# Logistics firm at Govandi cheated of Rs10.89 lakh by online fraudster

Jayprakash S Naidu
jayprakash.naidu@hindustantimes.com

**MUMBAI :** A logistics company at Govandi recently lost $16,000, or Rs10.89 lakh, to an unidentified attacker who hacked its official email account to seek an early payment from its client in Italy.

Such frauds are, in cyber lingo, termed man-in-the-middle attack involving hacking an official e-mail account of a company and finding out about its upcoming transactions with other companies.

According to a First Information Report registered (FIR) with the Govandi police station on January 17, the company used to regularly deal with the Italian company. It used to deliver goods received from the foreign client to various addresses in the country.

The representatives of both companies would communicate through e-mails.

The unidentified attack somehow managed to hack the Gmail account of the complainant's company and sent an email to the Italian company's representative asking for an early payment.

In the message, he also provided the bank account number in which the money was to be deposited.

The transaction of $16,000 was made in September last year. The company, however, learnt about the fraud when it did not receive money and contacted the client.

They approached the Govandi police station and filed a case. The investigation revealed that the money has been sent to a bank account in a foreign country.

The police are trying to trace to which country this money has been sent.

**THE COMPANY LEARNT ABOUT THE FRAUD WHEN IT DID NOT RECEIVE MONEY AND CONTACTED THE CLIENT IN ITALY**

## WHAT IS A MAN-IN-THE-MIDDLE ATTACK?

**It is a cybercrime** in which the attacker hacks an official e-mail account of a company and find out about its upcoming transactions with other companies.

**Once the hacker gets** all the required information, including the invoice that has details of the transactions, he uses the company's e-mail address and asks the opposite party to send the money to a new bank account. An official from the cyber police said, "The hacker gives one of many possible reasons to justify the change in bank account — that a government audit is in progress, that there is some issue with the current bank account, or that they need the money delivered to a different branch in another country."

**The officer added** it is also possible that hackers get information they need from people within the companies they target.

**37% INCREASE IN MAN-IN-THE-MIDDLE ATTACKS IN 2016**

| | CASES REGISTERED | MONEY INVOLVED |
|---|---|---|
| 2015* | 19 | ₹4.33cr |
| 2016* | 26 | ₹14.54cr |

*In 2015, the police could not detect any case while for 2016 data is unavailable

## STAYING SAFE ONLINE

- Three ways to prevent online attacks and scams, suggested by the cyber police:
- Before making a financial transaction, phone the person and check the details of thebank account where the money is to be sent. Most business transactions with foreign companies take place on email. It is suggested company representatives meet in person to talk at length about the deals and keep in touch throughout to avoid being cheated.
- Apprise your employees about how man-in-middle attacks, data theft and other cyber offences.
- Beware of viruses and spam e-mails. Clicking on them may compromise your data.

**HOW TO CONTACT THE CYBER POLICE**

24x7 helpline: **9820810007**
Telephone: **022-26504008**
E-mail: cyberpst-mum@mahapolice.gov.in
Postal address: Cyber Police Station, First Floor, Bandra Kurla Complex Police Stn, Bandra (E), Mumbai 400051

# Long legal process hampers police's efforts to detect cases

Jayprakash S Naidu
jayprakash.naidu@hindustantimes.com

**MUMBAI:** The number of man-in-middle attack cases rose by 37% to 26 in 2016 from 19 in 2015. While in 2016, victims lost Rs14.54 crore, the amount stood at Rs4. 33 crore in 2015.

All man-in-the-middle cases in 2015 remained undetected. The police attribute it to the cumbersome legal process of a particular country from where the crime was committed and non-cooperation from social networking sites and Internet service providers for personal information and location of overseas servers.

These are just the cases which are registered with the police. "There are cases where private firms do not come forward to avoid disrepute," said cyber expert Ritesh Bhatia.

All bank accounts, where money has been deposited, are in foreign countries. When contacted by the cyber police, these banks authorities take a month to reply and eventually deny giving any information. They ask the police to approach them through legal channel (letters rogatory) which is a lengthy process.

For the legal remedy, the stat home department co-ordinate with the central home depar ment. After getting the govern ment's approval, the police ar allowed to write to a foreign cour try's court, which give a go-ahea to probe the case.

The legal tangle is, howeve not the only stumbling block.

When contacted, internet se vice providers and social ne working sites too take weeks t reply and later ask the police t move court before divulgin information about a hacker