



"Worms" & "Con-tricks" Update

1. E-mail Viruses & Worms

MyDoom, SoBig, Blaster, Melissa, Iloveyou ... Microsoft say these strange sounding names represent one of the biggest threats to modern business - the computer virus. The MyDoom virus spread faster than any other virus in history; with computers more connected than ever before, the risk to business is growing.

The **MyDoom.A** and **MyDoom.B** worm variants have been spreading rapidly through e-mail messages. They attempt to entice e-mail recipients into opening a file attachment, most commonly those with a .zip file name extension. If the attached file is opened, the worm installs malicious code on the computer user's system and sends copies of itself to all contacts in the user's address book. Both versions of the worm leave a file on the infected machine that can potentially allow a malicious individual to access that machine. Mydoom.B also reportedly blocks access to some web sites, including Microsoft.com and some anti-virus vendors' web sites.

The latest is **Netsky.B** which is a mass-mailing internet worm that arrives with a varied subject, message and attached file containing the "worm". It attempts to spread itself through both e-mail and file sharing folders.

Systems affected are: Windows 2000, Windows 95, Windows 98, Windows NT and Windows XP.

Systems **not** affected are: Linux, Macintosh, UNIX and Windows 3.x

The "worm" is spread through incoming short e-mails with the subject usually one of the following: **approved; document; fake; greet the day; hello; here; hi; information; my details; read it immediately; something for you; stolen; thanks; the summary; unknown; warning; word file; your archive; your bill; your document; your letter; your music.**

The message is usually very short, up to five words, that might tempt you to open the attached file. The files attached to these e-mails will end in one of the following extensions: **.com .exe .pif .scr .zip**

DO NOT OPEN - DELETE ALL SUCH UNRECOGNISED FILES IMMEDIATELY!

Symantec recommend you take the following steps to avoid becoming infected by this "worm":-

- Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files.
- Isolate infected computers quickly to prevent further compromising your organization. Perform a forensic analysis and restore the computers using trusted media.
- Train employees not to open any attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

If you have been caught look at your anti-virus software supplier's website for example: www.symantec.com They provide a free downloadable removal tool with full instructions.

To get advice on e-mail viruses go to: www.myantivirusfinder.com

WARNING: One Chamber member had opened the attached file before realising the problem and was hit with 12,652 e-mails in just half a day. Their whole system was soon choked and unable to operate. They had to shut-down and clean out using the special removal tool.

BUSINESS WATCH - Security Alert No 12 - page 2

2. Internet Name Scam

Businesses throughout the region are receiving calls from various companies offering to sell them domain names. The domain name is usually your company's name if you do not have a website or the .com or .co.uk suffix, depending upon which one you already own.

The caller states that he has another prospective purchaser on the line for this domain name and is calling you out of courtesy first so he needs a quick decision from you. The costs charged will normally be considerably more than if you or your existing hosting company registered the domain name.

Trading Standards officials advise businesses that they can obtain a similar service themselves for approximately £50 merely by registering the additional domain names. Details of how to do this would normally be obtainable from your Internet service provider and guidance can be obtained from the UK Internet governing body www.nominet.org.uk.

Please call North Yorkshire Trading Standards on 01609 768606 or you can fax documents to 01609 768649, if you are contacted by one of these rogue domain sales companies.

3. Bogus "Microsoft" Security Updates

Beware of Bogus Bulletins - If you receive an e-mail message that claims to contain a **Microsoft software update**, it is probably a virus trying to trick you into infecting your computer. Microsoft never widely distributes software in e-mail. To learn how to spot a bogus bulletin click on:

http://www.microsoft.com/security/antivirus/authenticate_mail.asp

We received one of these on 03/02/04 which even carries the Microsoft name and a variation on their logo. The text was as follows:

"This is the latest version of security update, the "February 2004, Cumulative Patch" update which fixes all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express as well as three newly discovered vulnerabilities, the most serious of which could allow an attacker to run executable on your system. This update includes the functionality of all previously released patches." **DO NOT CLICK ON ANY OF THESE LINKS!!**

4. Mobile Phone Call Back Scam

The latest scam plaguing mobile phones is costing a fortune. Ringing back a missed call that shows the number 0709 020 3840 will cost mobile phone users £50 per minute. The last four numbers may vary, but the first four numbers stay the same. This is perfectly legal, and mobile phone users should remain vigilant. Most phone users will not realise that they have been scammed until they receive their bill.

The Independent Committee for the Supervision of Standards of Telephone Information Services (ICSTIS) controls premium rate numbers. To visit its website, go to: <http://www.icstis.org.uk>

5. Advertising Sales Calls

North Yorkshire Trading Standards received a complaint from a photographer in Scarborough who was approached by someone who claimed to be calling on behalf of the Council. He did not state which council. Eventually, in response to questioning, he admitted that he was calling from an advertising agency in Lancashire. Similar problems have been featured on BBC TV's "Watchdog".

Local Authorities will, on occasion recruit outside businesses to carry out work, but they will always make it clear which council they represent. If in any doubt ask and they will tell you. Publications aimed at local schools are a "soft touch" so insist on samples and evidence of satisfactory distribution before agreeing to pay for advertising in such books.

If you need further advice please contact Trading Standards on the details below.

North Yorkshire Trading Standards

Tel: 01609 768600

Fax: 01609 768649

E-mail: trading.standards@northyorks.gov.uk

Harrogate Chamber of Trade & Commerce

PO Box 8, Harrogate, HG2 8XB Tel: 01423 879208 Fax: 01423 870025

e-mail: info@harrogatechamber.org web site: www.harrogatechamber.org