BASSEIN CATHOLIC CO-OPERATIVE BANK LTD

Dakshata: Cyber Security Initiative by BCCB **Date: 7th Oct 2022**

“Dakshata” is Cyber security awareness initiative started by BCCB. This initiative is to provide cyber security awareness to BCCB employees, Depositors, Customers, Directors and shareholders to protect from Cyber threats and frauds. The online digital transactions to receive or make payment are very convenient to use but should be used with caution.

Cyber threats are attacks happening from Internet or Online Digital world. The attacker or hacker can steal your personal information, PIN, passwords, OTP Data 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 first sends Phishing email /SMS which is malicious email /malware (Malicious software or virus) into your mobile / laptop via Internet. When 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 discount schemes, winning of lottery, free gifts etc, and call them to get their Debit / Credit card details, password , PIN, CVV and OTP. Never share your Passwords / OTP / CVV / PIN / Card 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.Protect your Mobile, PC, Laptop with strong password and change password regularly. Never keep ATM card and PIN together in wallet.

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

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

5.Always be vigilant when using ATM card to protect from Skimming attack. Do not share OTP, CVV, card number to strangers.

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

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

8.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

BASSEIN CATHOLIC
CO-OPERATIVE BANK LTD

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

10.Remove unwanted softwares or applications from your Mobile / PC. Also Remove unnecessary extra permissions given to Mobile apps.

11.The mobile/ Laptop used for mobile banking, Netbanking should be restricted for Social networking access. The transaction limit should be set to avoid big financial loss.

12.Do not use public Wifi or free Wifi (at Railway station, Hotel Launge) for Financial transactions. The fraudster can get your account details to flush your account. Use mobile device Internet or private wifi for financial transactions.

13 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.

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

15. UPI PIN should be used only to make the payment, from the well known Apps
UPI PIN is NOT required to receive the payment.
UPI PIN should not be disclosed or shared with strangers
QR code should be scanned only to send money and NOT for receiving money

16.Please Visit your nearest Branch and 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 on phone.

17.If your BCCB ATM card is lost or if any suspicious card transactions are observed please HOTMARK your card by sending SMS “HOTC” from your Registered Mobile Number to 9222272407.

18. Take above precautions and use BCCB Netbanking , Mobile banking Digitouch, POS, ECOM, UPI services with confidence as it is highly convenient and available 24X7.

19. In case any query or any suspicious activity observed please call BCCB call center 18002662407 or Email to customerservice@bccb.co.in