LOVELY PROFESSIONAL UNIVERSITY

Graphical Abstract

For

Social Engineering Attacks

Submitted by:

Daniella Esther Melingui Ndiengwasa

Registration Number: 12224313

Section: K22LE

Roll number: 48

Social Engineering Attacks

Manipulating individuals into divulging confidential information (in India)

Organized Sector

- **Industries /Companie**
- **Government / Military**

Common types

-Phishing

-Baiting

-Smishing

Unorganized sector

- **Individuals**
- **Businesses**
- **Social Media**

Reasons

-Human mistake

-Lack of awareness

-Spread to digital space

-Digital Banking

-Resentful employees

Consequences

-Financial loss

-Violation of confidentiality

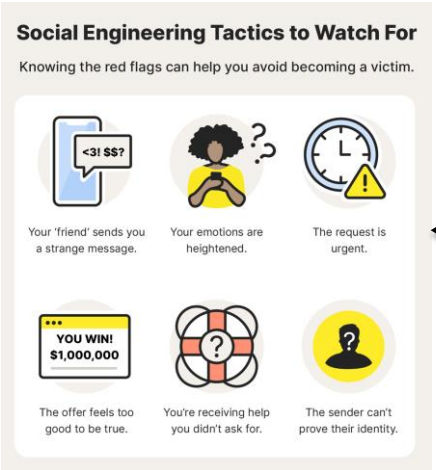
Survey Results

-Over 3,061 attacks on companies per week

-64% of SME's attacked in 2023

-Over 2,084 weekly attacks on government/military

-Over 700 attacks in a year in average company



Solutions

-Spreading awareness

-Utilizing spam filters

-Using sophisticated tools to secure data

-Check and Update security patches

-Multi-factor authentication

-Penetration testing

-Verify email sender's identity

-Report suspicious emails/ messages

Summary of Graphical Abstract

In recent years, India has seen a notable rise in social engineering attacks, driven by the country's increasing internet usage and digital transformation. These attacks leverage psychological tactics to trick individuals into divulging confidential information. According to cyber security data, phishing—the most common social engineering method—has surged by 103% from 2019 to 2023. This increase has had severe financial impacts, with losses estimated at over 12.5 million in 2022 alone, marking a 30% rise from the previous year.

Popular types of social engineering attacks include phishing, pretexting, baiting, whaling, vishing and quid pro quo tactics, which collectively accounted for about 40% of cyber incidents in 2022. Phishing emails were especially prevalent, making up 68% of social engineering-related cases. Additionally, the financial, healthcare, and e-commerce sectors, which are highly lucrative, saw approximately 85% of all attacks.

Mobile usage is also a contributing factor, with mobile-based phishing and smishing (SMS phishing) on the rise. In 2023, it was reported that nearly 57% of these attacks targeted mobile devices—a sharp increase from previous years. Although awareness is slowly growing, only 30% of Indian organizations have implemented thorough social engineering prevention training. This trend underscores the need for enhanced cyber security policies and public education to reduce the nation's exposure to such risks.