

Best practise for small business networks.

Small business networks allow you to share files, printers, the internet and e-mail with all client computers on your network. The addition of VPN (virtual private network) or RAS (remote access services) will allow you, or anybody with suitable permission, to access the network from anywhere in the world. Whilst all of these are very useful features, they all carry inherent dangers, which if you follow these guidelines, will be minimised. Problems fall into four categories.

Security

Having shared your files with the world it is vital to control who can access them. "In house" - this is the most vulnerable area. Make sure that all your client computers are password protected and can only access files that you want that user to see. Test this regularly by going to a workstation and making sure that you cannot access sensitive data that you would not want available to everyone. For example, I have seen a case where a workstation was placed in a workshop area and used mainly for invoicing. A bored sixteen year old work experience lad was able to access and modify the accounts data and cause the company serious problems.

Make sure that your server is secure, preferably in a locked room. If I could have unfettered access to your server for five minutes I could find your password and give myself permission to modify anything,

The most important security issue deals with disgruntled former employees. If you feel a working relationship is breaking down, then it is vital to change not only the employee's password, but any other passwords that they may know. In fact it is good practise to change all passwords at least once a month. On the subject of passwords, they should be at least eight characters long and contain at least one number, this combination is the most difficult to "hack".

Keep your server and workstations up to date. Microsoft regularly brings out updates that repair security flaws within the operating system. This however, can be a double edged sword as it advertises to the world what those flaws are and whilst initially only a few might be aware of them, once the upgrade is released, it is common knowledge. If you haven't implemented the updates then you are vulnerable to that security flaw.

In these days of portable storage, it is easy to back-up your data on to CDs DVDs and particularly data sticks. Great care must be taken with these back-ups, as if you have all your data backed up on one of these, and put it on your key ring or in your pocket, it contains all your company data and can be easily lost or stolen. Treat it as you would your wallet!

The Internet

Firewalls and good password security will protect you from hacking. But by far the biggest danger to your network is from undesirable material being allowed in, either by e-mail floppy disc /CD, or by being downloaded from various sites on the internet. The best way to protect yourself from these dangers is to have an IT policy pointing out what is, and what is not acceptable use of the business network and to get your employees to sign it. Below is a list of practices which should not be allowed.

- 1: Opening of “unexpected “e-mail attachments. Even “expected” attachments, or those from a reliable source, should be treated with caution. Never open an executable file.
- 2: Bringing material in from outside on floppy disc CD or data stick etc. If it must be done then the material should be scanned by an anti-virus programme before it is allowed onto the network.
- 3: Installing any programmes onto any work-stations without permission.
- 4: Using peer to peer music sharing software. This is not only illegal but it is also an open door for malicious software.
- 5: Visiting any sites that may contain illegal and offensive material. (Yes, I do mean pornography!) Even if you dismiss the person responsible, the computer crime unit of the police could seize all your hard drives and take up to six months to investigate them.
- 6: Downloading anything without permission.

Anti-virus

Anti-virus software is only any good if it is regularly updated. If someone produces a new virus that your software is unaware of, it will go straight through the software and infect your network. There is normally an annual fee charged for anti-virus so make sure that your software is both valid and up-to-date I would recommend you use software that automatically updates itself once a day. Anti-virus software must be installed on every machine on your network, especially the server.

The best way to avoid spy-ware, which can dramatically slow down your network, is to stay off the internet, but as we all use the internet for a variety of worthy purposes every day, it is impossible to avoid. Use a good spy-ware scanner to clean up machines on a regular basis but beware some of them can cause more problems than they cure. We recommend Adware and Microsoft anti-spy ware as we have tested them and they work. Free copies are available from the internet or from us.

Back-up

This is the area that most companies fall down on; it is not good enough to have a tape back-up churning away every night. You must be able to demonstrate that if the worst happens you can quickly restore your data and get the company operating again.

I would suggest two different types of back-up, with one of them being stored away from the premises. It is also important to keep at least two weeks worth of back-ups in case of slow acting virus infection. Below is a list of possible back-up methods for you to consider. It is also a good idea to keep permanent back-ups every few weeks and also store them away from the premises.

- 1: Tape.
- 2: CD/DVD.
- 3: Memory stick.
- 4: Removable hard drive.
- 5: Off-site data storage.

Disaster recovery- have a plan! Think of all the possible things that could go wrong and how you would deal with them. What would you do if your server room caught fire or was flooded? What would happen if your IT administrator (God forbid) was run over by a bus? Are all the passwords stored in a fire proof safe, or with your solicitor? It is important to have a strategy to deal with all these possibilities.

Finally set up a good house-keeping policy.

Weekly: - Run full anti-virus and anti-spy ware scans; delete all read e-mails that you do not want to keep, not forgetting to empty the deleted items folder.

Monthly: - Delete all temporary files including internet files using the disc clean-up utility. (My computer right click the c: drive select properties and press the disc clean-up button.)

Run a disc defrag (All Programmes/ Accessories/ System tools / disc defragmenter. Check with windows update www.windowsupdate.com that your machine is up to date.

This should be applied to all machines on the network.

Useful shortcuts

Ctrl+C Copy

Ctrl+V Paste

Ctrl+X Cut

Cntrl+Z Undo

Windows key plus D minimises all open windows back to the desktop.

Windows key plus L logs the user off windows.

Copy write 2005 Ian Muxworthy I.R.G. Computers Ltd.