# The Human Hack:

## Social Engineering & the Psychology of Deception

Dmitriy Yeremin | CYSE201S | 04/22/2026

# What is Social Engineering (SE)?

- Attacks using email, mail, SMS, or phone calls that create false representations of trusted entities (banks, IT support, etc.) to trick victims into revealing sensitive information or clicking malicious links.
- These attacks exploit human psychology and behavioral tendencies — not technical vulnerabilities.
- SE sits at the intersection of cybersecurity and behavioral psychology.

**Human = Weakest Link**

# The Psychology Behind It

## 👑 Authority

Attackers impersonate figures of power — IT help desk, bosses, banks — to bypass skepticism.

## ⚠ Urgency / Fear

Creating time pressure (“act now!”) disables rational thinking and triggers reactive compliance.

## 👥 Social Proof

People follow perceived group behavior — “everyone else is doing it” — lowering individual suspicion.

## ⏳ Scarcity

Limited-time offers or exclusive access create FOMO, pushing victims to act before thinking.

Cialdini’s Principles of Influence (1984)

# Common Tactics With Examples

 **Phishing** 2020 Twitter Bitcoin scam — employees targeted via vishing phone calls

 **Pretexting** Attacker impersonates IT/HR staff to extract login credentials

 **Baiting** Infected USB drives left in parking lots — curiosity does the rest

 **Vishing / Smishing** Voice or SMS phishing — spoofed caller ID from “your bank”

# Real-World Case Study: 2020 Twitter Hack

| 69 | $118K+ | 24 hrs | 3 Phases |
|---|---|---|---|
| High-Profile Accounts | Bitcoin Stolen | Attack Window | SE → Takeover → Scam |

- Hackers called Twitter employees posing as IT Help Desk about a “VPN problem” — a classic vishing attack.
- Remote work (COVID-19) made employees more vulnerable; VPN issues were common and expected.
- Attackers accessed employee Slack channels to learn internal systems and escalate privileges.
- Victims were told: donate Bitcoin to a COVID-19 relief fund and get double back — exploiting urgency and authority.

**No malware, no exploits — just human manipulation.**

(New York State Department of Financial Services, 2020)

# Mitigation Strategies

## Technical

- Email filters & spam detection
- Multi-factor authentication (MFA)
- Hardware security keys
- Access control & least privilege

## Organizational

- Security culture & clear protocols
- Employee verification procedures
- Incident response planning
- Regular security audits

## Individual

- Security awareness training
- Skepticism habits — verify callers
- Slow down under urgency pressure
- Report suspicious contact

**Key Insight: Behavior change is harder than patching software.**

# References


- New York State Department of Financial Services. (2020, October 14). Twitter investigation report: Report on investigation of Twitter's July 15, 2020 cybersecurity incident and the implications for election security. https://www.dfs.ny.gov/Twitter_Report