

IT Backbones - itbvirus.com



Give your mouse a heart!

search 

itbvirus.com

- [Home](#)
- [About](#)
- [Contact](#)
- [Submit PR](#)
- [Search News](#)
- [What We Can Offer You](#)
- [IT Events](#)
- [Time & Money](#)

Olympic Torch Hoax Burns A Hole In Productivity, Again

Published 14th September 2006

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.

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.

Company Profiles powered by ITReseller.com

- MicroWorld - [View profile](#)

[Links](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#) | © 2004-2006 IT Backbones Limited

Site developed and hosted by [Design Solution](#) Ltd.