



Order product brochures on-line now!

Auto ID RFID    Printing Labeling    POS Technology    Doc Mgmt.

[click here](#)

[All brochures are complimentary](#)

**TOOLS**

- [Home](#)
- [Brochure Request](#)
- [Links Directory](#)
- [Newsletters](#)
- [RSS Feeds](#)
- [Advertise](#)
- [Digital Edition](#)
- [Help](#)
- [About Us](#)
- [Contact Us](#)

**TECHNOLOGY CHANNELS**

- [Channel News](#)
- [Channel Talk](#)
- [Data Capture](#)
- [Mobile Computing](#)
- [Print & Label](#)
- [Retail Technology](#)
- [Document Mgmt](#)
- [Networking](#)
- [Internet Security](#)
- [Data Storage](#)
- [Power/UPS](#)
- [Audio/Visual](#)
- [Events](#)
- [Personal Dev.](#)
- [Video](#)
- [Recruitment](#)

**VERTICAL CHANNELS**

## Internet Security

Internet control, email and network protection

### Weekly report on viruses and intruders

18 September 2006 MicroWorld

[EMAIL ARTICLE](#)    [PRINT ARTICLE](#)

#### Olympic Torch Hoax Burns a Hole in Productivity, Again

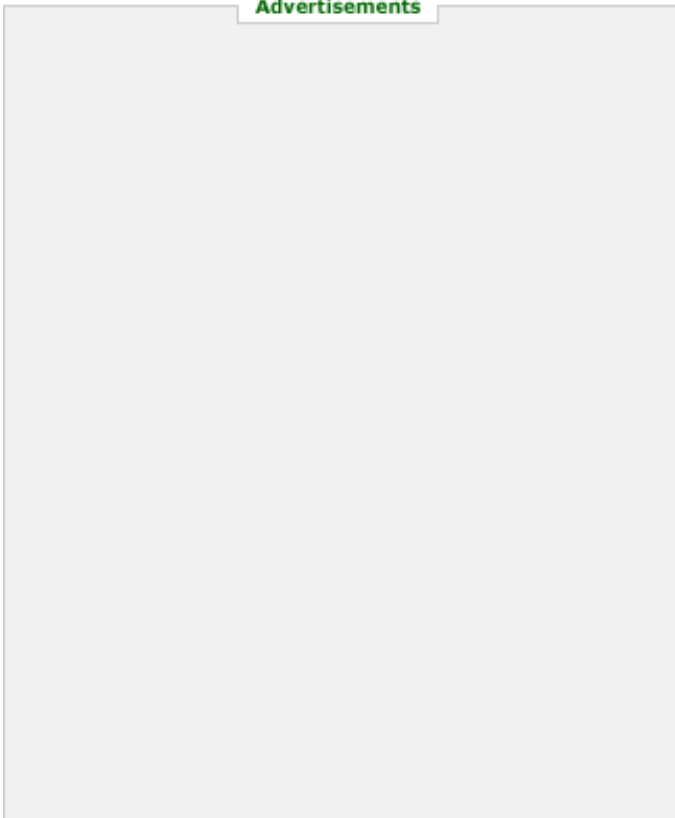
The Olympic Torch Virus Hoax is back in circulation in a big way. This time it's seen doing rounds predominantly among Orkut Online Community members, informs Security Analysts at MicroWorld Technologies.

The hoax mail that appeared for the first time in the second week of February 2006, says you should never open an email with an attachment named "Invitation", regardless who sends it to you. Like a typical scare monger it screams that the Virus will burn the whole hard disk of your PC! In the pretext of educating you about its spreading routine, the hoax goes onto explaining how the entries in the address book of a victim are stolen and how the Virus starts mass mailing to those email addresses.

To lend some fabricated credibility to the hoax, the email quotes CNN, Microsoft and Security firms. The message ends with a strong plea to forward it to as many people as possible so that the humanity shall save their computer hard disks from massive destruction.

"The psychology behind hoax mails is an intriguing subject to delve into. For many, it's just the curiosity to see how fast and far these false mails travel, while they derive some sadistic pleasure watching its geometrical progression. Some other chain mails are fraudulent, money-making tricks in the form of Ponzi Schemes and Multi-Level Marketing, where they just act as invitations to bigger troubles. And then there are absolutely malicious ones spreading false and harmful information among their recipients as well," analyzes Sulabh Mahant, Security Expert at MicroWorld Technologies.

