

Biztech Newsletter

Autumn Edition

24th April 2007
Volume 1, Issue 7



Backup+ Service Is Now Available

Inside this issue:

- Backup+ Service Is Now Available 1
- Home Backup 1
- Feature Product 2
- Protect Yourself Against Malware 2
- Spam, Spam, Spam 2

With systems now commissioned and online, the Backup+ service is now available to all support-Pak clients.

- What is it? - The service provides secure off-site automatic data backups from anywhere in the world. Designed to safeguard valuable client data from loss or accidental erasure, it will maintain offsite point in time backups for as long as you desire.
- How does it work? - A small program is installed to your main system or notebook that carries out scheduled backups of your data to a secure server located in Canberra.
- Is the data secure? - Yes, the data is encrypted automatically at your end and cannot be read by anyone including ourselves.
- How much data can it store? - 5 Gigabytes is available to all clients with a current support arrangement. Additional storage is available outside of our SupportPaks at a competitive price.

- What does it cost? - There is no additional charge for supported clients only the support time to install the program and an additional five minutes per week during your remote maintenance checkup session.
- Who is it best suited to? - The service is suited to small networks where the total data, office documents, databases, accounting systems and even pictures number less than two to three thousand. It is ideal for users who are mobile and have data stored on notebook computers and all our dental clients for the backup of the Oasis practice management system.
- How do I get it? - Contact us at our office and arrange a time for it to be installed on your system.

Home Backup

Have you considered how much of an impact it would be if your home computer stopped working and the data could not be recovered? Have you backed up your family photos, emails and other documents? These days it is easier for people at home to have their computers covered in the advent of a hardware failure causing data loss. External hard drives connected through USB can provide an easy way to keep those family pictures and other files backed up and accessible in the advent of a failure. Many companies are now

releasing products aimed at home users, for example Seagate now have enclosures that can be connected to your computer that can have upwards of 200



Gigabytes of data storage. Couple this with inbuilt backup programs within Windows XP and 2000 and it can be made into an effective backup solution for home.

More information about external storage products can be found on the Seagate website.

www.seagate.com

Feature Product

Protect Yourself Against Malware

\$1150ex**HP Compaq Business Desktop dx5150
+ 19" HP Monitor + 512MB Key**

MT ATH64 3500 + 2.2 GHz
1GB (installed)/ 4GB (max)
160GB HDD
DVDRW, XXP, 1 yr warranty

PN: F550PA-HP19

Valid until 15th May 2007 or until stocks last

For more special and product information
please call the sales team on (02) 6280-6998

Malware can be split into viruses and trojans. Viruses are capable of transitive self-replication which is a fancy way of saying that they are able to spread from computer to computer via E-mail or other file transfer mechanisms.

Once on your computer, many malware items are able to communicate with the outside world, some are designed to steal information such as your login key strokes, banking and credit card pin codes, email address lists and the identity of web sites you may have visited.

Besides having the ability to spread, many viruses are built to harm your systems. Some are capable of destroying computer hardware such as hard disks, motherboards or any computer peripherals.

With the simultaneous increase both in the rate at which new Malware appears and the sophistication of the programs, it is increasingly difficult for security professionals and IT departments to keep systems protected.

Most of the time these malicious programs succeed not through some advanced hacking mechanism, but simply by persuading the user to do something. Reply to an E-mail,

click on a link, download a program or go to a particular web site.

So what can we do to help prevent Malware from infecting our systems.

- If an e-mail sounds too good to be true, it almost certainly is. The best actions to take are don't try, don't buy and don't reply.
- Avoid software, or even links to software, sent by e-mail. Always use the internet to find out for yourself what others are saying about it before using it. Enter your own link address to download it and check for digital signatures if you can.
- Don't be tricked by e-mails just because they appear to come from people you know. Spammers and Phishers know how to disguise the real sender.
- Don't be tricked by correspondence which seems legitimate because it happens to match with your own interests.

If you are still in doubt, ask an expert for analysis on suspicious email or a programme. Your business will often be more at risk from your haste than realistic delays.

Buy a SupportPak and SAVE

50% discount on telephone support
40% discount on remote support

Spam, Spam, Spam

In this day and age when you mention SPAM most people think of annoying unwanted emails rather than something you put in a sandwich. You might have noticed that you're getting more spam now days. Have you ever noticed that despite spam filtering, people seem to be getting spam that isn't even addressed to them? Well the source of this spam is quite possibly from dictionary attacks, it's also known as dictionary spam. So you be asking what is dictionary spam and why am I getting it? Basically dictionary spammers get their spam to you by using every name out there in various combinations, for example, johnsmith@domain.com, jsmith@domain.com, john.smith@domain.com johns@domain.com and so on and so forth. Eventually they'll get your address right and the spam will get to you. As for the spam getting to your inbox without even having your email address listed, in the 'To:' header it seems that only a few addresses are listed here and the rest are 'undisclosed recipients'. So, if your email address doesn't appear in the 'To:' list then it's likely to be in amongst the 'undisclosed recipients'.

Most Internet service providers and well known domains such as hotmail.com and yahoo.com are prone to such attacks. Also you need to be careful if you reply to one of these dictionary spam messages or worse still, actually buy a 'product' from one of them, because if you do you'll probably get a lot more spam.

It's quite easy to identify dictionary attacks as you can usually see a number of other addresses in 'To:' list that have myriad of addresses with the same domain name as yours. It can be hard for ISP's to block this kind of attack as they have to cater for a great deal of users and deal with huge volumes of traffic. The problem they face is that if they tighten up their filtering some legitimate emails may no longer be delivered.

You might be asking, what could be done to reduce the amount of spam you receive yourself. Outlook has configurable junk folder which can filter out quite a large portion of your spam. Another alternative is to purchase a spam filter. Computer Associates Internet Security Suite has one as does PC-cillin Internet Security 2007. If you're running your own mail server then you might consider Computer Associates Secure Content Manager.