Dakshata : Cyber Security Initiative by BCCB Date: 20 Sep 2022

The BCCB have Cyber security awareness initiative called “Dakshata”. This initiative is to provide cyber security awareness to BCCB employees , Depositors, Customers , Directors and shareholders to protect from Cyber threats and Hackers.

Cyber threats are attacks happening from Internet or Online Digital world. The attacker or hacker can steal your personal information , passwords , Data and it can lead to financial loss.

How the hacker can get your information.....?

The hacker can get your personal information from your online devices (which are connected to Internet) such as mobile , laptop , PC etc. The hacker first sends Phishing email which is malicious email /malware (Malicious software or virus) into your mobile / laptop via Internet.

The Malware resides in mobile / laptop / PC and it then send your Data/ critical information, credentials to the hacker. Sometime Hacker sends Emails with malicious links or attachments. If you click on it then your mobile / PC may get Infected by Malware and it can send your critical information to 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 takeaways 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 never call customers to get passwords,CVV,PIN or OTP

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 received from unknown people.

7.Do not install Remote access apps such as Anydesk etc. The fraudsters can take admin control of your system and hack your mobile / Laptop / PC.

8.Do not visit untrusted websites or provide your personal details to unknown people on social networking websites.

9.Take Data backup of your system regularly.

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

11.Protect your privacy and be vigilant when using social networking and Internet

12.Do not use public Wifi or free Wifi for Financial transactions. The fraudster can get your account details to flush your accout.

13 Do not use free USB charging stations or Charger from unknown public places to charge your Mobile/Laptop. The fraudster can take away 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.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.

16.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.

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

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