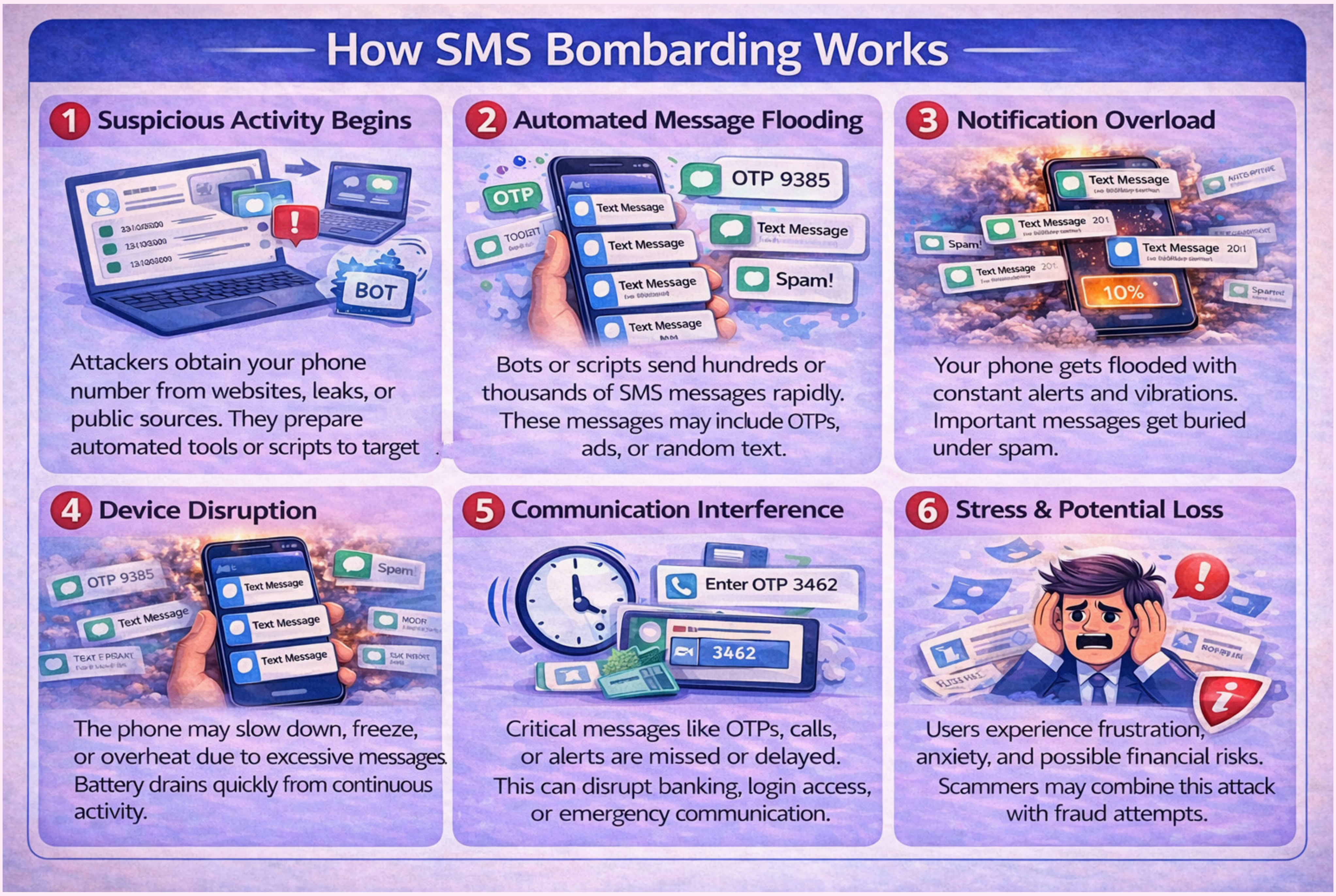
संचार मंत्रालय
MINISTRY OF
COMMUNICATIONS

सत्यमेव जयते

संचार साथी
SANCHAR SAATHI

भारत दूरसंचार
DOT
INDIA TELECOM

Beware of SMS Bombarding



How SMS Bombarding Works

1 Suspicious Activity Begins

Attackers obtain your phone number from websites, leaks, or public sources. They prepare automated tools or scripts to target .

2 Automated Message Flooding

Bots or scripts send hundreds or thousands of SMS messages rapidly. These messages may include OTPs, ads, or random text.

3 Notification Overload

Your phone gets flooded with constant alerts and vibrations. Important messages get buried under spam.

4 Device Disruption

The phone may slow down, freeze, or overheat due to excessive messages. Battery drains quickly from continuous activity.

5 Communication Interference

Critical messages like OTPs, calls, or alerts are missed or delayed. This can disrupt banking, login access, or emergency communication.

6 Stress & Potential Loss

Users experience frustration, anxiety, and possible financial risks. Scammers may combine this attack with fraud attempts.

KEY WARNING SIGNS

- Receiving a flood of spam text messages.
- Device slowing down, freezing or overheating
- Missing Important calls or texts amidst spam
- Don’t share your number on unknown websites

✓ Report suspected fraud at:
www.sancharsaathi.gov.in

✓ If Fraud has occured:
Report at cybercrime.gov.in or call 1930

Sanchar Sathi Mobile App

Download on the App Store

GET IT ON Google Play

Based on Cyber Fraud Trends,
advisory is issued in public interest