumb:
  - **Do Not Use**:
    - well-known personal information as your password(s). Spouse’s name, child’s birthday, title, etc...
  - **Do use:**
    - Both letters and numbers
    - At least two easy to remember components to you password.
    - If you like chili and you like golf. Your Password could be “chili_golf2”.
    - Misdirection or Substitution

Password and User Name Misdirection

- User Names
  - Use modified user names
    - First initial + Last Name
    - First Name + Last Initial
    - For instance: jsmith or joes, never joe or other common first names
- Passwords
  - Substitute easy to remember numbers for similar letters. (A=4, E=3, I=1, S=5, B=8, O=0)
  - My password : chili_golf2 = ch1l1_g0lf2

Keep Your Operating System and Software Updated

- Security patches are a fact of life. You should allow for operating system updates at least once a week.
  - Can be set to Automatically Update
- Keeping your Operating system updated is critical to system integrity.
- Most Software allows the user to check for updates on a regular basis.

Prepare for the Worst, and Hope for the Best

- When should I wonder if My PC is Infected?
  - System crashes and reboots multiple times during use
  - System or programs stop responding, or lock up often
  - System restarts, on it’s own, but fails to start normally
  - Distorted menus and/or unusual error messages
- Complete System Scans should be done once a week.
  - Anti-Virus Software has this ability
  - Available Online

Prepare for the Worst, and Hope for the Best

- What to do if you think your PC is infected
  - Run system-wide virus scan immediately
  - Additional Virus Scans may be necessary because some viruses can compromise already installed anti-virus software
    - Online Scans are available for this purpose
- What to do if you know your PC is infected
  - Disconnect your system from the network so you won't infect the entire network
  - Don't Shutdown or Log off . This is often a trigger mechanism for viruses
  - Call your System Administrator or other Computer Professional

Be Aware

- When you close your Internet Browser your computer is still connected to the Internet
- Messaging software applications such as MSN Messenger, Yahoo Messenger, and AOL Instant Messenger provide an always on port for hackers to come through.
  - Hackers can send viruses, malware, spyware, etc. through these openings
- Third Party Programs like NewsOK.com and Weatherbug can be harmful too.
  - These Programs use bandwidth and memory affecting your computer's performance

Be Aware

- Some computer viruses scan an infected PC's e-mail address book, and proceed to send deceivingly friendly e-mail messages disguised as the infected computers owner.
  - Sends a virus out to all members of your address book disguised as your email address
- Just because you receive an e-mail from a friend or acquaintance with a virus attached, doesn't necessarily mean that, that person's computer is infected with a virus.

Be Aware

- Most ordinary hackers are like any other thief or bully:
- Weaker targets are favored
- Stronger targets are avoided
- Avoid being a target at all
  - Pay attention to where you are and what’s happening to your computer.

Trojan Horses

- Definition of a Trojan Horse
  - A malicious program disguised as a legitimate file. Once installed on the victim's computer, the Trojan allows a remote hacker to take control of the machine and use it for any number of nefarious purposes.
- Trojan Horses are used to create zombie computers which are typically used to send spam email and viruses
- Eat up bandwidth

Spyware

- Software that monitors a user's keyboard activities and transmits this information back without the user's knowledge
- 90% of Internet-connected computers are infected with Spyware
- Spyware attacks expose individual users and corporations to identity theft, data corruption, or personal profiling
- Comes from downloading free software

E-Mail Security

- Protection should begin at the server level
- E-Mail is not secure.
- E-Mail is sent in plain text and every server the e-mail passes through could be capturing the text of the e-mail.