2. ANGLER PHISHING

Attackers pretend to be customer-support accounts on platforms like Twitter, Facebook, or Instagram. They watch for real user complaints and quickly reply with fake “support” messages, sending malicious links or asking for login details to steal accounts.

@ My account bs locked!
@BankSupport why no help?

BankHelp_Official

We can help! Click this secure link to verify:
bit.ly/faklink123

MALWARE

BameSupport ✓

Please DM us for assistance.

Scenario: Maryam Gets a Reply From “Bank Support”

Maryam tweets:

“My banking app isn’t working. Keeps showing an error.”

A support account replies instantly:

“Hello Maryam, we can help.

Please verify your identity here.”

The profile looks real logo, banner, polite tone, but the link leads to a fake bank login page.

Lesson: Always verify support accounts before clicking links.

Official pages never ask you to log in through random links shared in replies.


My banking app ins't working. Keeps showing ain error.
@Bank_Support
Hello Maryam, we can help. Please verify your identity here.
bank.faklink123.com

How Angler Phishing Tricks Employees?

- Fast response creates trust
- Username includes “support” or “helpdesk”
- Copied branding from the real company
- Fake “issue resolution” link that steals credentials

Red Flags Maryam Should Notice

- Account not verified
- Spelling errors in username (e.g., @BankSupp0rt)
- Only a few posts on the profile
- Link doesn’t belong to the official bank website

Prevention Tips

- Only trust verified support accounts
- Never enter credentials on a link from social media
- Check official website for correct support links
- Report fake support profiles immediately