The Co-Operative Bank of Rajkot Ltd.
Multi State Co-Operative Bank

Raj Bank

CYBER SECURITY AWARENESS TRAINING MATERIAL - ENGLISH

'Sahakar Sarita', Panchnath Road, Rajkot - 360 001 (Gujarat)
0281 - 2234454 / 2224120 Fax: 0281 - 2236682 info@rajbank.in rajbank.net

Phishing links

Modus Operandi:

- Fraudsters create a third-party phishing website which looks like an existing genuine website, such as - a bank's website or an e-commerce website or a search engine, etc.
- These kind of websites are circulated by fraudsters through Short Message Service (SMS) / social media / email / Instant Messenger, etc.
- Many customers click on the link without checking the detailed Uniform Resource Locator (URL) and enter secure credentials such as Personal Identification Number (PIN), One Time Password (OTP), Password, etc., which are captured and used by the fraudsters.

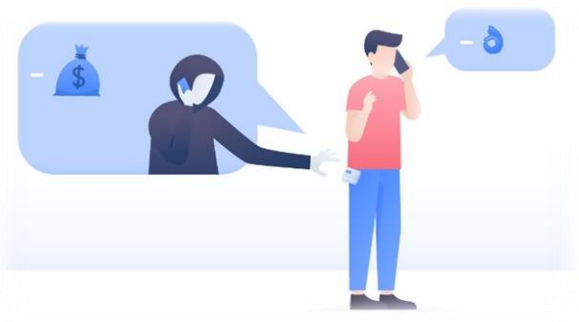
Precautions:

- Do not click on unknown / unverified links and immediately delete such SMS / email sent by unknown sender to avoid accessing them by mistake in future.
- Unsubscribe the mails providing links to a bank / e-commerce / search engine website and block the sender's e-mail ID, before deleting such emails.
- Always go to the official website of your bank / service provider. Carefully verify the website details especially where it requires entering financial credentials. Check for the secure sign (https with a padlock symbol) on the website before entering secure credentials.
- Check URLs and domain names received in emails for spelling errors.

Vishing calls

Modus Operandi:

- Imposters call or approach the customers through telephone call / social media posing as bankers / company executives / insurance agents / government officials, etc. To gain confidence, imposters share a few customer details such as the customer's name or date of birth.
- In some cases, imposters pressurize / trick customers into sharing confidential details such as passwords / OTP / PIN / Card Verification Value (CVV) etc., by citing an urgency / emergency such as - need to block an unauthorized transaction, payment required to stop some penalty, an attractive discount, etc. These credentials are then used to defraud the customers.



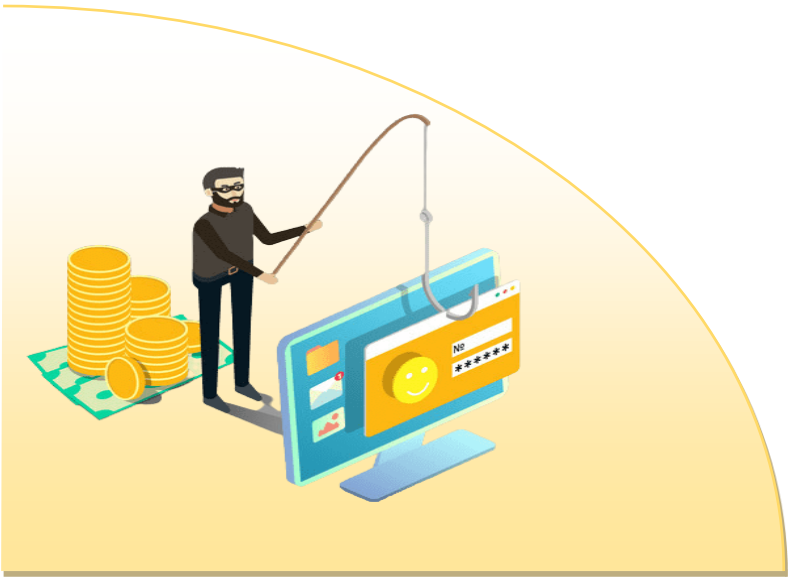
Precautions:

- Bank officials / financial institutions / RBI / any genuine entity never asks customers to share confidential information such as username / password / card details / CVV / OTP.
- Never share these confidential details with anyone, even your own family members and friends.

Frauds using online sales platforms

Modus Operandi:

- Fraudsters pretend to be buyers on online sales platforms and show an interest in seller's product/s. Many fraudsters pretend to be defence personnel posted in remote locations to gain confidence.
- Instead of paying money to the seller, they use the "request money" option through the Unified Payments Interface (UPI) app and insist that the seller approve the request by entering UPI PIN. Once the seller enters the PIN, money is transferred to the fraudster's account.



Precautions

- Always be careful when you are buying or selling products using online sales platforms.
- Always remember that there is no need to enter PIN / password anywhere to receive money.
- If UPI or any other app requires you to enter PIN to complete a transaction, it means you will be sending money instead of receiving it.

The Co-Operative Bank of Rajkot Ltd.

Multi State Co-Operative Bank

Raj Bank

Frauds using screen sharing app / Remote access

Modus Operandi:

- Fraudsters trick the customer to download a screen-sharing app.
- Using such app, the fraudsters can watch/control the customer's mobile / laptop and gain access to the financial credentials of the customer.
- Fraudsters use this information to carry out unauthorized transfer of funds or make payments using the customer's Internet banking/payment apps.

