



## HOW TO PREVENT A DISASTER STRIKING

**A new virus has disrupted Google, Yahoo and other leading search engines as it tried to spread itself by repeatedly performing automated queries for additional email addresses.**

Those simultaneous searches from thousands of infected computers worldwide taxed the search engines and slowed service for many legitimate internet users.

The latest virus is a variant of MyDoom, which first appeared in January. Craig Dennis, CEO of Australian Project consulting Services warns that “companies that do not take precautions can have downtime that goes for days, and it’s not unusual for a series of smaller problems to pop up in the weeks and months following the disastrous infection.”

If a company has 300 PCs in it's fleet and finds that it is infected, the responsible approach is to disconnect from the Internet (and lose email connectivity) and shut down every machine on the network. Each machine should then be treated in isolation and you can only re-activate your internal local area network (LAN) when all machines have been cleaned. One rogue PC on the network may cause a re-infection.

The alternative is to ensure that a high level of IT Governance is implemented. This includes technology responses such as at least two layers of virus/worm protection, including server based email scanning and an effective firewall. These systems must be maintained on a daily, or preferably, hourly basis. (This should happen automatically via a subscription service).

“This should extend to policies and procedures. Staff need to know what they are allowed to do on the system, and, perhaps more importantly, what they are not allowed to do,” says Dennis

### **Dennis offers the following examples;**

1. Don't share a floppy disk, CD-R or USB data key with your home PC unless it has been virus scanned on a standalone office PC. (Students sharing data on school PCs is a major issue.)
2. Don't open an email attachment unless it is from an absolutely trusted source.
3. Don't view graphics embedded in email unless they are from an absolutely trusted source.
4. Don't reply to unsolicited email.
5. Don't submit your work email address to a website unless there is a clear business requirement to do so.

**Media contact: Jennifer Muir**  
**T: 61 2 9818 1388 M: 0415 401 200 E: [Jennifer@juicegroup.com.au](mailto:Jennifer@juicegroup.com.au)**





IT user policies should be formally codified and circulated to all staff without exception. Ideally, everyone should acknowledge and sign the policy before being granted access to the system. Staff should be required to review and re-sign the document at least annually to ensure that familiarity is maintained, and that any changes are accurately communicated. They should also be made aware of the penalties in the event that they misuse/abuse the systems that they have been entrusted with.

“There is a cost involved with implementing robust security technologies, however this should be seen in much the same way as an insurance policy - an unavoidable cost of doing business. The alternative is the ever increasing risk of a virus attack and the potentially catastrophic effects in terms of your customer's perception and significant damage to the business' bottom line.”

**-ends-**

**Media contact: Jennifer Muir**  
**T: 61 2 9818 1388 M: 0415 401 200 E: [Jennifer@juicegroup.com.au](mailto:Jennifer@juicegroup.com.au)**

