



Baroda Rajasthan Kshetriya Gramin Bank

Head Office : Ajmer

Anti-Phishing Policy - 2015

Head Office : Plot No-2343, 2nd Floor, Anasagar Circular Road, Vaishali Nagar, Ajmer - 305 004
Phone : 0145-2642603, 2642621, 3297501 Fax:0145-2642603 e-mail: ho@barodarajasthanrrb.co.in



Anti-Phishing Policy - 2015

Version 1.0

1. Introduction

1.1 Social Engineering

Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. A person using social engineering might try to gain the confidence of an authorized user and get them to reveal information that compromised the network's or application's security. The Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might call customer or employee with some kind of urgent problem that require your password or access right. Virus writers use social engineering tactics to persuade people to run malware hidden email attachments, phishers use social engineering tactics to convince people to divulge sensitive information. In present day scenario social engineering will remain the greatest threat to any security system. Prevention of social engineering includes educating people about the value of information, training them to protect it, and increasing people's awareness of how social engineers operate. Major types of social engineering techniques are:-

1.1.1 Phishing

Phishing attack is a technique, largely used by hackers, who fraudulently acquire sensitive information through the Internet by using false links which might appear to be genuine, though not so. The term was derived after intruders began "fishing" for accounts and sensitive information from unsuspecting Internet users, in disguise. "Phishing" involves the use of e-mails to trick the customer into providing his/her personal details. These e-mails are designed to trick the customer into providing his / her personal and banking information. In other words Phishing e-mails point recipients to a bogus (or "spoofed") internet banking website that looks like bank's legitimate website. Their aim is to trick users into divulging their user IDs, Passwords and other confidential information.

1.1.2 "Vishing"

"**Vishing**" is a combination of the words **Voice** and **Phishing**. "**Vishing**" is very similar to phishing—the only difference is the technology. "Phishing" involves the

	Anti-Phishing Policy - 2015	Version 1.0
---	------------------------------------	-------------

use of e-mails to trick the customer into providing his/her personal details whereas “vishing” involves voice or telephone services. If a customer uses a [Voice over Internet Protocol](#) (VoIP) phone service, he/she is particularly vulnerable to a “vishing” fraud. A typical “vishing” call involves a culprit, posing as an employee from the bank or another organization, claiming to need personal details.

1.1.3 “Smishing”

Smishing is a combination of the words SMS and phishing. “Smishing” is very similar to phishing—the only difference is the technology. Phishing involves the use of e-mails to trick the customer into providing his/her personal details, whereas “smishing” involves mobile phones/SMS messages. Use of mobile phones is fast growing and so is the M-Commerce. If the customer uses mobile phone for purchasing goods, services and convenient banking, he/ she could be more vulnerable to a “mishing” fraud. A typical mishing call or message involves a fraudster, posing as an employee from the bank claiming to need customer’s personal details.

1.2 Cloning

The fraudster will ask the debit card customer that the ATM machine is not working and they need to swipe the card on their machine. After the customer hand over them his card they will swipe card in their machine and when customer is busy putting in his PIN code they swipe it again on a card recorder. The fraudster also capture the PIN code as customer type it in the machine.

The card recorder can then be used to make a duplicate debit card that can be used at any ATM machine. This method is by far the most popular because it is virtually impossible to trace the offender. The criminal can slowly take the money out of customer’s account over time without even knowing it. Most people don't find out they are being robbed until they receive their bank statement or SMS alert. By then the criminal would have made off with everything

1.3 Skimming

For ATM skimming, a fraudster attaches a skimming device over the card entry slot at ATM to capture customer’s card details, and a pinhole camera above the keypad or to the side of the keypad to capture his PIN. Skimmer will copy his account details from the magnetic strip on your debit card. The fraudster will



Anti-Phishing Policy - 2015

Version 1.0

then use his details to create a fake or 'cloned' card to withdraw money from any ATM.

