इण्डियन ओवरसीज़ बैंक **INDIAN OVERSEAS BANK**

Beware of Suspicious E-mail Attachments

E-mail attachments are a common source of **VIRUSES/MALWARE.** Attackers typically send these email attachments and provide email content that is sufficiently convincing to get the user to believe it is legitimate communication **(e.g.** subjects as "**swift", "Transfer", "Urgent", "Top Priority", "RBI", and "IMF", "Central Bank**" etc.). Attackers can attach files to email that can install malware capable of destroying data and stealing information.

DON'T open any e-mail attachments that end with .exe, .src, .bat, .com or other executable files that you do not recognize.

DON'T ever click embedded links in messages without hovering your mouse over them.

DON'T "unsubscribe"- It is easier to delete the e-mail than to deal with security risks

DON'T respond or reply to spam in any way. Use the delete button.

ALWAYS make sure that all your attachments are scanned by your antivirus program before you open them.

ALWAYS check the e-mail 'From' field to validate the sender. This 'From' address may be spoofed.

ALWAYS check for so-called 'double extended' scam attachments. A text file named 'safe.txt' is safe, but a file called 'safe.txt.exe' is not

ALWAYS note that www.microsoft.com and support.microsoft.software.com are two different domains.

Chief Information Security Officer
Indian Overseas Bank, Central Office, Chennai