(A) Fraud Awareness

Internet has revolutionized the way online users can shop and avail services like Online Banking from anywhere, anytime without physical presence. At Online Banking we use Secured Java Applet and Security Gateway technology that provides Triple-DES encryption to protect all your data transmitted over the Internet. From the moment you log-in to the time you log-out, all information is protected by strong end-to-end encryption; i.e. from your PC browser to the Bank's system. This also gives an opportunity for fraudsters to use internet as medium to commit frauds.It is important for online users to be aware of such frauds and protect themselves against them.

(B) Security Tips

Dhanlaxmi Bank has exercised great diligence to ensure confidentiality and security of your accounts. We use several layers of robust security methods including encryption, firewalls and timed log-outs amongst others, to ensure the confidentiality of your personal and financial information. However, the ultimate key to security lies in your possession. Online users should follow basic security tips to protect themselves from falling victims to online frauds.

(C) Security Measures

Protected by the most stringent security systems, our NetBanking allows you to transact over a completely secure medium. All your transactions travel via 128-bit SSL encrypted medium, the highest level of security on the internet. The servers are protected with firewalls that make unauthorized access impossible. Dhanlaxmi Bank has best of the breed security solutions backed with robust processes in place to extend secure NetBanking services to its customers. Each customer is, provided with a NetBanking ID and Password. Your password is generated in such a way that it is only known to you. Here are some additional steps that you as a user can take to ensure that you are taking the necessary precautions.

(A) Fraud Awareness

(A.1) Phishing & Spoofing

Phishing is a modus operandi where in a custom er gets an e-mail that decepti vely claims to be from a particular enterprise (like your Bank) and asking for account sensitive information. Phishing is a spoofed e-mail that closely resembles the Bank notices. The mail aims to convince customers to divulge account sensitive information such as Bank Account Details, Passwords, PINs etc.. These Phishing mails have legitimate -looking URL or an image, which when clicked directs the affected user to the Phishing site where in the account sensitive details are captured. Alternatively, sometimes the customer is asked to download and install "Security" software attached to the spam e-mail and doing so by the customer, the scamster can retrieve all the account related details.

It is advisable to be wary of fraudulent, suspicious or unsolicited emails, links hyperlinks or redirections from non-Dhanlaxmi Bank websites that may display our bank logos or graphics to mislead user into submitting confidential information such as NetBanking I D, password, card numbers, account numbers or other account information. Such e-mails typically cite variety of reasons, including technical reasons, verification reasons or convenient updating of your particulars like billing information and database. Such fraudulent practice is usually referred as "phishing".

Internet has revolutionized the way online users can shop and avail services like NetBanking from anywhere, anytime without physical presence. This also gives an opportunity for fraudsters to use internet as medium to commit frauds. It is important for online users to be aware of such frauds and protect themselves against them.

Scams such as Spoofing and Phishing to commit identity theft are becoming more prevalent. Protecting your personal information from identity theft is a crucial matter and there are many ways the unscrupulous can gain access to such information. Identity theft involves the use of your personal information - such as your name, NetBanking ID, bank account numbers, card number or other identifying information by someone else, to commit fraud or other crimes.

A.1.1 E-mail Phishing - Involves receiving an e-m ail that appears to be from a legitimate company, such as Dhanlaxmi Bank login page. It may even include the company's logo and a link to an Internet address that looks appropriate. This e-mail directs you to link to a website where you are to supply account or personal information. However, simply clicking the link could secretly install software on your computer. The software may infect your computer with a virus or record and transmit everything you type, including Passwords. Additionally, the website you link to may be spoofing the correct Internet site.

A.1.2 Website Spoofing - Involves you trying to visit a website but accidentally keying-in or linking-to a different address. This may lead you to a website that mimics the legitimate site that you were trying to visit. The spoof Internet site may route whatever information you provide to criminals. This can include your account numbers, NetBanking ID, passwords and other personal information. To make spoof site s seem legitimate, criminals may use the logos, graphics, names and code of the real company's site.

(A.2) Money Mules

A.2.1 What are Money Mules?

By phishing or other means of customer identity theft, the fraudster harvests customer NetBanking credentials i.e. NetBanking ID and IPIN(Password) with a motive to transfer money from customer account to another account holder of the same or different bank. The beneficiary account holder is referred as a "Money Mule". The beneficiary becomes accomplice unknowingly by social engineering techniques employed by the fraudster.