1.4 SIM SWAP frauds

With [mobile phones](#) becoming a convenient tool for Banking, [fraudsters](#) have begun to use SIM-swapping. Using this modus operandi a fraudster obtains victim's bank account details and registers his/her mobile phone number through [phishing](#) or malware. The fraudster approaches victim's mobile service provider with his/her fake identity proof, claiming loss of handset or SIM damage, seeks a duplicate SIM card. Following verification, the original SIM is deactivated and a new one is issued to the fraudster. Fraudster then initiates financial transactions from victim's bank account, details of which he had earlier stolen and receives payment confirmation requests on the duplicate SIM. Since the original SIM has been deactivated, victim remains unaware about the fraudulent transactions made in his account by fraudster.

2. Preamble

The word "Phishing" in this document refers any attempt by a third person to steal customer's identity/ credentials and carry out transactions in their accounts through **any channels other than Branch (internet banking, mobile banking, ATM etc).**

3. Scope of the Policy

The policy covers all operational procedures, rules and guidelines for combating "Phishing" and dealing with "Phishing" induced transactions. This policy is applicable to all domestic customers in India and overseas, all employees of the Bank and third parties engaged by the Bank, including, but not limited to, consultants, contractors and vendors involved in assisting the Bank in its delivery channel operations.

4. Objectives of Anti-Phishing Policy

This document attempts to capture Baroda Rajasthan Kshetriya Gramin Bank's policy with regard to the events related to phishing, smishing, vishing, cloning, skimming etc., risks and mitigating measures to safe guard its customers and employees from various attempts to steal their identity/credentials and carry out transactions in their accounts through online channels. The policy also covers processes/ procedures for handling customer complaints/requests if any of the



Anti-Phishing Policy - 2015

Version 1.0

customers becomes a victim of such identity theft. The policy also elaborates duties and responsibilities of end users of all online channels.

5. Approval/ Review

The policy is required to be approved by the Board and should be reviewed periodically at least once a year or more frequently if need arises. The revised policy will remain in force until further modification / revision as may be advised from time to time.

6. Steps initiated by the Bank to curb phishing

6.1 Internet Banking

To protect our customers from phishing, bank has envisioned multi-layered security solution as detailed below-

6.1.1 First layer – Beneficiary Registration

Beneficiary Registration for the third party fund transfer within and outside bank through Internet Banking has already been implemented. However “beneficiary registration” is not feasible in online bill payment transaction. Therefore the Bank has come up with 2factor authentication (2FA)

6.1.2 Second Layer – 2FA (2factor authentication)

In the second layer of authentication beside User ID/Password and tracker ID customer’s system is validated through “web fort” and transactions are validated through “risk fort” which increased the authentication of sensitive transactions with QnA and OTP. The genuiness of the bank’s website can be verified through the Personal Assurance Message (PAM) also.

6.1.3 Internet Banking User ID and Password

The internet banking user ID and passwords are printed by a centralized operations team in a sealed envelope. The password printing is done with proper physical security features. The user ID and password printed are dispatched to customer/branch through different communication mediums. Bank or its officials will not ask customers to provide their User ID, Password through any mediums such as phone, email etc.

6.1.4 Awareness/ Customer education

Educating customers and sensitizing them against phishing is an ongoing process and will be done periodically by the centralized operations team via SMS, emails and various pop up and ticker messages through bank web sites and internet banking portal.



Anti-Phishing Policy - 2015

Version 1.0

6.2 Mobile Banking (proposed to be implemented shortly)

6.2.1 First layer – Customer Registration

Customer Registration for the mobile banking facility through ATM/ HMBRR menu has been restricted to those mobile numbers only which are registered in customer master records.

6.2.2 Second Layer – 2FA (2factor authentication)

At the time of login into mobile banking application, the mobile banking server identifies not just a customer's application password but also his mobile number. Thus, even if a third person knows the passwords, he will not be able to use mobile banking application through any other mobile. Secondly, for every transactions separate password known as mPin is required.

6.2.3 Application Password and mPin

Application password and mPin are sent directly by the mobile banking server to the registered mobile number of the customer, thus, eliminating the chance of tampering via any manual intervention. These passwords need to be changed mandatorily at the first login.

6.2.4 Awareness/ Customer education

Messages/SMS alerts are sent on a constant basis to the customers to sensitize them about the security measures to be adopted. Branches are advised to educate customers to not provide any sensitive information like registered mobile number, passwords, etc regarding his bank details to any outside person which may lead to misappropriation of his funds.

