This Advisory is issued in the public interest and to caution the general public against fraudulent activities and misleading advertisements which intend to defraud gullible individuals by sending fraudulent email and messages that attempt to trick you into clicking on malicious links or opening attachments.

Taking advantage of the COVID-19 pandemic, hackers and cyber scammers are sending fraudulent emails/ messages with external links that may reveal your user name and password and can be used to steal sensitive information or attack your bank accounts. These emails/ messages may include approval of new loan at attractive interest rate, repayment links for existing loan, subsidized payment of your existing loan, relaxation in EMI payment etc.

Upon contacting the fraudster, the individual is requested to provide his/her details and may be asked to pay money towards processing fees, charges, application fees, click on the link for repayment etc. This money may be asked to be paid either in cash or into the account of the fraudster. Once the money is paid, the fraudster absconds with the same, leaving the individual with very little recourse for getting it back.

Steps to be taken in case of receipt of any such communication

- Check if the name of Centrum Financial Services Limited (CFSL) is genuine.
- Check whether the address given is genuine.
- Check the e-mail id of the sender. It must end with the registered domain of CFSL e.g. "xyz@centrum.co.in"
- Check whether the bank accounts into which the amount is asked to be credited are in individual names. If yes, it is not a genuine "CFSL" account.
- Check with the local CFSL office or send a mail to info@centrum.co.in to verify whether the email/ message is genuine.

CFSL will never:

- ask for your username or password to access safety information
- never email attachments you did not ask
- never ask you to visit an external link
- charge money to apply for a job, register for a conference, conduct lotteries or offer prizes, grants, certificates or funding through email and text messages.

Beware! Anyone dealing with such hacker/ cyber scammer/ fraudster will be doing so at his/her own risk and CFSL shall not be held responsible for such loss or damage suffered directly or indirectly.