

# ICICI BANK CUSTOMER EDUCATION SERIES

A TIMES BUSINESS ASSOCIATE COMMUNICATION

## Beware of SIM-Swap Fraud!

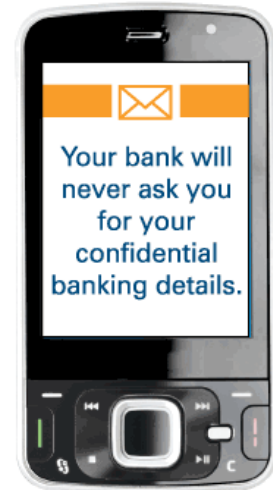
Your mobile phone is now also a convenient banking channel; but it can make you vulnerable to SIM-swap fraudsters if you do not take some simple precautions.

### How do SIM-swap frauds occur?

- The fraudster obtains your mobile phone number and bank account details through a phishing e-mail.
- He asks your mobile-phone-service provider for a replacement SIM card under some pretext, like changeover to a new handset or loss of SIM/handset.
- The service provider deactivates your SIM card and gives him a replacement SIM.
- The fraudster introduces a payee into your bank account using the phished data, transfers funds from your account to his and withdraws the money through an ATM.
- All this while, your service provider's alerts don't reach you because your SIM card has been deactivated.

### What are the safeguards that should be taken?

- Never respond to phishing e-mails.
- Do not disclose your mobile phone number on unknown websites.
- Change your banking passwords frequently.



If you find your mobile number inactive for an unusually long period or abruptly barred from calls; or if it displays limited access or says the SIM is inactive; contact your service provider without delay and find out the reason.



BE AN INFORMED CONSUMER. Watch this space every Monday.