Cybersecurity and Social Engineering

How Attackers Use Human Behavior

Ramzi Alkaifi

CYSE 201S| Diwakar Yalpi | 12/01/25

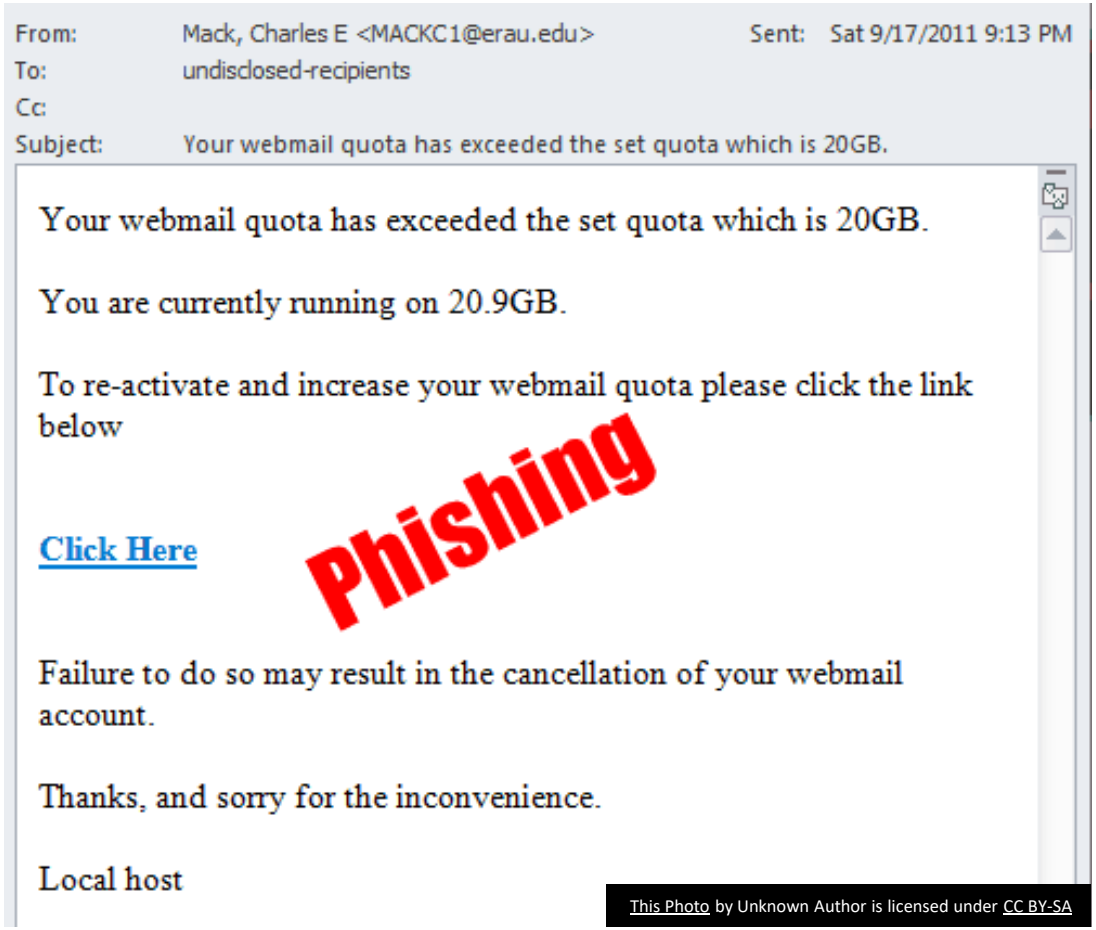
What Is Social Engineering?

- Social engineering is when attackers manipulate people—not computers—to gain access.
- Why it works:

- Exploits trust

- Exploits emotion

- Exploits mental shortcuts



Psychological Principles Behind Attacks

- Key psychological triggers include:
  - Authority bias
  - Urgency pressure
  - Fear of consequences
  - Curiosity
  - Social proof

Social Science Connection

- Social engineering is deeply connected to social sciences:
  - Psychology – persuasion, fear, cognitive biases
  - Sociology – trust, group behavior, organizational culture
  - Behavioral economics – decision-making shortcuts
  - Communication theory – influence and messaging

Real Examples & Why They Worked

- Examples of successful social engineering attacks:
  - Twitter 2020 Breach – Hacker impersonated IT support
  - Target Retail Breach – Vendor phishing exploited trust
  - CEO Email Fraud – Fake authority and urgency

How to Prevent Social Engineering

- Methods to reduce social engineering attacks:
  - Cybersecurity awareness training
  - Verify unusual or urgent requests
  - Use multi-factor authentication
  - Run phishing simulations
  - Adopt a zero-trust mindset

References

- Verizon (2023). Data Breach Investigations Report.
  - Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking.
  - Mitnick, K. (2011). The Art of Deception.
  - CISA (2024). Social Engineering Attack Prevention.
  - FTC (2023). Recognizing Social Engineering Scams.