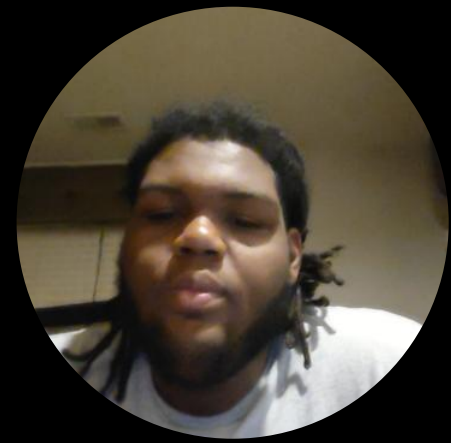
# Cybersecurity and Social Engineering

Understanding the Human Psychology Behind Cyber Attacks

Name: Deonta Carmack

Course: CYSE 201S

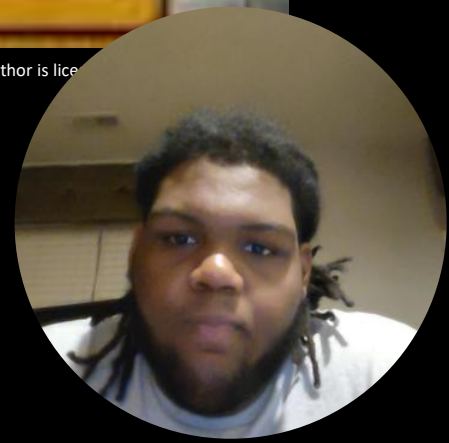




# What Is Social Engineering?

- - Psychological manipulation of individuals
- - Exploits trust, fear, urgency, curiosity
- - Targets people, not systems

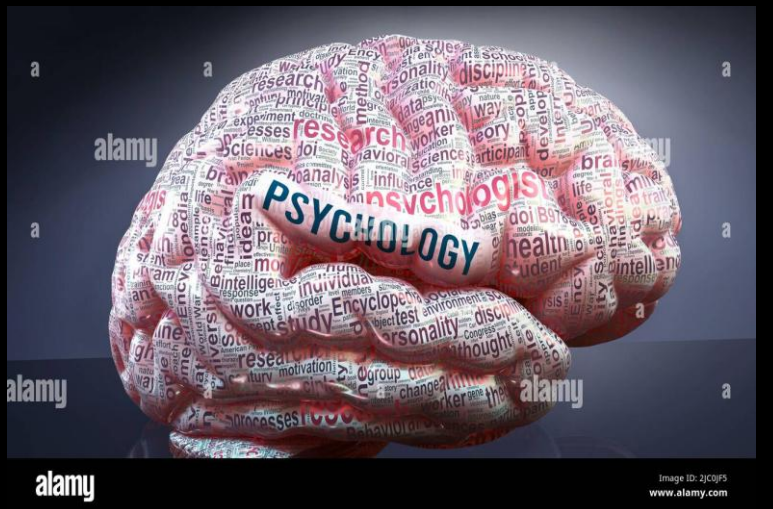


# Why Social Engineering Works

- Psychology Factors:
- - Authority bias
- - Fear and urgency
- - Reciprocity

- Sociology Factors:
- - Social norms
- - Group influence




# Common Social Engineering Attacks

- - Phishing
- - Vishing
- - Smishing
- - Impersonation
- - Pretexting
- - Baiting


# Case Study: 2020 Twitter Bitcoin Scam

- - Attackers used phone-based social engineering
- - Gained access to internal admin tools
- - Hijacked high-profile accounts
- - $118,000 stolen
- - Major trust and reputation damage

# Mitigation Strategies

- Technical Measures:
- - Multi-factor authentication
- - Email filtering
- - Zero-trust security

- Human-Centered Measures:
- - Cybersecurity awareness training
- - Simulated phishing exercises
- - Clear reporting procedures

# Barriers to Implement ation

- - Low digital literacy
- - Overconfidence (“It won’t happen to me”)
- - Limited training resources
- - Rapidly evolving attack methods

# Conclusion

- - Social engineering is a human-centered threat
- - Psychology + sociology explain why attacks succeed
- - Education + technology = strongest defense
- - Cybersecurity must integrate social sciences

# References


- - Mitnick, K. (2011). The Art of Deception.
- - Verizon Data Breach Investigations Report (2023).
- - Twitter Security Incident Report (2020).
- - Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking.
- - NIST Social Engineering Guidelines.