SAMATA CO-OPERATIVE DEVELOPMENT BANK LTD.

Dakshata : Cyber Security Initiative by SCDBL Date: 15-04-2024

"Dakshata" is Cyber Security Awareness Initiative started by SCDBL. This initiative is to provide cyber security awareness to SCDBL employees, Depositors, Customers, Directors and shareholders to protect from Cybercrimes and frauds. The cyber security awareness to each and every one is necessary because of increasing volume of digital transactions and cyber frauds. The digital transactions for payments are very convenient to use but should be used with caution to protect yourself from financial loss.

Cyber threats are attacks happening over Internet or Online Digital world.The hacker can steal your personal information, PIN, passwords, OTP Dai and it can lead to big financial loss.

How the hacker can get your information?

The hacker can get your personal information from your online devices such as mobile, laptop, PC etc. The hacker sends Phishing email /SMS which is malicious email /malware (Malicious software or virus) into your mobile / laptop via Internet. If you click on the link or attachment in email /SMS the hacker can take control of your device which may lead to financial loss.
When the Malware infects your mobile/ laptop / PC and it then send your important data/ critical information, passwords, credentials to the hacker.

There are some simple steps to protect yourself from Cyber Attacks:

1. The Fraudsters lure the people / Victims with various shopping discount schemes, investment schemes winning of lottery, free gifts, Work from home job offers etc., Initially the hacker may also give some gifts to gain your faith and call to get your Debit / Credit card details, Account details, password, PIN, CVV and OTP. Do not share these critical Card/ account Details and your personal information to unknown people. The Bank officials will never call customers to get Card details, Passwords, CVV, PIN, OTP or KYC details.

2. Your critical personal information on social sites can be used by hacker to make an attack. So do not share important info on social sites. Sometimes hackers call and panic the victims for closing of bank account or blocking of credit card. Do not click on such links or give your OTP, CVV, card number. Be careful on accepting friends request from unknown people.

3. Sometimes the victims are lured for high interest investments schemes and link for remote control app is sent on mobile. Do not install such apps in your mobile, Laptop, as it gives complete control of your device to hacker.

4. Recently Al and ML tools are used to make audio video calls which resembles like call from your friends or relatives to request for money. Please cross check by calling back to avoid fraud.

5. Protect your Mobile, PC and Laptop with strong password and change password regularly. Never keep ATM card and PIN together in wallet. Start using green PIN facility

6. Check that good Antivirus / Anti-malware is updated on your mobile / PC regularly.

7. Check the system updates and security patches are updated regularly. Enable Firewall in PC / Laptop System.

8. Always be vigilant when using ATM card to protect from Skimming/shoulder surfing attack. Do not share OTP, CVV and card number to strangers.

9. Do not click on link or download Email attachments / SMS received from unknown people. It could be phishing email with fraudulent link or malware.

10. Do not give Remote access or use screen sharing apps such as Anydesk etc. to strangers. The fraudsters can take admin control of your system and hack into your mobile / Laptop / PC. Your critical Data can be misused by fraudster.

11 . Do not visit untrusted websites or provide your personal details to unknown people on social networking websites. Protect your privacy and be vigilant when using social networking and Internet. Never share your personal and critical information on Social sites as it can be misused to make targeted attack

12.Take Data backup of your system regularly and keep it on separate device or USB drive

13.Remove unwanted software's or applications from your Mobile / PC. Also remove unnecessary extra permissions given to Mobile apps.

14.The mobile/ Laptop used for mobile banking, Net banking or financial transactions should have restricted access to Social networking/ gaming sites. The transaction limit should be set to avoid big financial loss.

15.Do not use public Wi-Fi or free Wi-Fi (at Railway station, Hotel Lounge) for financial transactions. The fraudster can get your account details to flush your account. Use mobile device Internet or private wifi for financial transactions.

16.Do not use free USB charging stations or Charger from unknown public places to charge your Mobile/Laptop. The fraudster can capture your critical data from your Mobile. In emergency the device can be powered off before charging.

17.Do not click on Internet link/ SMS attachment sent by Unknown people, as it can be Malware or Phishing attack.

18. UPI PIN should NOT be entered to receive the payment. UPI PIN should be used to make the payment, only from the well-known Apps.

19. UPI PIN should not be disclosed or shared with strangers

20. QR code should be scanned only to send money and NOT for receiving money

21. Please Visit your nearest Branch to update your KYC details such as Aadhar number, PAN Number, Mobile Number, Email ID so that Bank can communicate and alert you when necessary. The Bank officials never call you to get KYC details.

22. If your SCDBL ATM card is lost or if any suspicious card transactions are observed please HOT MARK your card by calling toll free Number to 1800-1200-107.

23. Take above precautions and use POS, ECOM, UPI services with confidence as it is very much convenient and available Download apps only from Google play store or iOS platform.

24. In case any query or any suspicious activity observed please Call SCDBL toll free number 1800-1200-107 or Email to care.customer@samatabank.org

25. If your money is lost due to online fraud then block your debit/ credit card or Debit freeze your account immediately by calling respective Bank authority and inform Cyber Crime Helpline number 1930 ASAP or visit https://cybercrime.gov.in