NAVI MUMBAI CO-OPERATIVE BANK LTD

Employee Information Security Awareness Training

Objectives

- Help you to identify common information security risks.
- Help you develop good security practices.
- It will also help in dealing with following things
- Passwords
- Social Engineering
- Securing your workstations
- E-mail Risks
- Unauthorized Software

Information Security

- Information security (IS) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions.
- Information security, sometimes shortened to InfoSec, is the practice of defending information. on from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Mis-Use of Information

Information that can be exploited

- Names, phone numbers, email addresses.
- Software and Hardware information.
- Process Information.
- Location Information.
- Projects.
- Work Schedules.
- Comments about employees/boss.

Ways of securing information

Things to be kept in mind.

- Dont discuss past, current or future company business in public areas.
- Dont discuss company issues in public area.
- Dont discuss computer related information publicly, including the types of software and other software you use in the company.

Things to be kept in mind (contd.)

- Talk to your management in case you are not certain about what you can/cant share.
- Remember every outsiders has eyes on your company each detail.
- Remember none of your online activities are anonymous.

Passwords

- Create at least 8 characters password which becomes difficult to guess by any hacker.
- Use special characters or numeric for making your password strong.
- Dont use simple dictionary words, common names, combination of reverse spelling words.
- Create passwords that are easy to remember for you but difficult to guess by others.

Protect your Passwords

- Protect your passwords as you protect your money and credit cards.
- Never share passwords unless authorized by management.
- Technical support personnel do not need your password to resolve problems.
- Passwords for accessing company related systems should be different from passwords of your social sites and shopping sites.

Social Engineering

- Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter.
- Hackers gets information mostly by asking for it.
- Studies have shown that even the best security technology cannot prevent devious acts as well as you can.

Guarding against Social Engineering

- Impersonating
- Dont share your passwords with anyone.
- Be suspicious about the information you have been ask for. In case of doubt ask them to contact management.
- Shoulder Surfing

- Dont let anyone watch you when you type your password.

Guarding against Social Engineering

- Eavesdropping
- Be careful when you discuss your company information specially related to company systems and vulnerabilities.
- Dumpster Diving
- Dont dispose companys information in public trashes.

Information Handling Classification

- Three levels of classification
- Based on risk associated with unauthorized modification, disclosure or loss of information.
- Such information should be protected according to Information Security Guidelines
- Secret serious loss
- Confidential Significant loss
- Internal some loss

Information Handling- Protecting

- Do not share classified information with anyone who is not bank employee.
- Dont leave secret or confidential information unprotected, always secure them.
- Sometimes even unclassified information also needs protection.
- Highly confidential information should be shredded properly.

Securing your Workstation (Desktop)

- Employees must restrict access to workstations when they’re left unattended.
- Properly lock or shut down your computers when it is in no use.
- Whenever you step away from your workstation you should make sure it is secured.

E-mail Risks

- Opening files attached to E-mails.
- Clicking URLs attached in email text.
- Email out of office feature.

Safe Email Practices

- If you receive an Execution Security alerts
- Call your local help desk.
- Never click trust signer or execute once.

- Chain Letters
- Do not pass chain letters.
- Newsletters or Newsgroups
- Use discretion when subscribing to newsletters or newsgroups.

Secure your Mobile Devices

- Never loose control of your device when you are outside or inside the company.
- Follow all remote access requirements if you are connecting remotely to the company network.

Information security - Do's and don'ts

Do:	Don't
• Seek advice from the IT Service Desk if you are unclear about any aspect of information security.	• Disclose your password to anyone. See further information on keeping your password safe.
• Report any loss or suspected loss of data. Find out how to report lost or stolen hardware or data.	• Use a personal email account for conducting Bank. See further information on using bank email.
• Change your password if you have any suspicion that it may have been compromised.	• Undermine or seek to undermine the security of computer systems.
• Ensure that personally owned equipment which has been used to store or process bank data is disposed of securely. See further information on hardware and data disposal.	• Make copies of restricted bank information without permission.
• Encrypt your mobile devices and make sure that restricted information is always encrypted before it's sent to others. See further information on encryption.	• Provide access to bank information or systems to those who are not entitled to access.
• Password protect your personally owned devices. See further information on mobile security.	• Use your password as the password for any other service. See further information on keeping your password safe.
• Keep all of the software on your personally owned devices up to date. See further information on protecting your computer.	• Connect personally owned storage or mobile devices to bank owned equipment if you are a member of staff or a research postgraduate.

Do:	Don't
• Comply with the IT policies. See further information on compliance.	• Send unauthorised bulk email (spam). See the bank emailing policy.
• Be mindful of the risks of using open (unsecured) wifi hotspots or computers in internet cafes, public libraries etc. See further information on working offsite.	• Leave your computers unlocked when left unattended.
• Do assume that Information Security is relevant to you. See the Information security website for comprehensive information on all aspects of information security at the bank.	• Leave hard copies of confidential unattended or unsecured. See further information on paper-based information.

Dos and Don'ts of Information Security Awareness

Computers are indispensable learning tools nowadays, and it is of utmost importance to understand how to secure the computers, the data, and other electronic devices. Below are some tips to help raising the awareness against information leakage and IT security attacks.

1. **General**

   People is the weakest link in information security as in many cases the leakage can be avoided if the person involved can have better knowledge in data protection. Users are recommended to develop information security mindset, build and reinforce good practice through regular updates of information security awareness.

