Cybersecurity & Social Engineering

CYSE 201S

Cybersecurity and the Social Sciences

Fatma Ankaya

What Is Social Engineering?

- A cyberattack technique that targets people instead of systems.

- Manipulates human emotions, trust, and behavior.

- Often uses deception to steal information or gain access.

Why Social Engineering Works (Psychology)

- Authority bias – trusting perceived authority.
- Urgency – acting quickly without thinking.
- Fear – responding emotionally.
- Curiosity – clicking unknown links.
- Social influence – following instructions easily.

Common Social Engineering Attacks

- Phishing (email scams)
- Spear phishing (targeted)
- Pretexting (fake stories)
- Baiting (malicious incentives)
- Tailgating (physical access)
- MFA fatigue attacks

Real-World Examples of Social Engineering

- MGM Resorts 2023: Help desk impersonation → system outages.

- Uber 2022: MFA fatigue attack → internal access gained.

- Google & Facebook scam: $100M invoicing fraud.

- CISA 2024: HR and payroll phishing campaigns.

- FBI 2023: $2.9B BEC losses in the U.S.

Societal Impact

- Financial loss to individuals & companies.

- Identity theft & privacy concerns.

- Loss of trust in digital platforms.

- Organizational disruptions.

Prevention & Mitigation

- Employee security awareness training.
- Multi-factor authentication (MFA).
- Email filtering + link scanning.
- Verification of requests (Zero Trust).
- Strong password and identity policies.

References

CISA. (2023). MGM Resorts cybersecurity advisory.

CISA. (2024). Payroll phishing alert.

FBI. (2024). Internet Crime Report 2023.

Bloomberg News. (2023). MGM attack coverage.

The Guardian. (2022). Uber security breach.

U.S. DOJ. (2019). $100M invoice fraud case.