

# SAFE BANKING TIPS

## DO NOT SHARE YOUR USER ID AND PASSWORDS WITH ANYONE

### TIPS FOR SAFE PASSWORDS

- Do not use familiar names which are easily discoverable (self, spouse, children, parents, pets, etc.).
- Avoid using commonly known facts about yourself (hobbies, birthdays, favourite sports, etc.).
- Don't use obvious words and numbers related to your identity (e.g. address, name of organization etc.).
- Don't use repeated letters, numbers or words or dictionary words – Intentionally misspell words.
- Use at least six or more characters. More the characters in a password, the more secure it is.
- Utilize a combination of letters and numbers to make it more difficult for a person / software programme to guess your password.
- Use special characters (@, #, %, \$, etc.) to make the password more difficult to crack.
- Use a combination of upper- and lower-case letters, where possible, to create a more secure password.
- Make it easy to remember, but hard to guess
- Change your passwords regularly, every few months if possible – don't reuse them.
- Secure your password records by memorizing or hiding/disguising them on your computer/phone/other device.

### EMAIL SECURITY

- Don't click on web links or attachments from suspicious emails
- Never share your passwords or financial details via email
- Create separate email accounts for different purposes or activities

### CHEQUE BOOK SAFETY MEASURES

#### DO'S AND DON'TS

- Record all details of cheques issued / cancelled.
- Do not leave your cheque book unattended. Always keep it in a safe place, under lock and key.
- Whenever you receive your cheque book, please count the number of cheque leaves in it. If there is a discrepancy, bring it to the notice of the Bank immediately.
- Do not sign blank cheques. Always fill in the date, the name of the beneficiary and the amount before signing the cheque.
- Remember to cross your cheque whenever applicable and prevent it from being misused.
- Always draw a line through any unused space.
- Never sign in multiple places unless authenticating a change.
- Avoid using cheques with changes on them. Issue a new cheque if possible.
- When you cancel a cheque, mutilate the MICR band and write "CANCEL" across the face of the cheque.
- Do not write / sign / mark / pin / staple / paste / fold on the MICR band.




# PHISHING

Not all phishing attacks require a fake website. Over time, fraudsters have found many innovative and sophisticated social engineering techniques of phishing viz. phone phishing, SMS phishing etc.

Hoax calls received from strangers – Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

Societe Generale does not send emails requesting you to confirm, update or disclose your confidential banking information. If you receive an email you believe may be a hoax please forward it as an attachment to [sgindia.ccare@socgen.com](mailto:sgindia.ccare@socgen.com) and to your IT department. Do not just delete these emails. If you happen to provide any confidential data to a phishing email or fake link, **change your password immediately** after if you have entered your personal data on a fraudulent link.

## DO'S AND DON'TS

- **Please do not respond to any phishing or vishing e-mails claiming to be from Societe Generale Bank.**
- Do not open spam or fake mails or click on links/attachments in such emails. Exercise due caution.
- If you suspect the email sender or hoax caller, it would be wise to call up and confirm that sender/caller is genuine.
- Communicate confidential information only via secure web sites. A secure web site has a lock sign  on the browser's status bar or a "https:" URL whereby the "s" stands for "secure" rather than a "http:".
- Do not enter your confidential data in any window that may pop-up while you are carrying out a financial transaction.

## INTERNET BANKING SECURITY TIPS TO AVOID PHISHING

- Ensure your computer is protected with the latest anti-virus and firewall protection software at all times.
- Never disclose your Internet Banking password to anyone, not even to the Bank employee.
- Disable any functionality on your computer or browsers that remembers your logon details.
- Always visit the Bank's Net Banking site through its homepage by typing the bank's website address (<http://www.societegenerale.asia/>) on to the browser's address bar. Users are encouraged to add the bank's URL to Favourites or Bookmark in the user computer browser.
- Check your bank account and bank statements to verify any transaction that you cannot explain. Report it to the bank immediately.
- Always logout of Net Banking using the Logoff button located on top right corner of the screen.
- Avoid the use of public computers in cyber cafés. Only connect to known and trusted Wi-Fi hotspots.
- Register for e-mail alerts to check your account regularly.

## SPEAR PHISHING

Spear phishing is a targeted phishing attempt through an e-mail that appears to come not only from a trusted source, but often from someone in your own company, a superior in many cases, or from a close relative. The subject line address is customised/personalised and often will be one of relevance to either current projects of developments within the company, or may be related to family event. The violation occurs when the user opens the e-mails, clicks on the link attached and then trojans or malware gets downloaded or a form appears on the screen, in which data needs to be filled in by the recipient. This information is confidential and could be useful for accessing and transacting on internal organisation's application.

## DO'S AND DON'TS

- If the message prompts to disclose your personal confidential information any time STOP. Recheck.
- Do not respond or act without first contacting the 'sender' by telephone and verifying that the e-mail is legitimate.
- Do check the senders e-mail address displayed, whether it perfectly matches with e-mail address used within your company.
- Do check whether the sender associated with the e-mail is indeed from the company.
- Do not open attachments in such e-mails as they may carry virus.
- Do check the website where you might get redirected. The redirected website should belong to your company.
- Do not just delete these e-mails. Report them immediately to your IT dept or your company contacts for computer support.

## SIGNING ON BLANK DOCUMENTS



Security of your organizational information and accuracy and completeness of documentation before transaction is executed, is a vital step towards ensuring data security and confidentiality. The Bank requests you to sign only those documents (e.g. such as account opening forms, Standing Instructions, Fund Transfers, Service requests etc.) that are completed in all respects and are to your satisfaction. We urge you not to sign or hand-over any blank or incomplete document/s to any Bank Staff to help us protect your interests.

The Bank never requests you to disclose security details via e-mail or phone call. If you receive such an e-mail or call, kindly forward this to us at [sgindia.ccare@socgen.com](mailto:sgindia.ccare@socgen.com) or call us at +91 22 6630 9500 to enable us investigate the issue. The Bank urges you to remain alert and not to fall prey to frauds or scams perpetrated by individuals who impersonate employees of the Bank.

In case you suspect any discrepancy or unauthorized transaction in your account with the Bank, you should intimate about it to us at the earliest, either by sending an email to [sgindia.ccare@socgen.com](mailto:sgindia.ccare@socgen.com) or contacting us at +91 22 6630 9500. Kindly note any delay in notifying the discrepancy or unauthorized transaction to the Bank, could potentially lead to a higher risk of loss to you and / or the Bank.



### SOCIETE GENERALE, INDIA

19th Floor, Tower A, Peninsula Business Park, Ganpatrao Kadam Marg, Lower Parel, Mumbai 400013

+91 (22) 66309500

+91 (22) 66309696

[www.societegenerale.asia/](http://www.societegenerale.asia/)

Branch offices: • Mumbai • Delhi • Ahmedabad • Chennai