

Article from Financial Express - 22nd Sept 2008

<http://www.financialexpress.com/news/security-begins-at-home/364200/0>

## Security begins at home

**Indranil Chakraborty**

Posted: Sep 22, 2008 at 0039 hrs IST

Updated: Sep 22, 2008 at 0039 hrs IST

Mumbai-Based Madhuparna enjoyed connecting with her friends at social networking sites, till an email in her inbox warned her that the sender had her obscene pictures in his possession. He threatened to post the pictures on the internet, unless she met him.

She promptly lodged a complaint to the local police. The police team started tracking the IP address of the sender and discovered that it belonged to a company. Finally, the PC and its user were tracked through network monitoring logs. The preliminary investigation suggested that the user, by using multimedia software and tools, had created Madhuparna's titillating photographs.

Madhuparna can consider herself lucky. Bigger dangers lurk online. Terror mails sent after Delhi as well as Ahmedabad blasts are believed to have come from hacked Wi-Fi networks. Few users bother to secure or even password-protect their WiFi accounts, leaving it open for anyone in the radius of about 100-200 metre to get in easily. For terrorists, this is far safer than trying to go to a cyber cafe, where they would be asked for identification. Personal financial data could also be hacked. Hackers are also reported to have stolen personal data worth \$5 billion of up to eight million guests at over 4,000 hotels in 80 countries, belonging to the Best Western Hotel consortium.

Today, it is not tough to break into an unsecured network as the software to break into wireless internet is freely available on the internet and even pre-installed devices are available. The Wi-Fi market is estimated to touch \$900 million in about three years.

With terrorists, hackers and ever-increasing viruses on the prowl, the security equation is changing fast. Till recently, the task of creating firewalls to stop intrusion was limited to corporate networks and security for endpoints—desktops—began and ended with loading anti-virus, and receiving patches. Today, the IT security companies like Symantec and Check Point feel that there are more things to do to prevent intrusion at home computers and personal laptops.

Not long ago, the corporate network was the only focus of security. The anti-virus product was practically the only security device available. Now as PCs and laptops are becoming a part of the Web, securities like data protection through encryption technology, safe-boot password, port protection, program controlling network access points are slowly becoming a must for a PC and a laptop. Security issues have become individual-centric rather than organisation-centric.

The growth in home market could overtake the corporate sector in future. **“As more and more PCs acquire broadband connections, homes are becoming vulnerable to intrusion and security issues will be one of the main concerns. And people are no more satisfied with just antivirus package, but the demand for a total security solution is growing,”**

**says Prateek Agrawal**, a certified expert on information security and **director of Ivy professional school**.

“Portable devices like laptops, smartphones and personal digital assistants (PDAs) are increasing with each passing day. One carries most of his/her information in these devices. It is frightening to think if one has to lose his portable device, then the amount of money and sensitive information he would lose,” agrees Vishal Dhupar, managing director, Symantec India. With consumer behaviour shifting from a PC-centric to a Web-centric nature, the Web is also quickly becoming the distribution point for malicious code and attacks, he adds.

“Growth in the consumer segment will be dramatic. Nine out of 10 home PCs are used for official jobs. Rather than technology, the usage pattern would drive consumers to have a better security solutions in place against unauthorised hacking,” says Raghu Raman, chief executive officer of Mahindra Special Group.

There are many ways in which the security companies as well as the internet companies are trying to convince the home users about the need for a secured environment. The first step is awareness. Google, for one, is conducting a campaign to teach young students how to be a safe surfer. “We decided to start a campaign to help students know how to avoid misuse of the internet and inculcate in them the best cyber practices,” says Rishi S Jaitly, policy analyst, Google India. He is participating in an awareness campaign called BeNetSmart to educate school students about the potential hazards of cyber crime, being jointly conducted by the police and Internet and Mobile Association.

The tips given to students include—never give out personal information like name, phone number, passwords or birth date, online to anyone whom they do not know. Google advises the students that they should never answer mails or chat with people whom they do not know; make sure that the names included in the contact list are all known to the user; not to meet anyone acquainted through the internet without an elder’s presence. Further, they should never fill out any questionnaires forwarded to them, even if they come from friends.

All these messages for better security are fine. But will Google stop at an awareness campaign or launch security products for the desktop, which can be downloaded straight from the internet like its spreadsheet and word processor? Jaitly says that though Google does not have any plans but if there is a need, the company may think it over. Cyber security analysts feel that the next step would be for Google to play a major role in preventing cyber crime by launching its own desktop security software to prevent misuse of its own social networking site Orkut and video sharing site, YouTube.

Raghu Raman feels that Google would be happy if it succeeds to convince the consumers that the desktops are inherently insecure and thus, one should keep all documents in the Google server. It may not happen today because of the bandwidth issue, but the concept of thin client will be there in the next few years. **Prateek Agrawal believes that not only Google, but many of the software players will have software as a service model for the consumer segment. “The home market is growing. As more and more consumers connect to the internet, the demand for a total security solution is growing. People are not satisfied with just an anti-virus package.”** says **Agrawal**.

“As more PCs and notebooks are being exposed to the internet, consumers are prone to attacks by the intruders and cyber crimes like hacking, phishing and spamming are increasing,” says KPMG India forensic services head Deepankar Sanwalka. “One of the most common practices of the spammers is to send anonymous emails with malicious codes. Once

the mail is opened, the scripts start sending information like mail addresses in the address book back to the spammer,” says Sanwalka.

Though home and personal security market is still nascent, security firms seem bullish as the consumer segment accounts for over 35% of total PC sales. Estimates from IDC peg the Indian security market, including products and services at Rs 1,416 crore in 2007-08, compared to Rs 999 crore in 2006-07. IDC India estimates the security content management market at \$ 61.2 million and predicts the market to grow at a CAGR of 28% over the next five years.

“The rise in internet connectivity in the home segment, proliferation of social networking, video sharing and chat sites, are all exposing the home market to cyber crime. The sale of security products for the desktops and personal mobile devices will be sizeable in the future,” says CheckPoint Software country manager, India and Saarc, Bhaskar B