A.2.1 How does the Fraudster operate?

Many phishing fraudsters are located overseas. They need a Money Mule to route the money into their country of origin. A Money Mule is someone who receives the illegal funds into his account, withdraws it and sends it to the fraudster after keeping his commission. This may be easy money, but is illegal. Such requests could come to you through emails, advertisements on genuine recruitment web sites, instant messaging / SMS, and advertisements in newspapers and even on social networking websites.

These fraudsters generally operate from across a country other than where the fraud is to be committed to keep themselves away from local law enforcement agencies. They either maintain anonymity or use fictitious identity to commit these frauds. Fraudsters launch their attack using social engineering techniques by contacting the prospective money mules either by sending emails, in chat room s, job search websites or through internet blogs. Fraudsters lure the prospective money mules to share their bank account details by telling them a fake story and convincing them to

receive money in their accounts. Fraudsters also offer a part of their money or commission and persuade them to unknowingly act as money mules.

Fraudsters then transfer money from the bank customer account whose NetBanking ID and IPIN (Password) has been harvested either by means of phishing or through other means of identity theft. Money Mule is then directed by the fraudster to retain commission and transfer balance money either through wire transfer or to an account of another money mule by means of online transfer or cash deposit thereby forming a chain of fraud. Such money transfers would ultimately lead to funds transfer into fraudster's account thereby maintaining anonymity. When such frauds are reported, the money mule s become the target of law enforcement agencies as their bank accounts are used and their identity is established.

A.2.3 How do you protect yourself from becoming a money mule?

The fraudster may cook different stories; however, his motive will be to convince you to share your bank account details, receive money and act as per his directions. Do not respond to email from strangers asking you for your bank account details. For any overseas job offer, confirm the identity and contact details of the company offering the job to you. They may have hosted a company web site to make it look authentic, but there may not exist any company at all in reality. Do not get carried away by attractive offers or prizes.

Follow these Dos and Don'ts:

- Do not be conned by emails offering you a chance to make 'easy money', especially if it is coming from overseas
- Check out the company making you a job offer if any fund transfer to them is involved. Check their contact details to find out if they are genuine
- NEVER share your bank details
- Beware of ads / notices seeking 'UK Representatives' or 'Agents' to act on their behalf for a period of time
- Should you get any suspicious email, IMMEDIATELY forward it to customercare@dhanbank.co.in

(A.3) What are the symptoms of an infected computer?

- Your computer behaves strangely, i.e. in a way that you have not seen before.
- You see unexpected messages or images.
- You hear unexpected sounds, played at random.
- Programs start unexpectedly.
- Your personal firewall tells you that an application has tried to connect to the Internet (and it is not a program that you ran).
- Your friends tell you that they have received e-mail messages from your address and you have not sent them anything.
- Your computer ‘freezes’ frequently, or programs start running slowly.
- You get lots of system error messages.
- The operating system will not load when you start your computer.
- You notice that files or folders have been deleted or changed.
- You notice hard disk access (shown by one of the small flashing lights) when you are not aware of any programs running.
- Your web browser behaves erratically, e.g. you cannot close a browser window.

(A.4) Vishing

"Vishing" or "Voice Phishing" is the act of leveraging a new technology called Voice over Internet Protocol (VoIP) in using the telephone system to falsely claim to be legitimate enterprises in an attempt to scam users into discloses personal information. The victim is contacted by a phishing e-mail directed to a VoIP based telephone number. The user may receive a telephone call from another individual with a spoofed caller ID or a recorded incoming call with a spoofed caller ID directing him or her to a phishing site.

A.4.1 Vishing Operation Procedure

Fraudsters use a spoofed (fraudulent) caller ID matching the identity of a misrepresented organisation and they invite you to punch your telephone information through your telephone keypad. The content of the incoming message is designed to trigger an impulsive reaction from you. It can use upsetting or exciting information, demand an urgent response or use a false pretense. Any of the personal information such as bank account number, credit card number, PIN etc should not be typed in your telephone keypad in response to above mentioned calls. As a customer, you also have a role in stopping Vishing scams. You are encouraged to recognize it, report it and stop it. Do not react immediately without thinking.