2. **Computer/Data Usage**

Risk	DOs	DON'Ts
○ Loss of data ○ Compromise security policies ○ Misuse of data	○ Be accountable for your IT assets and data ○ Adhere to Policies on Use of IT Services and Resources ○ Use good judgement to protect your data ○ Protect your laptop during trip ○ Ensure sensitive information on the computer screen is not visible to others ○ Protect your user ID and password	○ Don’t store sensitive information in portable device without strong encryption ○ Don’t leave your computer / sensitive documents unlocked ○ Don’t discuss something sensitive in public place. People around you may be listening to your conversation

3. **Surfing Web**

Risk	DOs	DON'Ts
○ Virus ○ Worms ○ Trojan ○ Spyware ○ Malware	○ Validate the website you are accessing ○ Install personal Firewall ○ Be cautious if you are asked for personal information	○ Don't download data from doubtful sources ○ Don't visit untrustworthy sites out of curiosity, or access the URLs provided in those websites

	○ Use encryption to protect sensitive data transmitted over public networks and the Internet ○ Install anti-virus, perform scheduled virus scanning and keep virus signature up-to-date ○ Apply security patching timely ○ Backup your system and data, and store it securely	○ Don't use illegal software and programs ○ Don't download programs without permission of the copyright owner or licensee (e.g. the use of BT software)

4. **Email**

Risk	DOs	DON'Ts
○ Junk mail ○ Spam mail ○ Virus ○ Phishing Email	○ Do scan all email attachments for viruses before opening them ○ Use email filtering software ○ Only give your email address to people you know ○ Use PGP or digital certificate to encrypt emails which contain confidential information; staff can use confidential email ○ Use digital signature to send emails for proving who you are	○ Don't open email attachments from unknown sources ○ Don't send mail bomb, forward or reply to junk email or hoax message ○ Don’t click on links embedded in spam mails ○ Don’t buy things or make charity donations in response to spam email

5. **E-Commerce**

Risk	Dos	DON'Ts
○ Identity theft	○ Check the terms and disclaimers of an e-shopping site before acquiring its service ○ Choose well-known or trustworthy e-shopping sites ○ Check the trustworthiness of the e-commerce website (e.g. checking the SSL certificate)	○ Don’t make any e-shopping transactions using computers in Internet cafe ○ Don't visit untrustworthy sites out of curiosity ○ Don’t use easily-guessed password, such as HKID card number, phone number, date of birth

- Use digital certificate for executive transactions over the web
- Use strong password, and change your password on a regular basis
- Logout immediately after you finished your e-shopping activities
- Retain and review your transaction records
- Use different passwords for bank accounts, university accounts and external accounts
- Don’t share your IDs with others

6. **Public Terminals**

Risk	DOs	DON'Ts
○ Account Access ○ Information Loss	○ Always reboot when starting to use the public PCs ○ Clean up cache files after use	○ Don’t leave without closing all browsers and logging out from the public PCs ○ Don't let others watch over your shoulder while logging in or doing online transactions

7. **How to Secure Your Computer**
   - Patch the system regularly
   - Install security software (e.g. web filtering, anti-Virus, anti-Spam, anti-Spyware, personal firewall etc.)
   - Beware of P2P software (e.g. BT, Foxy, eMule)

Computer Security Do's and Don'ts

DO'S

- Create strong passwords that are at least eight characters long, and including at least a numerical value and a symbol, such as #, to foil password-cracking software. Avoid common words, and never disclose a password online.
- Change your password every ninety days.
- Perform regular backups of important data.
- Create a password for your files in order to protect file sharing activities.
- Physically secure your laptop
- Delete any message that refers to groups or organizations that you are not a part of.
- Download and install software only from online sources you trust.
- Never click on a link from an untrusted source.
- Close windows containing pop-up ads or unexpected warnings by clicking on the "X" button inthe upper most right hand corner of that window, not by clicking within the window.
- Use antivirus software, and update it on a regular basis to recognize the latest threats. Heed ITR security alerts to download antidotes for newly circulating viruses and worms.
- Regularly update your operating system, Web browser, and other major software, using the manufacturers' update features, preferably using the auto update functionality.
- Set Windows or Mac updates to auto-download.
- Save attachments to disk before opening them. McAfee "Auto-Protect" will automatically scan your attachments if you save them to disk.

DON'TS

- Never write down your password. Especially on a Post-It note stuck to your computer!
- Never give out your password to anyone, whether you know them or not.
- Never select the "Remember My Password" option. Many applications do not store them securely.
- Never purchase anything promoted in a spam message. Even if the offer isn't a scam, you are only helping to finance and encourage spam.
- Please refrain from opening an e-mail attachment, even from someone you know well, unless you were expecting it.
- Avoid creating common passwords such as your name, social security, UNI, etcetera.
- Do not leave your laptop unattended, even for a few minutes.
- Never reply to e-mail(s) requesting financial or personal information.
- Avoid opening e-mail(s) or e-mail attachments from an unknown sender.
- Please refrain from clicking on the close button within pop-up ads.
- Under no circumstances should you install or use pirated copies of software.
- Do not install P2P file sharing programs which can illegally download copyrighted material.
- Never set your e-mail program to "auto-open" attachments.