6.3 ATM/Debit Card

6.3.1 ATM/Debit Card and PIN

The ATM card is made by a centralized team with proper physical security features. The ATM PIN is also printed by centralized team in a sealed envelope and is also done with proper physical security features. The ATM card and PIN printed centrally are dispatched to branch through different couriers .Card and PIN are in possession with two different officers of Bank. Inventory of card and PIN are maintained separately. Identity/ of the customer is confirmed before delivery of card and PIN. Acknowledgement of the customer is taken at the time of delivery of card and PIN. Bank or its officials do not request customers to provide their PIN, Password through any communication mediums such as phone, email etc. The card can be activated at any of the ATMs. The customer is



Anti-Phishing Policy - 2015

Version 1.0

advised to change the PIN immediately on activation of the card. They are further advised not to divulge PIN or password

6.3.2 Usage of Debit Card for Card Not present transactions (CNP)

Customer will be availing the facility through CVV (Card verification value)

Customer will have to register for e-commerce transactions using PIN on internet for creation of Personal assurance message and Password through Debit Cards.

6.3.3 Second Layer – 2FA (2factor authentication)

At the time of login, server identifies the card number expiry date and customer's application password for authentication. Thus, even if a third person knows the expiry date, card number, he will not be able to use as the password is available with the customer only

7.0 Guidelines to deal with phishing related transactions

Bank will be following the below guidelines for dealing with phishing related issues of all online channels (internet banking, mobile banking and ATM etc)

7.1 Guidelines for the branch where phishing debit transaction has taken place

Branches maintaining the account of phishing victim (account in which phishing debit happens) will be following the below guidelines.

7.1.1 No FIR to be lodged by Bank/ Branch for victim

Since the alleged phishing transaction in the customer's account occurred outside the Bank premises, due to the customer's negligence or a fraud played upon the customers, filing of FIR by Bank will not be considered.

7.1.2 Lodgment of complaint with Cyber Cell by victim of phishing

Branches will insist the complainants (victims of phishing induced transactions) to lodge a complaint with the Cyber Cell of Local Police Authorities/ Local police authorities and submit the copy of FIR to the branch, as they have compromised their credentials/ password and suffered loss due to phishing or other similar act.

7.1.3 No promises to the customer to restore the amount phished away:

It will be made very clear to victim (whose a/c has been debited as a result of Phishing attack) that Bank assumes no responsibility to restore the amount. However, the Bank would help him/her, by providing the details/logs of transaction.



Anti-Phishing Policy - 2015

Version 1.0

The complainant will be advised for giving his grievances in writing describing full facts. The branch will acknowledge the receipt of such complaint. Draft Reply to be given to such client; When a client lodges a complaint to Bank informing/refuting/challenging the Debits to his/her account, then after verifying the facts, the branches may, in close consultation with Regional Office, reply to him/her as per DRAFT (APPENDIX-I).

There are also instances, when the complainant is denying/hiding the fact that he had ever responded to such Phishing mail and has not clicked on any such websites and has not compromised the password etc.

7.1.4 Other precautions/ actions to be taken by the branches where fraudulent debit has taken place

- No fraud to be reported as the transactions is done using valid credentials.
- Take necessary steps to block online facility the customer from the concerned team/contact centre.
- Contact the beneficiary branch immediately and arrange to earmark the amount in beneficiary account.

7.1.5 Bank assumes no responsibility to restore the money:

In all phishing or identity theft cases the customer has authorized the transactions or wilfully or obediently compromised/ revealed the credentials/ password to others and hence bank does not take any responsibility of such phishing transactions.

7.1.6 Victim account will be immediately blocked from any further misuse:

- The debit originated Branch (victim's branch) comes to know the incident by way of complaint from the victim (customer) or any other means will immediately:-
 - Inform the centralized team/contact centre to block the online channel facility given to customer.
 - Debit freeze the victim's account till the time branch get confirmation from the centralized team that the online facility given to the victim is blocked.