**Advertisements**



**Related Articles**

None

[POS/hospitality](#)  
[Logistics](#)  
[Field Service](#)  
[Education](#)  
[Healthcare](#)  
[Manufacturing](#)  
[Office Automation](#)

## MAGAZINE

[Editor](#)  
[Subscribe](#)  
[Media Kit](#)  
[Feedback](#)  
[Digital Edition](#)

There is a real, tangible cost to hoax mails. It will dent your Collective Productivity, occupy large Server spaces, choke bandwidth, clog mailboxes with unwanted stuff and spread totally misleading information in business communities. In year 2001, a false alarm was raised by a hoax mail saying that a Windows Utility file named 'sulfnbk.exe' with a funny looking icon, was a Virus and got countless victims to delete that useful OS component from their computers. If you see, the harm it did was no less than a Virus!

"Regular technologies used in Spam fighting like Real-time Black List, Reverse DNS or Gray Listing, will fall flat in front of hoax mails as here the sender is someone you know. Your spam fighting system should be smart enough to learn and apply an acquired Intelligence to spot and stop these mails from entering mail boxes. That's where our unique and patent pending technology called Non-Intrusive learning Patterns (NILP) succeeds in filtering Mail Traffic using a combination of Self-learning Capability and continuously updated, research based feeds from MicroWorld Server," points out Govind Rammurthy, CEO, MicroWorld Technologies.

### Other Internet Security News

#### [Report Reveals 'Safe Surfing' Britain](#)

British citizens are fighting back against the threat of viruses and spyware channelled through the internet according to a new survey from the British Computer Society (BCS).

#### [Internet Security Systems Appoints Two New Members to its Northern Europe Management Team](#)

Internet Security Systems (ISS), the worldwide leader in pre-emptive, enterprise security, today announced the appointment of Andrew Lawton and Bridget Charles as part its Northern European Management Team.



#### [Netintelligence Gains the Highest Trust of Customers Worldwide](#)

Info Security Products Guide names Netintelligence Enterprise Manager Winner of the 2006 Global Excellence in End Point Security Award

### Security White Papers

#### [CONTENT FILTERING SOLUTIONS TECHNOLOGY REPORT APRIL 2006](#)

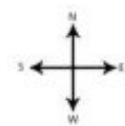
Source: West Coast Labs/Netintelligence



#### [The Trend of Threats Today: 2005 Annual Roundup and 2006 Forecast](#)

*Trend Micro*

The report that follows is not only an account and analysis of 2005 threat incidents. It also serves as a forecast of what the future holds in 2006 and onwards. Through Trend Micro's extensive research and analysis of the 2005 incidents, this paper documents how threats evolved into the multi-purpose threat regime – thus providing corporate and home users information on what to do to ensure they remain protected against future threats. Download free white paper.

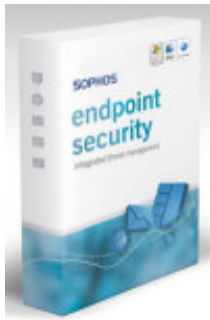


#### [If you can't beat it, manage it](#)

Rob Nash, director of eBusiness at Unipalm, looks at the challenges facing IT managers with the growing use of Instant Messaging in the workplace.

#### [How to keep spam off your network](#)

#### [The corporate threat posed by email Trojans](#)



**CHANNEL WELCOMES  
SOPHOS'S NEW  
INTEGRATED SECURITY  
OFFERING**

Sophos Endpoint Security simplifies management of intrusion, adware, malware and spyware protection from one console

**SAN Management in Secure Environments**

*Decru*

SAN security is a growing concern for enterprise and government alike. Recent innovations in technology have delivered significant improvements in vendor interoperability, software functionality, supported distance (switch-switch and switch to storage), availability and scalability. However, whilst all of these improvements have sped the adoption of SANs, they have been at the expense of security.

[More >>](#)

**Secure Computing's Sidewinder G2 Security Appliance Cryptographic Module for SecureOS Achieves FIPS 140-2 Validation**

The Sidewinder G2 Security Appliance is a comprehensive unified threat management (UTM) gateway security appliance. It comprises a wide variety of Internet security functions...

**Websense Boosts Channel Training Programme**

New accreditation programme builds on current success and creates new revenue opportunities for the channel.

[More >>](#)