

## Sections

- Top Stories
- National
- International
- Regional
- Business
- Sport
- Sci. & Tech.
- Entertainment
- Agri. & Commodities
- Health
  
- Index
- Photo Gallery

## The Hindu Print Edition

- Front Page
- National
- Tamil Nadu
- Andhra Pradesh
- Karnataka
- Kerala
- Delhi
- Other States
- International
- Opinion
- Business
- Sport
- Miscellaneous
- Index
  
- Magazine
- Literary Review
- Metro Plus
- Business
- Education Plus
- Open Page
- Book Review
- SciTech
- NXg
- Entertainment
- Cinema Plus
- Young World
- Property Plus
- Quest

## Sci. & Tech.

### Phishers start angling for Facebook, Twitter

New Delhi (IANS): Twitterers and users of Facebook, beware!

For hackers have now begun targeting popular social networking sites, and chances are that the sites' members maybe hoodwinked into revealing their identities and, worse, even credit card details, warn experts.

Last week, hackers twice attacked Facebook — arguably the world's most popular social networking site — causing a host of users to reveal their personal information.

The hoax cleverly duplicated the site's messaging service to send messages to the users. Those gullible enough to click on the link were transported to a look-alike log-in page and asked to re-enter their credentials.

Those who complied ended up divulging their personal information.

"Phishing and spam will continue to increase on social networks as users migrate large portions of their Internet activity such as e-mail to these properties," said Govind Ramamurthy, chief executive and managing director of MicroWorld Technologies, an anti-virus, anti-phishing solutions provider.

Identity theft or phishing (pronounced 'fishing'), as it is known in Internet parlance, is when a fraudster sends out e-mails pretending to represent an established company or bank to extract personal information.

Though hacking has been prevalent since the World Wide Web became popular, experts say hackers are re-inventing themselves to gain access to confidential information.

In fact, for opportunistic scammers and spammers looking for an issue to exploit, nothing is too trivial, not even AH1N1 flu.

Following its global outbreak, "spamvertising" links to pharmaceutical scams and bogus "Swine Flu Survival Guides" have sprung up across the web using search engine optimisation techniques.

Result: users searching for swine flu information on Google were directed to bogus sites.

Said Akhilesh Tuteja, head of information security at global consultancy firm KPMG: "When one goes fishing, he throws his net in the area where there would be maximum number of fish. Similarly, social engineering sites have the maximum number of catch for hackers."

What's particularly alarming is that people can be trapped even when browsing for something innocuous on Google.

"What we read in fiction has now become real. Sometimes, when you are searching for the link to your bank, a thousand other links pop up. One needs to be sure of the link one is clicking on," Mr. Ramamurthy told IANS.

"More than 12 banks have been phished in 2008-09 in India including ICICI and Bank of India."

So how safe are the solutions against phishing?

"No solution promises 100 per cent secure network. It is the user who has to be careful and cross-check any link or URL (uniform resource locator) before clicking on it," Mr. Ramamurthy said.

"Though anti-phishing solutions flush out most fake Websites, it's always possible hackers will infiltrate through email or SMS (short message service) on your mobile."

According to Indian Computer Emergency Response Team (CERT-In) under the Communications and Information Technology Ministry, 505 security incidents were reported last month. Of these, about 8 per cent were phishing-related.

Anti-virus Internet security firm Symantec, in a recent Internet Security Report to CERT-In, said global malicious code activity continued to grow at a record pace through 2008, primarily targeting confidential information of Net users.

"Due to a rapidly growing Internet infrastructure, a burgeoning broadband population and rampant software piracy, India is expected to witness increased malicious activities," said Symantec managing director Vishal Dhupar in the report.

"Over the past year, Symantec has observed a 192 percent increase in spam detected across the Internet as a whole, from 119.6 billion messages in 2007 to 349.6 billion in 2008."

The report said 55,389 cases of phishing were detected in 2008, a 66 percent growth over the previous year.

According to Mr. Tuteja, it is vital that anti-malware solutions are installed instead of a simple anti-virus solution. "Awareness remains the key," he said.

[Sci. & Tech.](#)

---

Sections: [Top Stories](#) | [National](#) | [International](#) | [Regional](#) | [Business](#) | [Sport](#) | [Sci. & Tech.](#) | [Entertainment](#) | [Agri. & Commodities](#) | [Health](#) | [Index](#)

The Hindu Group: [Home](#) | [About Us](#) | [Copyright](#) | [Contacts](#) | [Subscription](#)

Group Sites: [The Hindu](#) | [Business Line](#) | [Business Line News Update](#) | [Sportstar](#) | [Frontline](#) | [Publications](#) | [eBooks](#) | [Images](#) | [Home](#)

Copyright © 2009, The Hindu. Republication or redissemination of the contents of this screen are expressly prohibited without the written consent of The Hindu

---