Small Office Best Practices – Top 10

mantra COMPUTING, INC

Network Management

Computer and network support for the small business… your freedom to focus.

1. Protect LANs with a quality SPI or DPI (new standard) firewall appliance such as those provided by Sonicwall or Cisco.

2. Protect all laptops as well as computers that access a company LAN remotely through a VPN with a personal firewall such as Windows XP SP2 built-in firewall or ZoneAlarm personal firewall.

3. Protect all computers with Up-to-date antivirus software that updates its virus definitions twice daily and performs weekly full system scans. Networks with 5 or more computers should implement centrally managed virus protection and gateway protection where possible.

4. Ensure you have a documented and tested backup routine with adequate levels of redundancy and retention for your organization.

5. Establish a Network Use policy that all network users are required to read and sign.

6. At the Server level, filter incoming emails for SPAM, executable file attachments (EXE, PIF, CAB, VB, VBS, INF, SCR, and BAT) and known viruses.

7. Protect network hardware including switches, routers, firewalls, etc. as well as servers and critical computers by using UPS equipment (Uninterruptible Power Supply).

8. Educate network users on privacy concerns as it relates to electronic communications and data storage. Encryption and metadata removal tools should be implemented to limit your organization's exposure to liability.

9. Maintain good network password policy – Passwords need to be long enough (6+ characters) and complicated enough (Mixed Capital, lowercase, numbers and symbols) to protect users, but not so complicated they forget them or write them down (Ex. meRRyxma$).

10. All Windows computers should be setup for automatic download and installation of Microsoft Windows Security patches.

Bonus Entry:

11. Have a Spyware mitigation strategy in place that includes SPAM filtering, Internet content control and/or centrally managed antispyware software such as Webroot's Spysweeper or Sunbelt's CounterSpy.

MANTRA COMPUTING, INC.
233 Needham St.
3rd Floor
Newton, MA 02164

Phone: 617.454.1310
Fax: 617.454.1001
www.mantracomputing.com
info@mantracomp.com

Mantra Computing Small Office Best Practices – Top 10 for Individuals

1. Good password practice:
   a. Maintain two passwords: One for high security applications including online bank and credit card accounts and a second for low security applications which include email and network accounts. Network and email passwords are often seen by individuals and organizations that have weak or no privacy and security policies.
   b. Passwords need to be long enough (6+ characters) and complicated enough (Mixed Capital, lower case, numbers and symbols) to protect users, but not so complicated they forget them or write them down (Ex. meRRyxma$).You should change your passwords every six to twelve months.

2. Good email practice:
   a. If you have the option, use an email client such Eudora www.eudora.com, PocoMail www.pocomail.com, and Pegasus Mail www.pmail.com other than those by Microsoft (Outlook Ex press or Outlook).
   b. If you can tolerate it, disable the preview pane.
   c. Never open emails that have attachments with executable or double extensions (Ex. note.txt.exe, .scr, .exe, .pif) or that have nonsensical subjects, even if they are from people you know.

3. Use Up-to-date antivirus software such as Norton Antivirus or eTrust EZ Antivirus that updates its virus definitions twice daily and performs a full system scan weekly.

4. Setup and follow a Backup Routine that is simple to follow and has adequate levels of redundancy and retention.

5. Use personal firewall software such as Windows XP SP2 built-in firewall or ZoneAlarm personal fire-wall.

6. Protect yourself from Internet Spyware by using a Spam filter and installing Antispyware software such as Webroot's Spysweeper or Sunbelt's CounterSpy.

7. Educate your self about privacy concerns as it relates to electronic communications and data storage. Encryption and metadata removal tools should be implemented to limit your exposure to liability.

8. Always include a 3-year parts and labor warranty with any new computer purchase.

9. Use UPSs (Uninterruptible Power Supply) on critical computers and network equipment.

10. Maintain as few applications on computers as possible. The risk of conflicts, errors, and crashes sig-nificantly increases with every new program installed.