

## VIRUS ALERTS

During the past week there have been two very serious computer viruses, which have choked the Internet and brought down many computer systems. The essential points are summarised on this Business Watch Alert in case any members are having problems or need to remind staff of the golden rules of virus protection.

### 1. Blaster Worm-virus

The following Microsoft Windows versions are vulnerable to infection by this worm:

**Windows 2000, XP, NT4.0, Server 2003**

Windows 95, 98, ME and 3.x are not vulnerable to this virus.

The most common symptom is error messages that state the system is shutting down automatically. Other symptoms include system instability and crashes. This virus does not spread by e-mail, but it looks for Internet ports that have not been patched by the latest Microsoft updates.

**Visit the following web site for further information on this virus:**

Microsoft: [http://www.microsoft.com/security/security\\_bulletins/ms03-026.asp](http://www.microsoft.com/security/security_bulletins/ms03-026.asp)

Or <http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp>

**More information and removal tools are available from the following Anti-Virus web sites:**

Symantec: <http://www.sarc.com/avcenter/venc/data/w32.blaster.worm.html>

McAfee: [http://us.mcafee.com/virusInfo/default.asp?id=description&virus\\_k=100547](http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=100547)

Computer Associates: <http://www3.ca.com/virusinfo/virus.aspx?ID=36265>

Trend Micro: [http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?Vname=WORM\\_MSBLAST.A](http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?Vname=WORM_MSBLAST.A)

We have further information on removal tools and detailed instructions if you wish to undertake a rescue process.

### 2. Sobig Virus

**This virus affects all Windows operating systems except the old 3.x series.**

This new virus was discovered on 19<sup>th</sup> August and is a mass-mailing worm that sends itself to all the e-mail addresses it finds in computer address books, web sites and text files.

The characteristics of this virus, which can be readily identified, are attached file name extension PIF coupled with a very short text message, such as "See the attached file for details". Typical attached file names include:

your\_document.pif; document\_all.pif; thank\_you.pif; your\_details.pif; details.pif; document\_9446.pif; application.pif; wicket\_scr.scr; movie0045.pif.

Subject headings that have been noted to-date include:

Re: Details; Re: Approved; Re: Re: My details; Re: Thank you!; Re: That movie;  
Re: Wicked screensaver; Re: Your application

E-mails with this virus appear to come from unknown senders in a variety of countries, particularly Finland. Sometimes there is an automatic receipt message generated, which in turn produces a further error message back to your computer.

A removal tool is available from: <http://www.sarc.com/avcenter/vinfodb.html?prodid=nav2002>

### 3. Golden Rules

These two virus infections highlight the importance of the following golden rules for operating any computers with connections to the Internet:

- 3.1 Ensure automatic live update of your Anti-Virus software
- 3.2 Ensure regular weekly scanning of all files using the latest virus definitions
- 3.3 Configure your e-mail server to block or remove e-mails that contain file attachments that are commonly used to spread viruses, such as .bat, .exe, .pif, .scr, and .vbs file extensions.
- 3.4 Train employees not to open attachments unless they are expecting them from a known sender.
- 3.5 Do not execute software that is downloaded from the Internet unless it has been scanned for viruses.
- 3.6 Do not accept e-mail invitations to click on a link to a web site that is unknown. This is the latest way in which viruses are being spread.

*BusinessWatch Security Alert compiled by Brian L Dunsby and Maggie Hall with acknowledgements to Microsoft, ntlworld and Symantec.*