Best Practices and Recommendations: Debit Card users

- Memorize your PIN. Do not write it down anywhere. Do not disclose your ATM PIN details to anyone.
- Block the view of the number pad, so that nobody can notice your PIN. Never allow anyone to stand near you or help you complete transactions while at an ATM.
- If you get a transaction slip, tear it into pieces immediately after use if not needed.
- Remember to take your card and cash with you.
- Do not conduct any transaction if you find any unusual/suspicious device connected to your ATM. Please report the same to the Bank.
- Change your ATM PIN number regularly. Do not keep birthdays, anniversaries as PINs.
- While doing transactions at merchant establishment (POS), keep eyes on person swiping the card, if merchant asks for PIN, do not give it away. If PIN is required to be fed, please enter the PIN yourself.
- Erase the CVV number on backside of the card and memorize the same or store it confidentially.
- While doing ATM transactions if card is stuck in the machine, then do not get help if any stranger offers to do so. Cash retraction facility has been withdrawn.
- If your ATM card is lost or stolen, report the same to Bank branch, alternately you can block your card on your Mobile Banking app immediately. Please avail mobile banking facility to activate this service 24 * 7. If you have any complaint about your ATM/Debit/Credit Card transaction at an ATM, please take it up with your Card-issuing branch.

******End******

Best Practices and Recommendations: Android Mobile app users

- Reduce the risk of downloading potentially harmful apps by limiting your download sources to official app stores, such as your device's manufacturer or operating system app store.
- Prior to downloading / installing apps on android devices (even from Google Play Store):
    - Always review the app details, number of downloads, user reviews, comments and "ADDITIONAL INFORMATION" section.
    - Verify app permissions and grant only those permissions, which have relevant context for the app's purpose.
    - Do not check "Untrusted Sources" checkbox to install side loaded apps.
- Install Android updates and patches as and when available from Android device vendors.
- Do not browse un-trusted websites or follow un-trusted links and exercise caution while clicking on the link provided in any unsolicited emails and SMSs.
- Install and maintain updated anti-virus and antispyware software.
- Look for suspicious numbers that don't look like real mobile phone numbers. Scammers often mask their identity by using email-to-text services to avoid revealing their actual phone number. Genuine SMS messages received from banks usually contain sender id (consisting of bank's short name) instead of a phone number in sender information field.
- Do extensive research before clicking on link provided in the message. There are many websites that allow anyone to run search based on a phone number and see any relatable information about whether or not a number is legit.
- Only click on URLs that clearly indicate the website domain. When in doubt, users can search for the organization's website directly using search engines to ensure that the websites they visited are legitimate.
- Consider using Safe Browsing tools, filtering tools (antivirus and content-based filtering) in your antivirus, firewall, and filtering services.
- Exercise caution towards shortened URLs, such as those involving bit.ly and tinyurl. Users are advised to hover their cursors over the shortened URLs (if possible) to see the full website domain, which they are visiting or use a URL checker that will allow the user to enter a short URL and view the full URL. Users can also use the shortening service preview feature to see a preview of the full URL.
- Look out for valid encryption certificates by checking for the green lock in the browser's address bar, before providing any sensitive information such as personal particulars or account login details.
- You should report any unusual activity in your account immediately to your branch with the relevant details for taking further appropriate actions.

******End******

Cybersecurity Awareness Campaign: Phishing

This is an awareness campaign regarding phishing attempts, as detailed below.

What is Phishing?

Phishing is a way of attempting to acquire information such as usernames, passwords, PIN, bank account, credit card details by masquerading

as a trustworthy entity details through electronic communication means like e-mail. Phishing is typically carried out by e-mail spoofing

or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate

one. Phishing is an example of social engineering techniques used to deceive users.

If something seems fishy...it's probably phishing. Here are some tips to keep in mind to avoid falling victim so that we protect our Bank and its data:

- Double-check that the sender's email address matches who they claim to be
- Don't click a link or download from emails sent by someone you don't know, or weren't expecting
- Typically, these emails will be poorly drafted with spelling mistakes. This should serve as an alert.
- Don't reply to a suspicious email or message from an email you don't recognize

******End******

Cybersecurity Awareness Campaign: Smishing

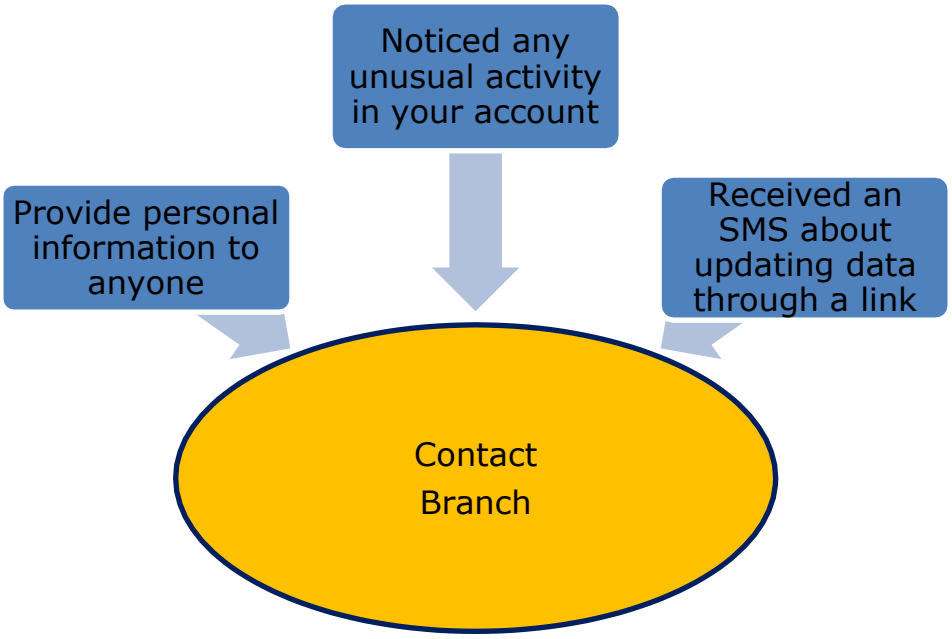
Smishing uses cell phone text messages to lure users in a similar fashion like Phishing. They take the form of text messages that claim to be from legitimate entities and are often used in combination with other techniques to bypass inbuilt protections. They might also direct victims to malicious websites on their phones.

Typical Examples of Smishing Attacks

Best practices to follow to avoid Smishing attacks:

- Be suspicious of any text messages containing urgent request for personal or financial information.
- Do not share any sensitive information over text messages.
- Do not click on any links on the SMS.
- Please call the branch for help or refer to the information only on the official website of the bank.

Get in touch with your branch if you have



******End******