(B) Security Tips

B.1 Do not store your NetBanking ID/PIN in the browsers

Remember to disable your auto-complete function on your browser, as this will make your NetBanking ID & password automatically available to anyone having access to your system. To turn this function off in MS Internet Explorer browser,

- Click the Tools menu,
- Click "Internet Options",
- Click the "Content" tab,
- and click the "AutoComplete" button.
- Then disable the "User names and passwords on forms".

B.2 Verify the integrity of the website

Before performing NetBanking transactions, make sure that the Bank website you access is genuine. Always login Dhanlaxmi Online through the hyperlinks in Dhanlaxmi Bank's websites: www.dhanabank.com when you want to perform NetBanking transactions. Do not login NetBanking through hyperlinks embedded in emails or third party websites.

- If you are using Internet Explorer - Double click the "padlock" icon at the bottom right corner of the screen to check the security certificate of Online NetBanking.

- If you are using Netscape Navigator: - Click "Security" and click "View Certificate". Check the certificate details of Dhanlaxmi Bank.

B.3 Change Password regularly

Passwords (Login and Transaction) is randomly generated by the system and directly printed on tamper proof media such that it is not accessible by anyone other than the customer. Customer is forced to change his Password such upon first login such that customer is assured that Password is not compromised before delivery. Password is stored

by the Bank by use of encryption technology such that it is not accessible to anyone including the system administrator. Create passwords to protect your computer from unauthorized access. Do not conduct your NetBanking transactions in public or shared computers. If you are using a wireless network or device, you are strongly advised to consult your vendor/service provide to ensure that your network or devices are configured with adequate security settings.

Change your password when you receive it the first time, and thereon regularly. Your passwords should have a minimum of eight characters containing both letters and numbers with a combination of uppercase (CAPITAL LETTERS), lowercase (small letters) and Special Characters – when these are case sensitive. Use passwords that are hard to guess. Avoid real words or those that can be easily identified, such as, name, family name, date of birth, telephone number, pet's name, parent's name etc. Avoid using the same password on different websites. Always use unique passwords for each website. Do not write down your password or store it in your mobile or email. Do not give your password to or share your password with anybody, including the employees of Dhanlaxmi Bank.

Avoid using it when others can observe you. Change your Password regularly (once in 30 days).You can change your Password anytime function available on NetBanking. While entering your NetBanking ID and Password, please ensure that others cannot see your screen and also you are not being observed from behind Change Password immediately if you suspect that it has been revealed.

B.4 Phishing Mails Tips

These emails generally ask for sensitive account information like Usernames, Passwords, Card Numbers over the email. The emails may include content, which is bound to make you react. For example, the email may have content, which would state, "Please click here to update your Account Information in order to keep your "Bank Account Active". Dhanlaxmi Bank will never send such emails. In such cases, always back check with the Bank. Always look on the address bar to ensure that the NetBanking site has https:// in the address link. The Dhanlaxmi Bank internet banking address bar link is https://netbank.dhanbank.in/DBRetilBank

B.4.1 Do not share your account details

Many phishing fraudsters are located overseas. They need a Money Mule to route the money into their country of origin. A Money Mule is someone who receives the illegal funds into his account, withdraws it and sends it to the fraudster after keeping his commission. This may be easy money, but is illegal. Such requests could come to you through emails, advertisements on genuine recruitment web sites.

B.4.2 Protection from Phishing

Unless the e-mail is digitally signed, you can never be 100% sure of its source! .Do not click any links inside an e-mail of which you have the slightest suspicion. Instead use a web browser to reach a particular web address. (Type http://www.dhanbank.com) instead of clicking on the link.

B.4.3 Look for PAD Lock 

Always verify the authenticity of the Bank's NetBanking webpage by checking its URL as https://www.dhanbank.in and the PAD Lock symbol at the bottom corner of the browser before putting in your NetBanking ID and Password. Another indication is a padlock icon at the bottom of the screen, which when clicked, displays a security certificate. After 3 seconds the page will be redirected to www.dhanbank.com

B.5 Email Tips

B.5.1 Do not publish your email ID on Internet

Do not disclose your email ID on websites, chat rooms, and internet blogs or subscribe to mailing lists without having read the privacy policy of these sites. Your email ID could be shared or sold to marketing companies and may land up in the spam databases which become the target for receiving spam emails.

