OUTLOOK india.com
FULLY LOADED MAGAZINES
Hindi Traveller Money Business

Business MAGAZINE | NOV 17, 2003

CREDIT CARDS

World Wide Web

India's e-commerce is expected to rise to Rs 2,300 crore by 2006. But where are the laws to check abuse?

HARSH KABRA

- Over 600 employees of an Indian company receive an e-mail from info@amazon.com offering a book discount. They swamp the link, only to realise that an employee has spoofed the address to glom money and card numbers.

- A man pays for jewellery worth lakhs with a card. But the jeweller never gets money because the code on the card's magnetic strip has been rigged to get another computer, instead of the bank server, to authenticate the transaction.

Plastic money can buy you problems, and technologies can be ready accomplices. The hazard of credit card abuse stalks you in the virtual as well as the real world today. Gartner reports that over seven million Americans were victims of stolen credit card information last year. According to the American Banking Association, its members suffer identity fraud losses of around $1 billion and credit card companies absorb losses of around $1.5 billion every year. Identity thefts in the UK, reveals the UK Fraud Advisory Panel, cost victims nearly £#62.5 million and the UK economy £#1.3 billion.

Hackers use sophisticated software that can be installed on the computer and siphon off data on the sly.

Isn't India too at risk, with cardholders rising to 100 million in the next five years? A recent CII study pegs the share of e-commerce at 12 per cent of the total revenues generated on the Net. Nasscom pitches e-commerce activity in 2002 at $300 million (over Rs 1,383 crore), only half that of China now but expected to grow to Rs 2,300 crore by 2006. Pavan Duggal, Supreme Court advocate and cyber law consultant, says: "There's no law—not even for data protection—that actually deters people from misusing credit cards. The risk is far greater here."

And the conditions are only too conducive. Manual card swiping machines continue to be in vogue and the entire 16-digit card number is still printed on invoices, even as most countries have replaced all but the last four digits with asterisks. Banks hush card frauds fearing damage to their credibility, so less than 0.1 per cent cases are reported in India. No card-related complaints have yet come to Bangalore's Cyber Crime Police Station set up in 2001, DySP Chandramohan Singh reveals.

Meanwhile, hackers continue to outsmart their pursuers. Says Kuji, a former hacker: "Every time a form is filled on the Net, no matter what the website declares, there's a possibility of that information leaking to unauthorised viewers." Today, Kuji's tribe is armed with programmes that can identify the bank issuing a card, harvest the three-digit card verification number, finagle the owner's personal details, check the card's validity, and even engineer the available credit limit.

A recent report by the Honeynet Project, a group of online security experts, says that the Internet Relay Chat (a messaging system for large networks) now abets online credit card fraud. Hackers also use sophisticated spy softwares, often dowloaded from the Net, that get installed on the computer and siphon off data on the sly.

Yerra Ravi Kiran Raju, certified "ethical" hacker, researcher at the Pune-based Centre for Information and Network Security and principal consultant with Network Security Solutions, demonstrates how searching for certain keywords and queries using an everyday search engine like Google can gain him access to card databases. He takes us through some he has downloaded on his computer. We also accompany him to the Internet chatrooms teeming with "carders"—those who crack into card databases and sell info or stuff like pin decryptor.

Ravi explains how fraudsters can reprint cards using numbers pillaged during manual swipes and how cards devoid of data on their magnetic strip hold good for most transactions in India. Even the data on the magnetic strip can be copied using a special recorder that can be fitted in the swiping machine itself.Worse, such recording devices can be conveniently ordered over the Net by almost anybody. Even the data contained in smart chips, used by many cards to guard against abuse, can be copied to other smart chips. Says Ravi: "The effects of card abuse aren't visible for the first few months. When they begin to appear, the culprit is untraceable."

Says Debashis Nayak, a consultant with the Asian School of Cyber Laws (ASCL) and a partner at TechJuris, a law firm specialising in technology: "Card numbers are relatively safe when they travel in a secure, encrypted format. The danger is in the source and the destination computers." Ravi agrees: "The risk may start from your own computer. You won't know if your details are being fished out and stored elsewhere."

Even the ubiquitous call centres are vulnerable. "I can make separate phone calls to such centres and extract the required details in parts," says Ravi. "Like, I cite a number, obtain the cardholder's name and hang up. Then I pretend I want to change the date of birth in the cardholder's profile, obtain the exact date and hang up. By then, I have obtained sufficient data for extracting the pin number the next time."

From the instances reported thus far, says Nayak, two patterns are apparent. "The first is where card numbers are noted down from physical locations, such as petrol pumps, restaurants and shops, and later used online. The second involves the creation of bogus online shopping websites to lure prospective buyers to part with their credit card numbers, which are then misused on the Internet."

According to Ravi, e-mails can be spoofed in such a way that they appear to be originating from someone close to the recipient. If the sender requests some critical data, it is quite likely that the unsuspecting recipient will part with it in his reply. Alternatively, the moment that recipient opens the e-mail, it could trigger off the installation of a spy software, which will subsequently draw off more such data. That's petrifying—how many of us actually bother to verify the authenticity of the sender and his e-mail address?

Is it possible to nab such culprits? Yes, but a bigger problem is toothless laws. Says Duggal: "Credit card payments are a matter of contractual law between the concerned parties. Even the provisions of the Information Technology Act, 2000, haven't been tested practically. Convincing the police to act under those provisions is a challenge in itself. Plus, card companies simply wash their hands of cases involving big amounts." And the user is the worst-hit. Over 35 per cent of card users in India may have faced card abuse, Duggal says. And prudence and precaution alone can save them.

Click here to see the article in its standard web format