Cybersecurity & Social Engineering

Ava McLaughlin

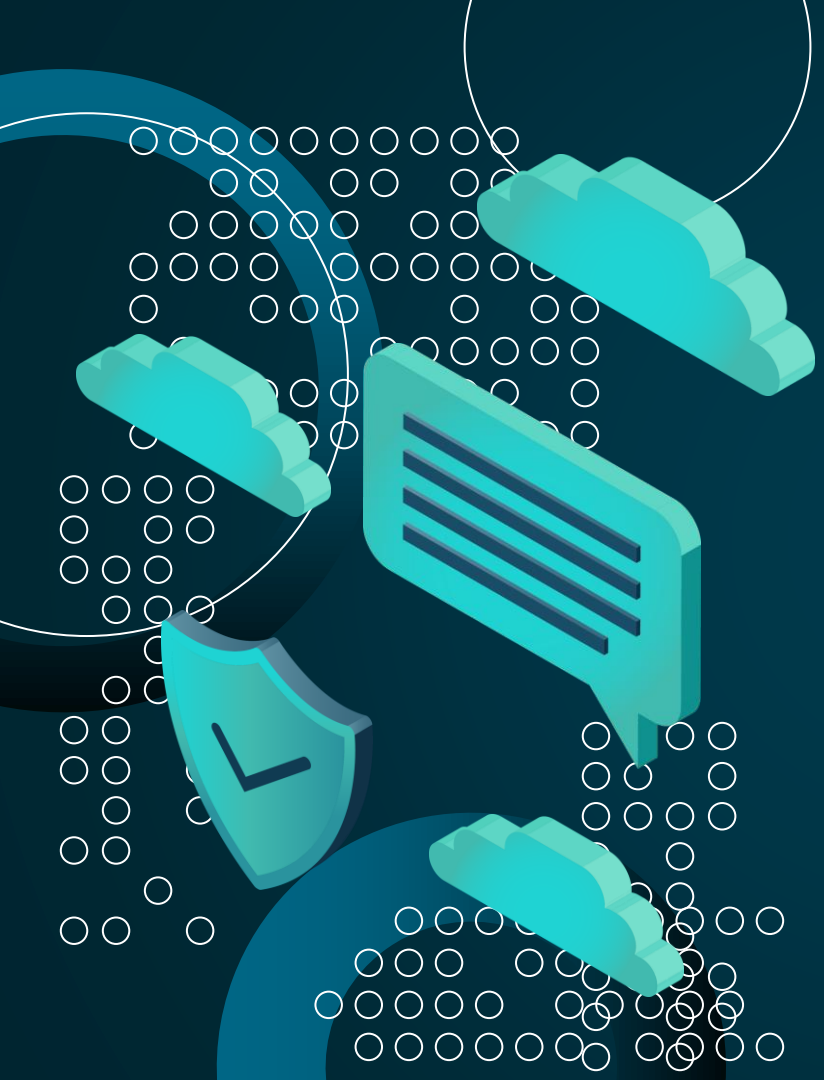
What is Social Engineering?

Social Engineering is the act of manipulating people into revealing confidential information or performing unsafe actions. Attackers often exploit human behavior instead of technical vulnerabilities to compromise cybersecurity.

01

Psychological Factors

Social Engineering is effective because attackers design tactics based on predictable behaviors.



Psychological Factors

Common behaviors that attackers exploit through social engineering include...

01

Trust

People trust familiar or official-looking sources.

02

Curiosity

People are tempted by curiosity & rewards.

03

Fear

Fear causes panic about negative consequences.

04

Urgency

Urgency leads to rushed, unplanned decisions.

02

Social Engineering Tactics

Many types of social engineering attacks target different psychological factors.

Social Engineering Tactics

Common social engineering attacks include...

Phishing

Attackers fake emails, texts, or phone calls to trick people into revealing information or clicking on malicious links.

Pretexting

Attackers create a fake story or identity to gain the trust of a targeted victim.

Baiting

Attackers offer something tempting to get victims to perform unsafe actions.

Quid Pro Quo

Attackers offer a service in exchange for sensitive information.

