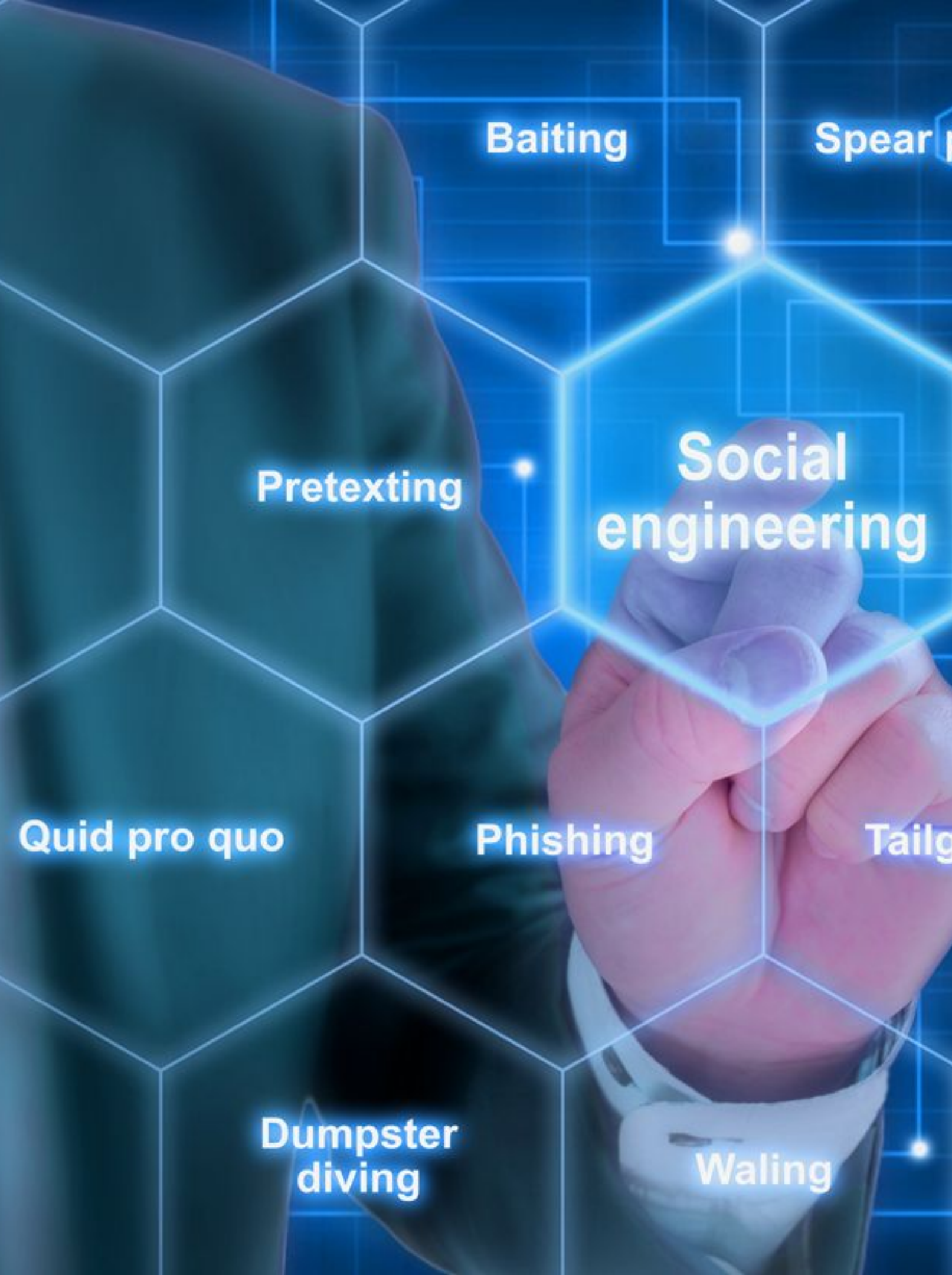




SOCIAL ENGINEERING AND HOW COMPUTERS CAN HELP WITH HUMAN FLAWS

**CLASS: XI A
ROLL NO. : 11121**





SOCIAL ENGINEERING

Social engineering is a deceptive and manipulative tactic used by cybercriminals to exploit human psychology and trust in order to gain unauthorized access to sensitive information, systems, or physical locations. It involves manipulating individuals into performing actions or sharing confidential information that can be used for malicious purposes. Social engineering attacks rely on exploiting human vulnerabilities rather than relying solely on technical weaknesses.