Anti-Phishing Policy - 2015

Version 1.0

- Inform the Branch where credits have been received by phone/email etc under advice to their Regional Office, centralised online channel team so that the credit receiving Branch gets alerted and freezes the account for subsequent debits.

7.1.7 Continuing with the online channel facility:

The customer (Complainant) will abide by any decision of the Bank in respect of withdrawing the online facility. Bank will recommend closing the account since all the details and confidential information related to the account is already known to the phisher. However customer will be allowed to continue with the same account(s) after obtaining written request. Customer will be further asked to change the credentials immediately-if desires to continue using the online channel facility through which he/she has become victim of phishing.

7.1.8 Victim (customer) will be advised to lodge complaint with Police/Cyber Crime Branch Police:

Bank will advise the customer to lodge an FIR with the Police/Cyber crime Branch of police to conduct investigation on this matter.

7.1.9 Facilitating investigation by Police or CYBER CRIME Branch of police

As per Section 80 of the Information Technology Act, an officer “*not below the rank of Dy. S.P.*” is competent to investigate and demand from Bank other related information. When such notice is received, the Branch should immediately contact their Regional office seeking further guidance.

7.2 Guidelines for the branches where credit transaction has taken place

Branches maintaining the account of phishing beneficiary (account in which phishing credit goes) will be following the below guidelines.

7.2.1 Beneficiary account will be immediately debit freezed:

- The beneficiary branch (Branch in which phishing credit goes) will come to know the incident by way of complaint from the victim's branch (customer whose account is debited) or through any other means will immediately:-



Anti-Phishing Policy - 2015

Version 1.0

- Debit freeze the beneficiary account and inform the beneficiary about the incident.
- The account will be in “debit freeze” status till the time the beneficiary branch gets confirmation from the account holder that the phishing credits in his account does not belongs to him/her.

7.2.2 If the phishing credit goes to online bill payment service providers.

Many phishers or fraudsters use online bill payment services instead of transferring the amount to a beneficiary account. In such cases the credit leg of the phishing transaction will fall on the pooling account maintained by the online service provider. The pooling account of online bill payment service provider cannot be debit frozen as the service provider is not the real beneficiary for this transaction. Most of the online bill payment transactions are instantaneous and there is a high probability that the services were already utilized by the originator of the transaction. In such cases, upon receipt of complaint from victim or victim’s branch or through any other means, the concerned centralized online channel team will contact the concerned service provider and request to stop the transaction/ reverse the transaction to the customer account if the services were not utilized by the beneficiary.

7.2.3 Guidelines to restore the amount lying in beneficiary account:

Given below are the guidelines for restoring the amount lying in the beneficiary account to the victims account.

- The victim of the phishing/complainant has to file an FIR with the local police/ cyber cell of the local police (as per para 7.1.8) The victim’s branch will obtain the copy of FIR from the victim.
- **Beneficiary is available/traceable:** After filing FIR by the victim and obtaining copy of the same by the victim’s branch, written consent will be obtained from beneficiary (by the branch where beneficiary account is maintained) as per APPENDIX-II. On written request from the base branch of the victim and on confirmation that copy of FIR has been obtained, beneficiary branch will initiate the transaction for credit of the

	Anti-Phishing Policy - 2015	Version 1.0
---	------------------------------------	-------------

amount so debited, back to the account, after satisfying the credentials of the beneficiary and after satisfying with regard to compliance of KYC/ other formalities of account opening, else matter be referred to their Regional Office for guidance.

- **Beneficiary is not available/traceable:** After filing FIR by the victim of Phishing and obtaining copy of the same by the branch maintaining account of the victim, a Registered notice (as per APPENDIX-III) will be sent at the last known address of the beneficiary by the branch where the beneficiary's account is maintained, after obtaining written request from the base branch with confirmation that FIR has been lodged etc. In case there is no response to the registered notice/ approach through the introducer (record of non-response to be maintained), money may be released to the victim by the beneficiary branch upon receiving approval from the Regional Authority. However, in such cases (where beneficiary is not traceable), base branch of the victim has to obtain an indemnity from the customer as per APPENDIX-IV. Each such case has to be approved by the Regional Manager of the beneficiary branch, after examining circumstances of each case, considering the amount involved, and other aspects such as KYC etc in the beneficiary's account.

