

## Social Engineering

By Saurabh Patil

The Antop Hill police, with the help of anti-terrorism squad (ATS)'s cyber unit arrested four persons for hacking into credit card holder's bank accounts and using the money for paying electricity bill online. The accused would also charge a "commission" from their customers, whose bills they would pay.

The prime accused, Ramzan Aurangzeb, has been sent to police custody.

The Antop Hill police registered a case of cheating on July 1 after Yogendra Singh, an engineer, approached them. He told the police that he received a call from an unidentified caller who introduced him as a customer care executive from a leading bank. Singh had a Citibank credit card. "Asking if I would want a Standard Chartered Bank's credit card, the caller took down details, such as my date of birth, mother's name and the last two digits of my Citibank card. The next day, another man came and collected documents supporting these details and said I would get a new credit card," Singh told the police.

A few days later, he received another call and this time, the

man posed as Citibank employee. He asked Singh if he would like to increase the credit limit on his card. "Even after a week, when no one from Citibank did not contact me about the credit limit, I tried to log on to my bank account, but failed. It was hacked," Singh told the police. Singh called up the customer care service and learnt that his password had been changed and Rs 82,940 had been transferred from his account to pay Reliance Energy bills of several people.

The Antop Hill police then took help from inspector N T Kadam, API Nasir Kulkarni and ATS officers to solve the case.

The ATS traced the IP address to Ashish Cyber Cafe in Kandivli and instructed the owner, Ashraf, to keep a tab on the suspect, Aurangzeb. Ashraf checked CCTV images in his cafe and a few weeks later, when he spotted the man, he alerted a Dahisar police station's constable who detained Aurangzeb. The accused has admitted to being involved in at least eight such cases.

above attack come under

### **Social Engineering:**

Social engineering has always been a dangerous threat to organizations of all types. One of the more common reasons for someone to use social engineering is to try and obtain sensitive organizational information or access to a system or facility that normally would not be available to an outsider.

Social engineers achieve their goals by identifying targets within an organization to exploit. These targets are either people in certain roles, such as help desk, human resources, and general users, or they are physical elements, such as side entrances and garage access points.

What the social engineer wants is either informational based or action/result based, and social engineering is either part of the intelligence-gathering process or the exploit and penetration process.

Although we call it social engineering, there is actually a social side and a technical side to the process: Social methods include phone calls, email, and face-to-face contact. Technical methods include posting a fake login page or impersonating a web site.