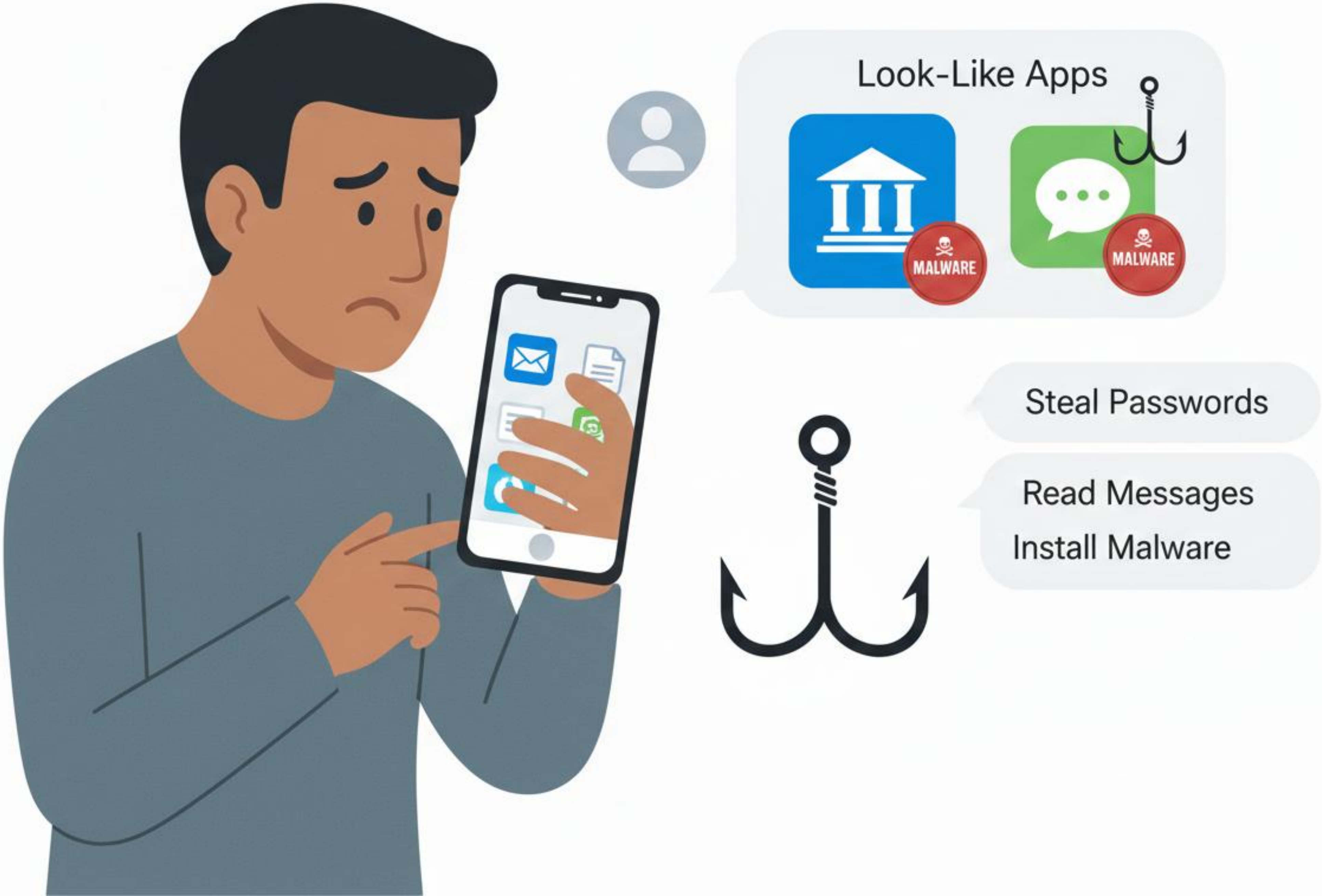
FAKE APPS / APP STORE PHISHING

Attackers create malicious apps that mimic real ones banking apps, email clients, office tools, or system utilities. They use similar names, icons, and interfaces to appear legitimate. Once installed, these apps can steal passwords, read messages, track activity, or silently install additional malware.


Look-Like Apps
MALWARE
MALWARE
Steal Passwords
Read Messages
Install Malware

Scenario: Arham Installs a “SecureMail Fast” App

Arham wants a quick email client for his phone.
He finds “SecureMail Fast – Official” on a random website.
The app logo looks professional,
the screenshots look real… so he installs it.
The app asks for:

- Email password
- Contacts access
- Notification reading

Within minutes, all his emails are forwarded to the attacker.

Lesson: Always download apps from official stores and verify the publisher.
If an app asks for unnecessary permissions, stop immediately, it’s a major red flag.

SecureMail
Fast – Official
Install
□ Email password
☑ Contacts access
□ Notification reading
□ Forward Emails

How Fake Apps Trick Employees?

- Look-alike icons and names
- Fake positive reviews
- Copied screenshots from real apps
- “Recommended by users” banners on shady websites

Red Flags Arham Should Notice

- App not from Google/Apple official store
- Long list of unnecessary permissions
- Unknown developer name
- App has very few downloads

Prevention Tips

- Only install apps from official app stores
- Check developer name and app history
- Avoid apps with extremely low downloads
- Report suspicious apps to IT/security team