 - The beneficiary's branch will lodge a police complaint in case the branch comes to know that beneficiary is absconding or his credentials are doubtful/ fraudulent.

7.3 Reporting of Phishing Transaction

7.3.1 As soon as the phishing incident comes to the knowledge of the branch, details of the incident will immediately reported to the concerned Regional Office /contact centre in the prescribed format (APPENDIX-V) over fax /email with a copy to the Head Office. Branches are also required to furnish the information on status of phishing incidents on monthly basis in the format provided as per APPENDIX-VI.

7.3.2 Branch to make arrangements to collect the CCTV footages from our ATM managed services provider for investigation where cloning/skimming incident is reported by a customer



Anti-Phishing Policy - 2015

Version 1.0

7.4 Precautions to be taken by the Branches in dealing with Phishing related issues.

- No mail will be sent to a customer by personal email id of any staff.
- The branch will lodge a police complaint in case the branch comes to know that beneficiary is absconding or his credentials are doubtful/ fraudulent.
- If any disputed/fraudulent withdrawal is timely detected then CC TV footage will be preserved (wherever CCTV are installed) to help the investigating authorities.

8. Internal Investigation by bank

The bank will be conducting an internal investigation of each phishing incidents reported. Detailed investigation will be done by the Regional office of victim branch as well as beneficiary.

8.1 Investigation – Victim’s Branch

The regional authority of the victim’s branch will conduct an investigation of the matter by deputing a senior officer. The investigation report will be covering the modus operandi adopted by the phisher, statement from the victim, details of phishing transactions (individually), KYC details of victim and other relevant details. The investigation report should be submitted to General Manager within 15 days from the date of reporting phishing incident to Regional Office of victim’s branch.

8.2 Investigation –Beneficiary’s Branch

The regional authority of the beneficiary’s branch will conduct an investigation of the matter by deputing a senior officer. The investigation report will be covering the, statement from the beneficiary, statement from introducer of beneficiary (if applicable), KYC details, Nature of transactions in his account and other relevant details. The investigation report should be submitted to General Manager within 15 days from the date of reporting phishing incident to regional office of beneficiary’s branch.



Anti-Phishing Policy - 2015

Version 1.0

9. Duties and Responsibilities

The below mentioned duties and responsibilities will be assigned to online channel users, branches and centralized administrators of online channel to prevent phishing.

9.1 Role of Centralized administrators of respective Online Channel

- 9.1.1 Responsible for notifying the ORMC/ General Manager about any security relevant events such as phishing transactions, fraudulent sites, emails, or residual risks reported by customers/branches
- 9.1.2 Depending on nature of incidents/modus operandi, RO/HO team initiate customer education about phishing, new features etc over SMS, email etc.
- 9.1.3 Devise a method for secure and prompt delivery of online authentication credential to the end user. The process or method should get approval from ORMC.
- 9.1.4 Decide/modify various parameters for online channel with the approval of ORMC/ General Manager depending on risk/non risk related issues

9.2 Branches

- 9.2.1 It is the duty and responsibility the branch to ensure the online facility given to customer is in accordance with the instruction given by the customer. (Mode of operation/ resolution etc)
- 9.2.2 Preserve the online channel application form given by the customer for future retrieval.
- 9.2.3 Educate customer about phishing / Vishing / Smishing and display customer awareness message in branch premises etc.

9.3 End Users of Online Channel

- 9.3.1 Should not respond to any phishing mail, SMS, phone calls (pretending to be from Bank, RBI etc asking about personal details.
- 9.3.2 Should immediately inform the bank if their mobile phone is deactivated/lost as it may be related to a SIM-SWAP fraud.
- 9.3.3 Should protect their PCs from various viruses by installing latest antivirus software.
- 9.3.4 Should not disclose sign on password, transaction password, tracker ID, OTP, QnA to any website forms/anybody even to bank officials.
- 9.3.5 Should follow the guidelines given by the Bank over SMS,e-mail, website security tips like Dos and Don'ts, Phishing alerts etc.