SurakshaAI

Fraud Intelligence Report

Report #113 | Profile: general | Generated: 2026-02-22 12:14:33

CRITICAL RISK - 100/100

RISK ASSESSMENT

100 /100

Rule Engine Score	**100**
AI Probability	**6.8%**
Psychology Score	**70**

ORIGINAL MESSAGE

```
Dear customer, your SBI account has been blocked due to KYC expiry.
Share OTP and click http://sbi-kyc-update.in to verify immediately
or account will be permanently closed within 24 hours.
```

PSYCHOLOGICAL TACTICS DETECTED

- **Authority**
- **Fear**
- **Urgency**

SAFETY RECOMMENDATIONS

1. Verify the sender's identity independently. Scammers often pretend to be banks, government departments, or police.
2. Call the organisation's official number (from their website) to confirm any request.
3. Messages with specific time deadlines ('within 6 hours', 'before 5 PM') are designed to create panic. Genuine deadlines are communicated through official channels.
4. If a message gives you a short window to act, step back and verify independently. Scammers use artificial time pressure.
5. Scammers use fear (account blocked, legal action) to cloud your judgement. Verify threats through official channels.
6. No bank or government body will threaten you via SMS or WhatsApp. Always cross-check.
7. Legitimate companies process refunds automatically ? they never ask you to 'confirm account details' to receive a refund.
8. If you receive a message about a failed payment or billing issue, log into the service directly (not via a link) to check.
9. Refund phishing scams often create urgency ('within 6 hours') to pressure you into sharing banking details. Take your time.
10. Never update payment methods through links in emails or messages. Go to the official website or app instead.