B.5.2 Protect your email box against spam

Spam emails are unsolicited emails sent in large numbers to recipients for sales and marketing or some promotional activities. Do not reply / respond to spam emails as it may lead you to receiving more spam in your email box.

B.5.3 Do not open email attachments in haste

Do not open attachments received from unknown sender or unexpected attachments from known senders. They may contain virus infected files most of the times. Do not click on the links in emails asking for confidential information

B.5.4 Beware of fraudulent emails

You may receive emails well crafted to establish communication with you and lure you into a professional or personal relationship leading to using your Bank account for financial transactions over the internet also known as money laundering. We would like to caution you against the fraudulent emails which claim to have come from the Dhanlaxmi Bank. These emails ask the customer to verify their personal details by clicking on a link and some of them threaten to restrict the NetBanking access or similar such action in case you do not respond.

We would like to re-iterate that as a policy we do not ask for the following details from our customers through emails: Card number, Customer Identification Number, Account Number, NetBanking Password and ATM PIN (Personal Identification Number). Internet Banking is a safe way to manage your money. However, there are Internet Fraudsters a round who will try to gain access to your accounts by E-mailing you and prompting you to disclose your on-line banking security details to them. Banks will never send E-mails that ask for confidential information. If you receive an E-mail requesting your Internet Banking security details, you should not respond.

How do fraudulent emails work? -

Typically you will receive an E-mail claiming to be from your bank, either requesting your security details (perhaps as part of an update or confirmation process) or asking you to follow a link to a site where you will be encouraged to provide a range of information such as your credit card number, personal identification number (PIN), passwords or personal information, such as mother's maiden name. Clicking on the link then takes you to a fake website, designed to look like that of your bank, but operated by the Fraudster. Fraudulent E-mails and websites can be very convincing and Fraudsters are continually inventing new approaches to get you to divulge your security details.

B.5.5 Report it

Do not be conned by emails offering you a chance to make ‘easy money’’, especially if it is coming from overseas. Check out the company making you a job offer if any fund transfer to them is involved. Check their contact details to find out if they are genuine. NEVER share your bank details. Beware of ads/notices seeking ‘Representatives’ or ‘Agents’ to act on their behalf for a period of time. Should you get any suspicious email, IMMEDIATELY forward it to customercare@dhanbank.co.in

What to do if you have accidentally revealed password/PIN/TIN etc:

- If you feel t hat you have been phished or you have provided your personal information at a place you should not have, please carry out following immediately as a damage mitigation measure.
- Change your password immediately. If you use the same password at other sites, we Suggest you to change your passwords there, too.
- Report to the bank – customercare@dhanbank.co.in
- Check your account statement and ensure that it is correct in every respect.
- Report any erroneous entries to Bank.

B.6 Online Shopping / Payment security Tips

1. Always shop or make payments through trusted / reputed websites and add those to favorites if you use them regularly.
2. Ensure that the URL of the website is correct by verifying it in the address bar of your computer browser.
3. Do not click on links in emails or on referral websites to visit the online shopping site.
4. Always type the URL in the address bar of the browser to visit the website.
5. Do not enter your confidential account information such as card numbers, expiry date, cvv values, etc on any pop-up windows.
6. If you are a frequent online shopper, signup for Verify by Visa and Master Card secure code program.
7. Check for PAD LOCK symbol on the webpage before furnishing your payments.
8. Make note of the transaction IDs for future reference incase of disputes.
9. Check your account statements regularly and bring any fraudulent transaction to the notice of Bank.
10. Do not respond to any emails seeking your confidential account information that try to lure you with offers, jobs or prizes etc.

B.7 Internet Browsing Tips

B.7.1 Internet Browsing Security

You must observe click discipline while browsing through different websites. You may land up clicking on to malicious link that could download malicious code / software or virus on to your computer.

B.7.2 Do not download software from non trustworthy sites

Downloading software from non-trustworthy sites may lead to infecting your computer with virus. Users should particularly be careful of downloading freeware, which may have Trojans installed that would transmit your confidential information to a hacker or fraudster without your knowledge.

B.7.3 Read privacy policy of the website

Make sure that you read the privacy policy of the website before parting with any personal information such as name, email id, contact number, etc and be aware of how your information would be used by the website owner.