Scareware

Attackers pressure victims into downloading malware with fake security threats.

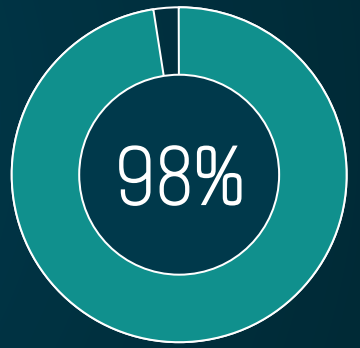
Watering Hole Attacks

Attackers infect a resource that a targeted group frequently accesses.

03

Real-World Examples

Social engineering is extremely common & can happen to anyone.



of cyberattacks rely on social engineering.

Real-World Examples

Some recent cyberattacks driven by social engineering include...

2023

MGM Cyberattack

The Scattered Spider group vished the IT help desk of MGM Resorts by impersonating an employee, resulting in a $100M loss.

2024

$25M Deepfake Scam

A Hong Kong finance professional was deceived by deepfake impersonators on a conference call into transferring $25M.

2025

ClickFix

Fake CAPTCHAs embedded on legitimate websites. The most common initial access method for attackers in 2025.

2026

$285M Drift Hack

A North Korean group used long-term social engineering to gain insider access & steal $285M from Drift Protocol.

04 Mitigation Strategies

Cybersecurity systems must account for human capabilities & limitations in their design.

Mitigation Strategies

Proposed strategies for mitigating social engineering risks include...

01 **Employee Training & Awareness**
Helps employees recognize & resist tactics.

02 **Implementing Multi-Factor Authentication**
Creates an extra layer of protection.

03 **Regular Security Assessments & Penetration Testing**
Identifies vulnerabilities before they're exploited.

04 **Incident Response Planning**
Lessens damages & quickens recovery.

05 **Developing Clear Security Policies**
Defines acceptable behaviors and procedures.

06 **Phishing Simulation Exercises**
Tests awareness without real risks.

Resources

Bonnie, E. (2025, October 29). *85+ Social Engineering Statistics to Know for 2026*. Secureframe. https://secureframe.com/blog/social-engineering-statistics

Cyber Security Kill Chain Presentation. Slidesgo. (n.d.). https://slidesgo.com/theme/cyber-security-kill-chain#position-4&related-1&rs=detail-related

Lakshmanan, R. (2026, April 5). *$285 Million Drift Hack Traced to Six-Month DPRK Social Engineering Operation*. The Hacker News. https://thehackernews.com/2026/04/285-million-drift-hack-traced-to-six.html

Marchand, C. (2025, February 13). *The Psychology of Social Engineering*. Security. https://www.coalitioninc.com/blog/security-labs/the-psychology-of-social-engineering

Microsoft Threat Intelligence, M. D. E. (2025, August 21). *Think before you Click(Fix): Analyzing the CLICKFIX Social Engineering Technique*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/

Old Dominion University. (n.d.). CYSE201S (Module 4) *Cybersecurity and Human Factors*. https://canvas.odu.edu/courses/201835/files/59116295/download?download_frd=1

Resources cont.

PacketWatch Team Sixty43. (2025, December 1). *Cyber Threat Intelligence Report*. PacketWatch. https://packetwatch.com/resources/threat-intel/cyber-threat-intelligence-report-12-01-2025

Rowles, R. (2024, February 13). *The Psychology Behind Social Engineering* . Social Engineer. https://www.social-engineer.com/the-psychology-behind-social-engineering/

Schrader, D. (2025, August 18). *An Overview of the MGM Cyber Attack*. Netwrix. https://netwrix.com/en/resources/blog/mgm-cyber-attack/

Sprocket Security. (2024, December 11). *Social Engineering: 9 Attack Techniques and 6 Defensive Measures*. https://www.sprocketsecurity.com/blog/social-engineering-techniques

Young, K. (2025, August 11). *Cyber Case study: $25 Million Deepfake Scam*. CoverLink Insurance - Ohio Insurance Agency. https://coverlink.com/case-study/case-study-25-million-deepfake-scam/

THANK YOU!

Does anyone have
any questions?