DEFINITION



COMMON TECHNIQUES

TECHNICAL

- Phishing
- Pretexting
- Impersonation
- Tailgating
- Baiting

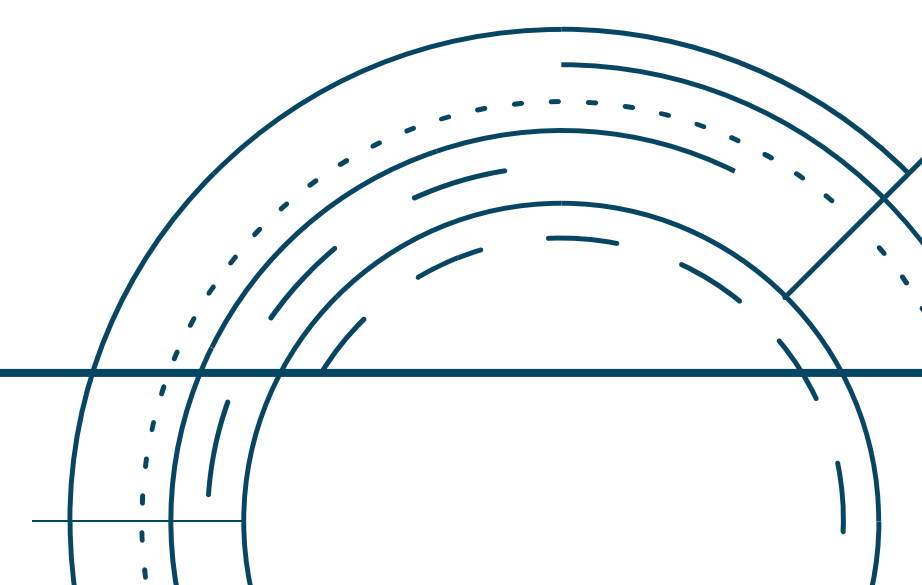
PSYCHOLOGICAL

- Authority
 - Urgency
 - Curiosity
 - Reciprocity
- 



PROBLEM STATEMENT

To understand social engineering,
unearthing its impact on the
impressionable youth of today, while
simultaneously creating an innovative
technological remedy.



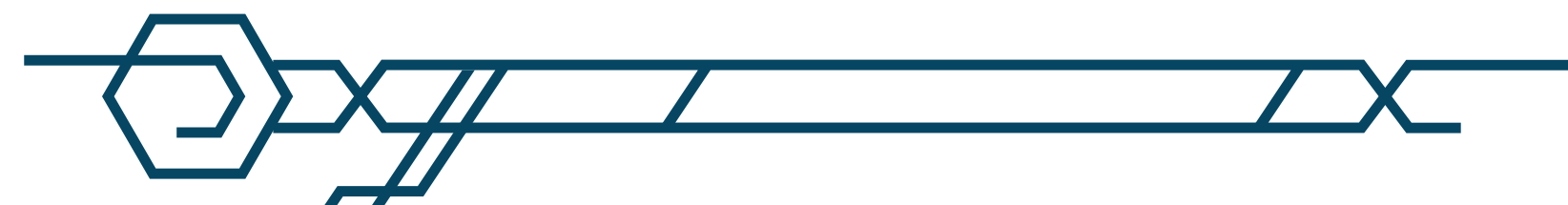


- Unusual or Unexpected Requests
- Sense of Urgency or Fear
- Impersonation or Spoofing
- Requesting Confidential Information
- Unusual Source or Context
- Rewards or Incentives
- Poor Grammar or Spelling
- Trusting Strangers or Unsolicited Contacts



PSYCHOLOGICAL SOLUTIONS TO SOCIAL ENGINEERING

- Education and Awareness Programs
- Critical Thinking and Skepticism
- Emotional Intelligence and Empathy
- Trust Building and Relationship Management
- Mindfulness and Self-Awareness
- Behavior Modification and Reinforcement
- Personal Boundaries and Privacy Protection
- Building Resilient Organizational Cultures



SOME TECHNOLOGICAL SOLUTIONS TO SOCIAL ENGINEERING

- Email Filtering and Anti-Phishing Measures
- Multi-Factor Authentication (MFA)
- User Awareness and Security Training Software
- Secure Communication Channels and Encryption
- Security Information and Event Management (SIEM)
- Continuous Security Updates and Patch Management





DISADVANTAGES OF THE SOLUTIONS

Multi-Factor Authentication (MFA)

- Implementation Complexity
- User Experience and Convenience
- Dependency on Additional Factors

Email Filtering and Anti-Phishing Measures

- False Positives and False Negatives
- Increased Administrative Overhead
- User Friction and Impact on Productivity

User Awareness and Security Training Software

- Cost
- User Engagement
- Lack of Real-World Context

Secure Communication Channels and Encryption

- Complexity and Technical Expertise
- Performance Impact
- User Experience and Adoption

Security Information and Event Management (SIEM)

- Implementation Complexity
- Cost
- Expertise and Training

Continuous Security Updates and Patch Management

- Disruption of System Availability
- Compatibility Issues
- Resource Intensiveness



AI AND BEHAVIORAL ANALYTICS

SOLUTION

- Behavioral analytics focuses on understanding and analyzing human behavior to identify deviations from normal patterns
- AI refers to the simulation of human intelligence in machines, enabling them to perform tasks that typically require human intelligence
- When AI and behavioral analytics are combined, they create a powerful defense mechanism against sophisticated cyber threats.
- AI algorithms can analyze vast amounts of data, including user behavior, network traffic, and system logs, to identify unusual patterns or behaviors that may indicate a security incident.
- Behavioral analytics techniques then come into play, analyzing the identified patterns and anomalies to assess their risk level and determine whether they represent a security threat.