2. SMISHING (SMS PHISHING)

Smishing is a form of phishing that uses SMS (text messages) to trick victims.

Attackers send messages containing malicious links, fake alerts, or requests to call a number, aiming to steal personal information, login credentials, or financial data.

Because text messages often appear urgent or personal, victims may act quickly without verifying the source.

SMISHING

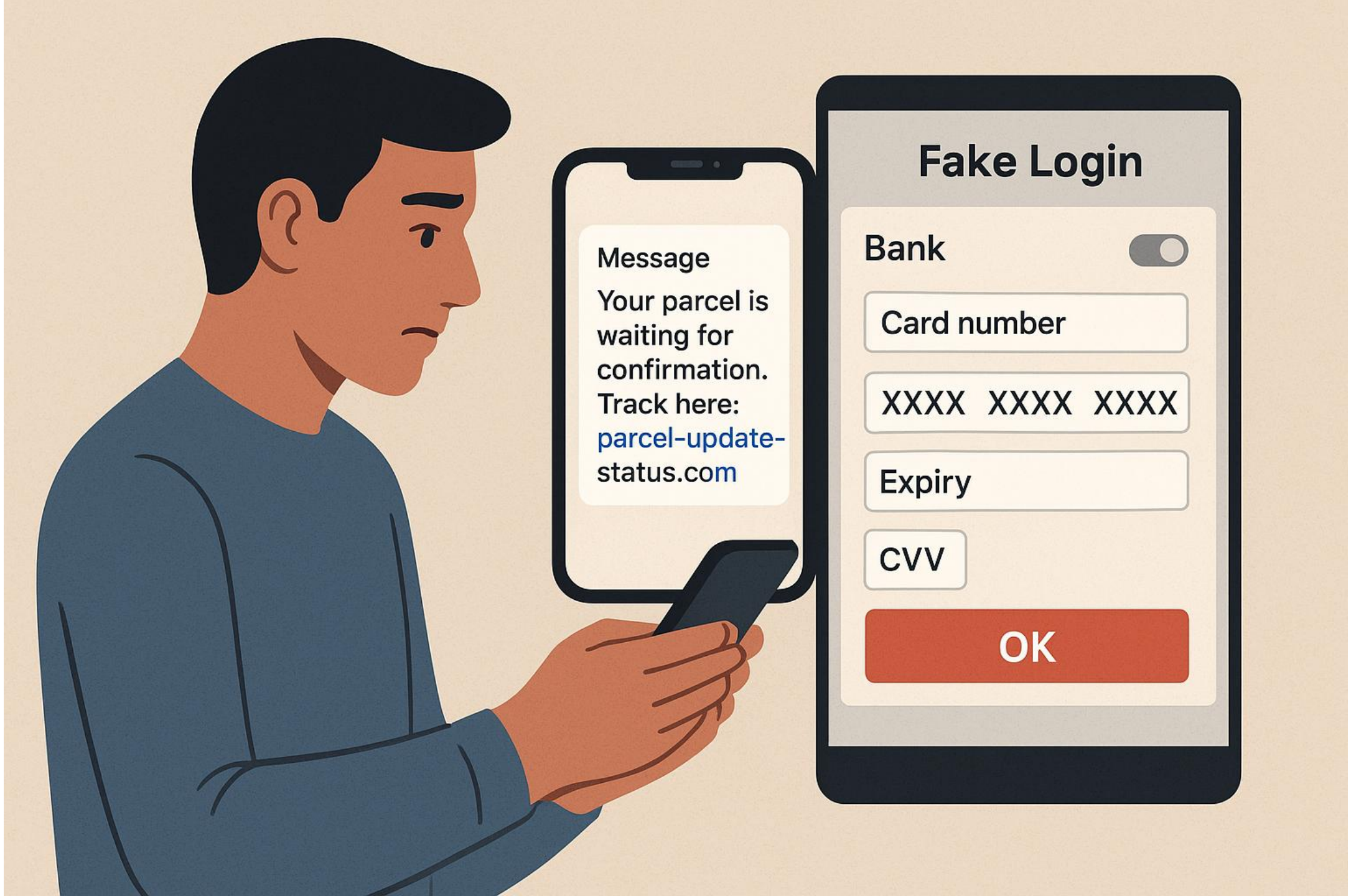
Phishing through SMS with malicious links or callback requests

Scenario: Hassan Gets a “Package Delivery” SMS

Hassan receives a text: “Your parcel is waiting for confirmation. Track here: parcel-update-status.com.”

He clicks the link and is taken to a fake login page that asks for his banking information.

Lesson: Always verify delivery messages through official courier apps or websites and avoid clicking links in unexpected texts.


Message
Your parcel is waiting for confirmation. Track here: parcel-update-status.com
Fake Login
Bank
Card number
XXXX XXXX XXXX
Expiry
CVV
OK

Common Smishing Themes

- Fake banking alerts
- Fake delivery (DHL, TCS, FedEx)
- Mobile wallet promotions
- Payroll/bonus messages

How Attackers Push You?

- Use short, scary messages
- Add fake tracking numbers
- Use “Reply STOP to unsubscribe” (triggers link)

Prevention Tips

- Don’t click links from SMS
- Manually visit official website instead
- Be careful with short URLs (bit.ly)
- Block suspicious senders