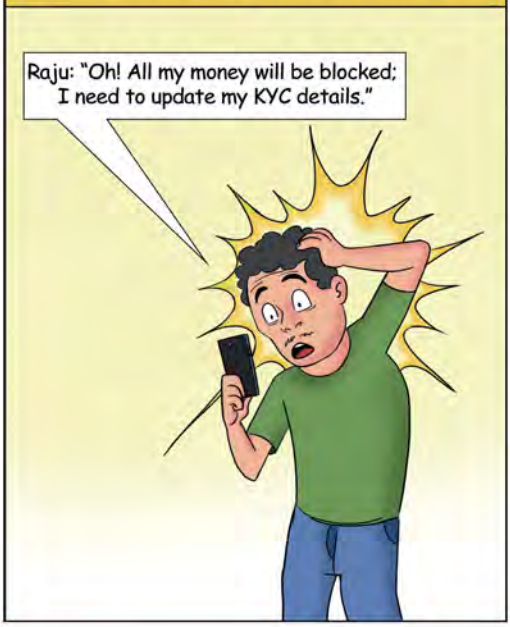
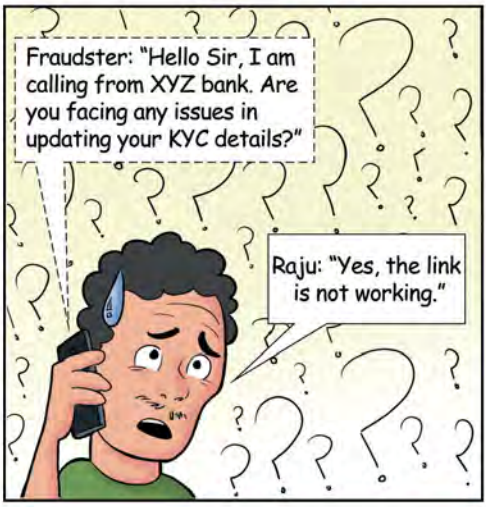
1. FRAUD THROUGH PHISHING LINKS

One day, Raju received message on his phone: *'Dear customer, if your KYC details are not updated within two days, your account will be blocked. Use the below link to update the details at http://updateKYC.XYZbank.com'*

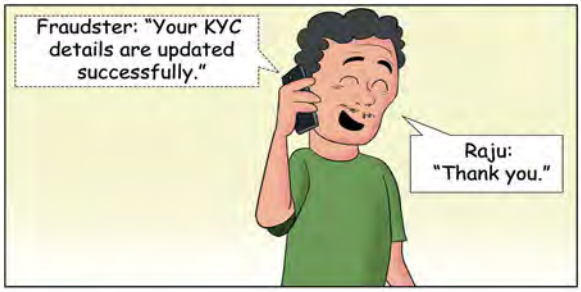


Raju clicked on the link, but the link to update KYC details did not work. Soon, he gets a call.



Do's:

- ✓ Always cross-check the KYC status with your home branch or through your relationship manager when you receive calls, links or SMS from unknown sources requesting you to update KYC.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in



After some time, Raju received SMS alerts on his phone stating that Rs 50,000 was debited from his account.

Raju immediately called the other person, but he didn't answer the calls. Raju realized that the person was a fraudster and he should not have shared any personal details with him.

Don'ts:

× Don't click on unknown/unsolicited links received on the phone/email without verifying it.

× Don't share your confidential details with strangers.