Short Tips

These tips can prevent you from majority of frauds

1. Trust but verify - Emails, phone calls, fax, impersonators
2. Be mindful of whom you add and what you share on internet
3. Control the Greed - Anything which is simply too good to be true, probably is.
4. Protect yourself and family against Identity Theft- Secure your passwords, documents and bank related information
5. Never use pens provided by others while writing cheques

Short tips to prevent cheque frauds

1. Don’t issue cheques to unknown people, sometimes fraudsters offer deals which are “Too good tobe true” to get a cheque sample from victims.
2. Don’t act as “Money mule” by depositing cheques on behalf of others and making them partpayment in cash/transfers from your account.
3. If someone offers you a pen to write on certain documents, be careful and check whether this couldbe a “magic Ink” pen.
4. All cheques have security features, some of which are printed on the front/back of the cheque.Please ensure that any cheque being presented by you contains those security features.
5. Consider having different set of signatories depending upon amount thresholds.

Short tips to prevent Business Email Compromise frauds

1. Confirm requests for transfers of funds and changes in vendor payment accounts through alternatemediums such as a previously used phone number or fax.
2. Keep your PC/phones updated with latest anti virus/anti malware to prevent email compromise
3. Be careful when posting financial and personal info on the internet
4. Should one become a victim of a business email scam, one should immediately notify the concerned bank. Afunds recall message can then be sent to the beneficiary bank by the remitting bank and if funds are available in the beneficiary account, they may get returned.
5. Victims should consider filing a police complaint at the earliest.

Short tips to prevent SIM replacement frauds

1. Please keep your contact details updated with your bank, if any of your phone number is not workingupdate the new number immediately with the bank
2. As soon as you realise that your phone is not working, call up your bank and consider putting debitfreeze on your account
3. Contact your telecom service provider and inquire whether any duplicate SIMs/Multi SIM have beenissued for your mobile number. If any are issued without your consent, get them deactivated.
4. Keep your laptop/PC/mobile phone updated with latest anti virus/malware to prevent against datacompromise.
5. Victims should consider filing a police complaint at the earliest.

Short tips to prevent Advance fee scams

1. Bank letters or financial documents provided by fraudsters are generally badly written withsome obvious spelling mistakes and poor grammar.

2. Avoid opening emails from unknown senders, adding unknown people to chats & socialmedia platforms etc.

3. Don’t give you bank details or any documents to fraudsters, if you have already given,alert your bank immediately.

4. Remember, “Something which is too good to be true”, is rarely true

5. Should one become a victim of a fraud, one should immediately notify the concerned bank/exchange house.Victims should consider filing a police complaint at the earliest.