Cybersecurity and Social Engineering

How attacker use psychology to bypass technology



What is Social Engineering?

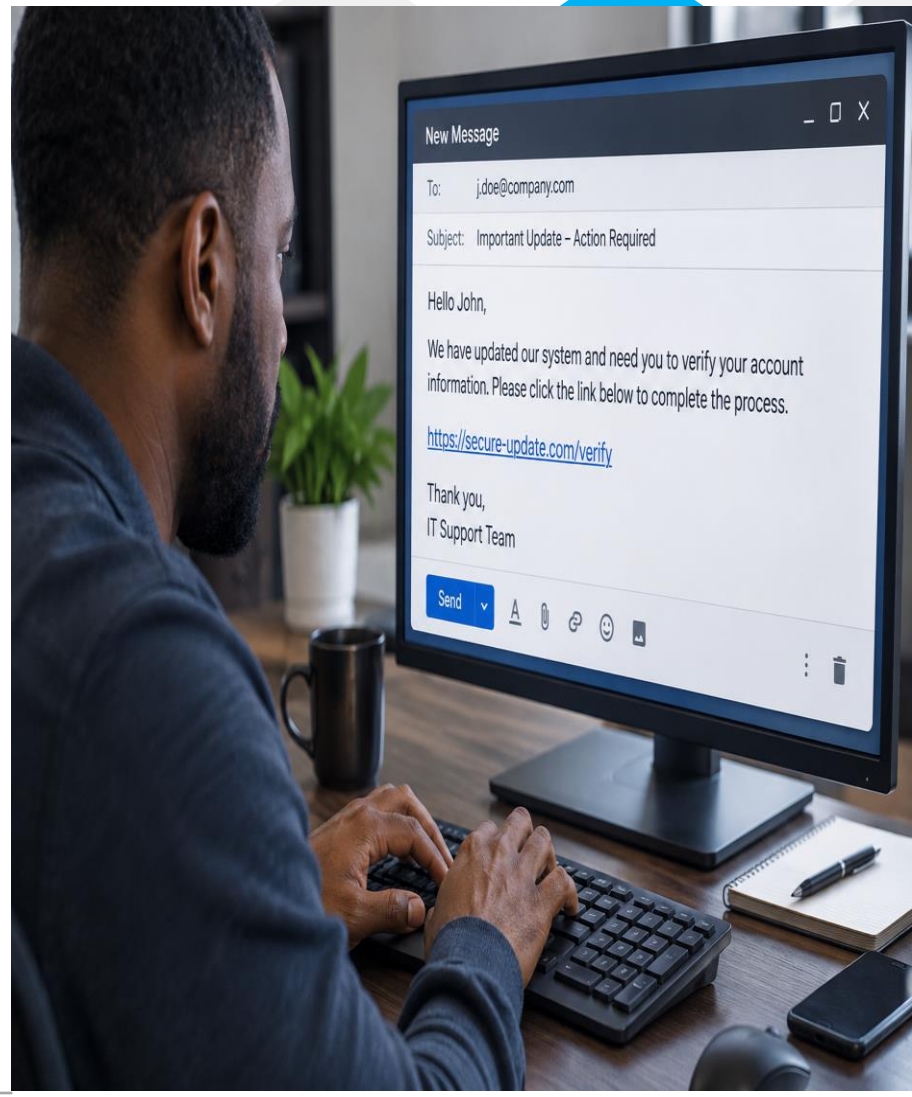
- A cyberattack that uses psychological manipulation instead of hacking alone.
- The attacker tries to make a person share information or take an unsafe action.
- Targets a person’s trust, emotions, authority, and habits.
- Often begins with research from email, social media, company websites, or public records.

Why it works: Psychology

- Fear: Your account will be locked unless you act now.
- Urgency: pressure makes people react before thinking.
- Trust and authority: messages appear to come from a boss, bank, school, or IT staff.
- Curiosity and reward: fake prizes, job offers, or important documents encourage clicks.

Common Social Engineering Tactics

- Phishing: a fake email that looks legitimate.
- Spear phishing: a targeted message aimed at a specific person or department.
- Whaling: spear phishing aimed at executives or high-value employees.
- Pretexting: an attacker creates a fake story or role to gain trust.
- Baiting: an attacker offers a reward, free download, gift card, or USB device.
- Business Email Compromise (BEC): fake or compromised email used for payments or data.



Examples of Social Engineering

- Workplace impersonation: an attacker pretends to be a manager, vendor, coworker, or technician.
- Thread hijacking: an attacker enters a real email conversation and sends a malicious link or payment request.
- Romance or honeytrap scam: a fake identity builds trust, then asks for money, gifts, or information.
- Bangladesh Bank Heist: attackers used phishing and pretexting to gain access and steal funds.
- Social media research: attackers study public profiles to make messages more believable.

Cybersecurity and Social Sciences

- Psychology explains how emotion, trust, bias, and decision-making affect security choices.
- Sociology explains how workplace culture and group norms influence risky behavior.
- Criminology helps explain why offenders manipulate victims and how opportunity affects crime.
- Human factors help design security tools that people can actually use correctly.
- Ethics reminds us to protect people, privacy, and organizations without blaming victims.

How to Reduce the Risk

- Pause before acting on urgent requests.
- Verify identity through a separate trusted channel, such a a known phone number.
- Use multi-factor authentication on important accounts.
- Check email addresses, links, attachments, spelling, and unusual requests.
- Report suspicious messages quickly so others can be protected.
- Practice awareness training with realistic examples, not just rules.



Key Takeaways

- Social engineering succeeds when attackers exploit people, not just systems.
- Common tactics include phishing, spear phishing, pretexting, baiting, whaling, and BEC.
- The strongest defense combines technology, training, verification, reporting, and culture.
- Cybersecurity professionals must understand both networks and human behavior.



References

- Singh, T. (2025). *Cybersecurity, Psychology and People Hacking*. Palgrave Macmillan. Chapters 7-8.

Question?