B.8 Log out always properly

Always log out of NetBanking after using the service or when you will be away from your PC. For security reasons, your login session of Online NetBanking will be terminated if your browser is left idle for a while. Always remember to close the browser application after logging out. Avoid accessing NetBanking through PC's installed in public/open areas, e.g. cyber-cafes or libraries.

B.9 Update your contact information

Always update with your latest personal contact information with Dhanlaxmi Bank. Check your account and transaction history details. Check your last login date and time each time you login to Online NetBanking. Check your account balances and statements regularly to identify any unusual transactions. Contact the Bank immediately if there are suspected accesses or transactions.

B.10 Install virus detection software in your computer

Install industry-recommended firewall and virus detection software to protect against hackers, virus attacks and malicious "Trojan Horse" programs. These security programs can help to increase security and are available at most computer software stores. Update the anti-virus and firewall softwares with security patches or newer versions on regular basis. A Trojan is a program which cannot spread by itself and appears to be a legitimate application but does something harmful on the victim computer OR A Trojan refers to a program that appears to be safe, but hidden inside, is usually something harmful, probably a virus.

- Delete and block junk or chain mails.
- Do not install software or run programs of unknown origin.
- Do not open email attachments from strangers.
- Disable the "File and Printer Sharing" feature on your Operating system.
- Keep your PC updated with the latest anti-virus / anti-spyware software
- Install a personal firewall on your PC to protect your account
- Keep your PC updated with the latest security patches and, most importantly,
- Do not click on links or open attachments in unknown or unsolicited (spam) emails
- Do not to make purchases on unknown sites or sites whose credentials are doubtful

B 11. Risk Mitigation – Do's and Dont's

Do's

- Always logon to a site by typing the proper URL in the address bar.
- Give your user id and password only at the authenticated login page.
- Before providing your user id and password please ensure that the page displayed is an
- https:// page and not an http:// page. Please also look for the lock sign ( ) at the right bottom of the browser and the certificate from the verification authorities.
- Provide your personal details over phone/Internet only if you have initiated a call or session and the counterparty has been duly authenticated by you.
- Please remember that bank would never ask you to verify your account information through an e-mail.

Dont's

- Do not click on any link which has come through e-mail from an unexpected source. It may contain malicious code or could be an attempt to 'Phish'.
- If you get an e-mail that you believe is a phishing attempt, you do not reply to it, click on the links or provide your personal information.
- Do not provide any information on a page which might have come up as a pop-up window.
- Never provide your password over the phone or in response to an unsolicited request over e-mail.

- Always remember that information like password, PIN, TIN, etc are strictly confidential and are not known even to employees/service personnel of the Bank. You should therefore, never divulge such information even if asked for.

(C) Security Measures

C.1 Digital Certificate

The webpage of the Dhanlaxmi Bank's internet banking server is identified by means of a digital certificate provided by Verisign to ensure its customer that they are on the correct site and protect themselves from revealing their confidential account information on some fake website.

C.2 Security Solutions

All banking systems are secured using state-of-the-art security solutions acknowledged world wide viz, firewalls, intrusion detection systems, intrusion prevention systems, anti-malware systems to extend secure banking services to our customers.

C.3 Security Teams

The Bank has robust processes, skilled people and competent service providers who monitor the security of our systems round the clock.

C.4 Login Security

Access to customer's NetBanking account is granted using a NetBanking ID and Password.Without a valid Password corresponding to the NetBanking ID, access to customer account cannot be gained by anyone. The customer's NetBanking service is revoked if not in use by customer for more than 90 days for security.

C.5 Session Security

Access to the customers are provided through a secure webpage that encrypts the session between the customer's computer and the webpage using 128-bit encryption so that the communication between the customer's computers and the webpage cannot be intercepted by anyone over the internet.

C.6 Email Security

Email has been most cost effective and convenient way of communication across the globe. Be aware of security while using Email. Your email ID i s your identity and address on the internet and anyone may reach you from any part of the globe in minimum time and effort. Protect your email id from being misused.Be suspicious of any e-mail with urgent requests for personal financial information. "Phishers" typically include upsetting or exciting (but false) statements to get people to react immediately. Avoid filling out forms in e-mail messages that ask for personal financial information. Communicate such information only via a secure website. Remember, Dhanlaxmi Bank does not send out emails to customers requesting personal, confidential or account information.