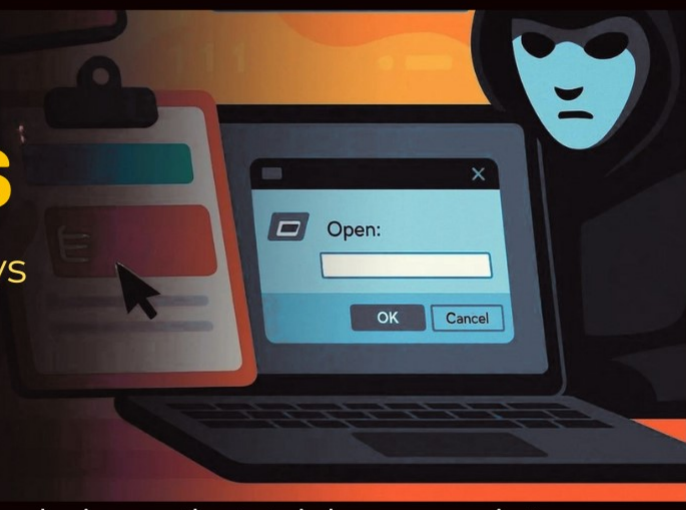
केनरा बैंक
Canara Bank
A Government of India Undertaking
Together We Can

CLICKFIX ATTACKS

"Don't paste to 'fix'— "When a Page Says 'Fix It', Stop & Verify."



The ClickFix attack is a social engineering technique that tricks users into running malicious code on their own computers by disguising the action as a "fix" for a problem, such as a fake CAPTCHA or error message. This method bypasses many traditional security measures because the user is the one who initiates the malicious activity.

What to look out for ?

- Instructions like "**Press Win+R and paste this**" or "**Run this command in your termina**l."
- Pages mimicking Google reCAPTCHA or system dialogs but hosted on suspicious URLs.
- Security warnings that don't match your OS or browser style.
- Unusual URLs — long domains, random characters, or slightly misspelled names.

Don'ts

- **Don't trust "fix" instructions from unknown websites.**
- **Don't ignore browser security warnings.**
- **Don't assume antivirus will stop scripts you execute yourself.**

Do's

- **Pause and verify before copying or running any code.**
- **Check the URL and close suspicious tabs immediately.**
- **Stay informed — learn to recognize fake verification pages**