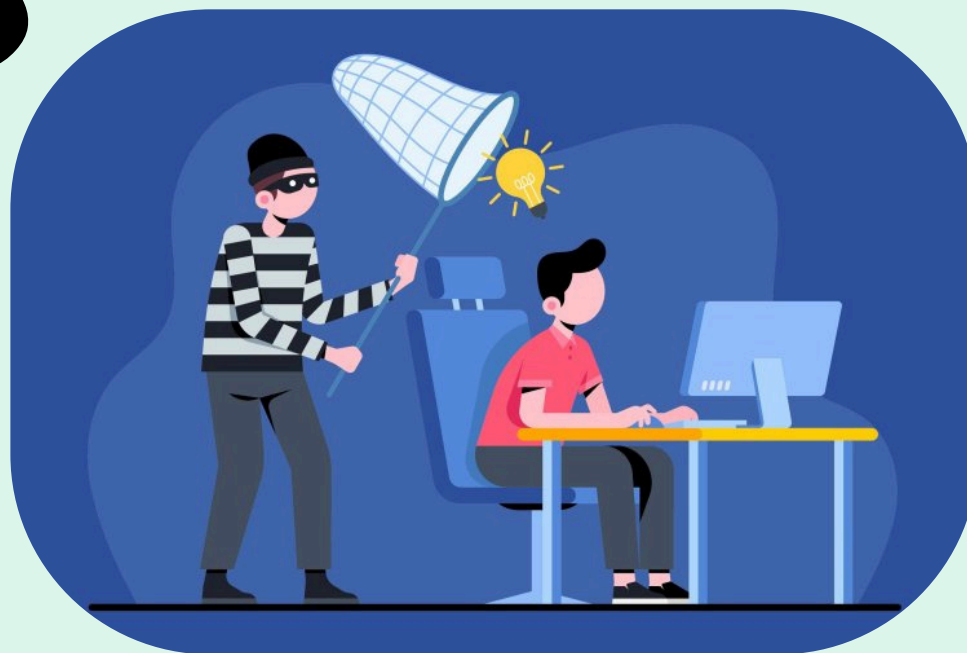




Think Before You Click

One wrong click can cost you your money, data — even your identity.

Cyber Security Awareness



Report suspicious messages to the IT team.

Verify the sender before clicking links or downloading attachments.

Use trusted websites and apps only.

Never share OTPs, CVVs, or PINs — not even with someone claiming to be bank staff.

Don't believe threats like "your account will be frozen today" — real banks don't threaten you like this.

Avoid clicking on shortened links sent through SMS or WhatsApp.

Don't share personal or financial info via unverified communication.

Don't click unknown links in messages, emails, or pop-ups.





GENERAL CYBER SECURITY GUIDELINES



Passwords and privacy settings matter.

- Use complex passwords (8+ characters, with uppercase, lowercase, numbers & symbols)



UPDATE PASSWORDS

- Change passwords at least every 45 days

USE MULTI-FACTOR AUTHENTICATION

- Use multi-factor authentication wherever available

REDUNDANCY

- Don't use the same password across sites

DON'T SAVE PASSWORD

- Don't store passwords in browsers or unsecured files