Precaution:

- If your device faces any technical glitch and you need to download any screen sharing app, deactivate/log out of all payment related apps from your device.
- Download such apps only when you are advised through the official Toll-free number of the company as appearing on its official website. Do not download such apps in case an executive of the company contacts you through his / her personal contact number.
- As soon as the work is completed, ensure that the screen sharing app is removed from your device.

'Sahakar Sarita', Panchnath Road, Rajkot - 360 001 (Gujarat)

0281 - 2234454 / 2224120 Fax: 0281 - 2236682 info@rajbank.in rajbank.net

Ransomware Attacks

Modus Operandi:

- Ransomware is a category of malicious software which, when run, disables the functionality of computer in some way. The ransomware program displays a message that demands payment to restore functionality. The malware, in effect, holds the computer system to ransom. In other words, ransomware is an extortion racket. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.
- Cyber criminals send an email to the victim containing suspicious attachment or phishing links. Victim downloads the attachment and opens the file.
- Once the infected file is opened, the victim's system gets locked and all files get encrypted. Alert message displayed on the computer screen demanding ransoms to be paid to unlock the screen or to decrypt the data.

Precaution:

- Do not open emails from unknown sources containing suspicious attachment or phishing links.
- Keep your antivirus up-to-date and windows firewall turned on and properly configured.
- Back up your most important files on a regular basis. Keep the important data on a separate hard disk.
- Enable proper spam filters in your e-mail account.

Cyber Crimes Using Social Media Platforms

Modus Operandi:

- Cyber bullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms, etc. It is a sort of repeated behaviour aimed at scaring, angering, or shaming those who are targeted.
- Examples include: spreading lies about or posting embarrassing photos of someone on social media, sending hurtful messages or threats via messaging platforms, impersonating someone and sending mean messages to others on his/her behalf.
- Perpetrators of cyber bullying (usually known to the victim) get the personal photographs and details of the victim from various social media sites.
- Perpetrators of cyber bullying create a fake account either in the name of the victim or a random name & post several memes and videos making fun of the victim, which goes viral.

Precaution:

- Learn about the privacy settings of the social media apps being used by you.
- Ensure your personal information, photos and videos are accessible only to your trusted ones.
- Think twice before posting or sharing anything online - it may stay online forever and could because to harm you later.
- Report hurtful comments, messages, and photos and request to the concerned Social Media Platforms to remove them. Besides 'unfriending' you can completely block people to stop them from seeing your profile or contacting you.

The Co-Operative Bank of Rajkot Ltd.

Multi State Co-Operative Bank

Raj Bank

Sim Card Swapping Fraud

Modus Operandi:

- It is a type of identity theft where cyber criminals manage to get a new SIM card issued for your registered mobile number through the Telecom Service Provider. With the help of the new SIM card, fraudsters get OTP & other confidential details required for financial transaction from your bank account.
- Cyber criminals get a blank SIM card from a retailer, who is also a gang member.
- Cyber criminals call the victim pretending a customer care executive of a TSP, to initiate 4G SIM upgradation by themselves otherwise services of their SIM will get blocked.
- In furtherance of their fraud, cyber criminals provide one SIM no. & ask the victim to send that SIM no. through SMS to customer care number to avail the services.
- Victim forwards the SIM no. from his mobile phone considering the fraudster as genuine customer care operator of the TSP.
- Now, the cybercriminal is able to access all the bank account details linked to the victim's mobile number and withdraws the money.
- The TSP closes the services of the victim's old SIM and issues the victim's mobile number to the blank SIM card.

Precaution:

- Never share any information related to your account and SIM over a phone call. The 20-digit SIM number mentioned on the back of the SIM is a very sensitive data.
- If your mobile number is inactive/out of range for a few hours, enquire from your mobile operator immediately.

'Sahakar Sarita', Panchnath Road, Rajkot - 360 001 (Gujarat)
0281 - 2234454 / 2224120 Fax: 0281 - 2236682 info@rajbank.in rajbank.net

General Cyber Safety Points

- Keep your antivirus and operating system updated at all times.
- Back up your sensitive/important data at regular intervals.
- Be careful while opening suspicious web links/URLs.
- Always scan external storage devices (e.g., USB) for viruses, while connecting to your device.
- To prevent unauthorized access to your device, consider activating your wireless router's MAC address filter to allow authorized devices only, Wireless router can screen the MAC addresses of all devices connected to it, and users can set their wireless network to accept connections only from devices with MAC addresses recognized by the router.
- Secure all your wireless access points with a strong password.
- Hackers usually scan for open access points and may misuse them to carry out unwanted activities. Log records may make you more vulnerable to such misuse.
- Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your device.
- File Shredder Software should be used to delete sensitive files on computers. Delete unwanted files or data from your computer device. It prevents unauthorized access to such data by others.
- Use 'Non-Administrator Account' or Standard Account privileges for login to the computer and avoid accessing with administrator privileges for day-to-day usage of computers.
- Make sure to install reputed mobile anti-virus protection to protect your mobile from prevalent cyberthreats and also keep it updated.
- In case of loss or theft of your mobile device, immediately get your SIM deactivated and change passwords of all your accounts, which were configured on that mobile.
- Do not leave your phone unattended in public places and refrain from sharing your phone password/ pattern lock with anybody.
- Never use or access public wi-fi networks & public charger ports.
- Never saved passwords in browsers.
- Always enable a password on the home screen to restrict unauthorized access to your mobile phone. Configure your device to automatically lock beyond a particular duration.
- Always lock your computer before leaving your workplace to prevent unauthorized access. A user can lock one's computer by pressing ‘Ctrl +Alt + Del' and choosing lock this Computer.