

A Dozen Recommendations for Your Organization

1. Plan to retire older computers

The life of a workstation is about 4 years, but for laptops it's only 3 years. Plan to retire 20% of your assets yearly if possible.

2. Standardize on an operating system for Workstations and Servers

Workstations and Servers should be installed with or upgraded to a current (and supported) operating system, and patched to the most recent service pack.

3. Choose an appropriate Network Environment

Offices with 5-9 workstations can enable a peer-to-peer network, but organizations with 10 or more computers will need to install and configure at least one server.

4. Choose the right Internet Broadband Connection

Organizations need a dependable Internet Service Provider (ISP). Depending on needs, smaller offices should aim for a 7-12 Mbps download speed, larger offices may need to go with 50 Mbps.

5. Install a hardware-based Firewall, don't depend on just software

If your employees connect to the Internet when they logon (a persistent connection) you probably need a hardware firewall in place to protect from unauthorized users gaining access. Unlike software firewalls, it cannot be turned off by malware, and it doesn't use any workstation processor or memory resources.

6. Secure your wireless Networks

All networks (peer-to-peer or client/server) using a WLAN (wireless network) need security implemented to limit access. Don't allow wireless connections from guests or clients without first establishing security.

7. Plan to Back Up and Recover

All organizations, regardless of size, need an installed, configured, tested and maintained back up system, for restoring files, folders, drives that are deleted or lost. Additionally, imaging a typical workstation and your servers provides the easiest way to recover from total failure.

8. Stop Email Spam

Email (webmail or installed/Outlook) has to be protected against viruses and phishing attacks. From training employees how to mark email as spam, to protecting your in-house Exchange server, to budgeting for a service, every organization has to decide how to deal with spam and phishing emails.

9. Secure the Browsers

Developing a policy of what employees can and cannot do at work is your first step to creating a more secure browsing environment. Workstation computers and laptops should be installed with a current and standardized browser software, and maintained to protect against pop-ups and malware.

10. Create strong password policies

Secure organizations enforce strong password policies. (6-14 char, one capital, one number, one symbol). Don't allow employees to be admins on their own computers, don't make everyone a domain admin by mistake.

11. Documentation

Use software to create detailed inventory reports about each computer and server on your network, which are invaluable for planning, budgeting and recovery operations.

