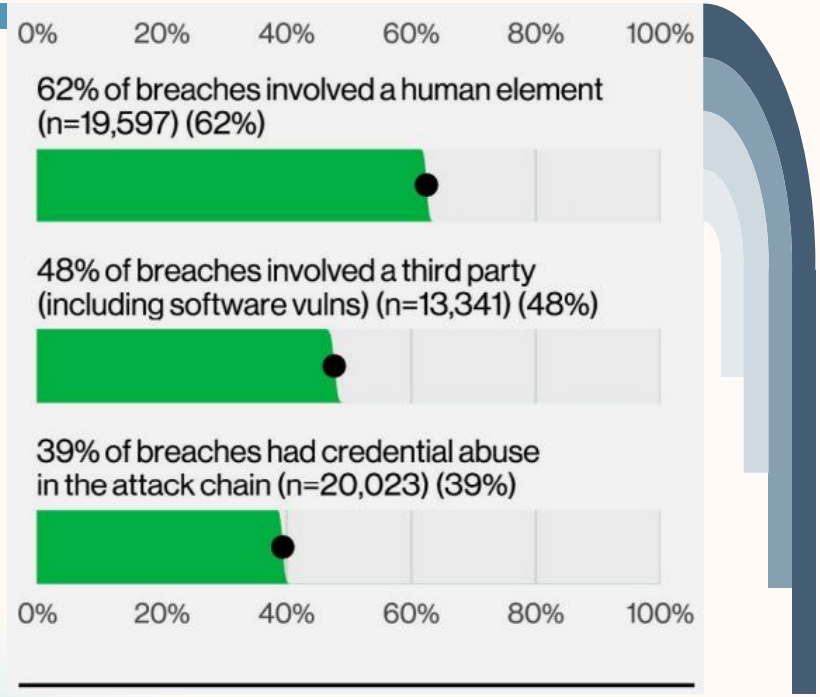
Social Engineering
By: Christopher Doyon

Hacking Humans

Why It Matters



Verizon's 2026 Data breach Investigations Report states that the “Human element was present in 62% of breaches.”

Technically strong security systems will always be vulnerable to the weakest link; humans. Social engineering threats can be accidental, environmental, due to human negligence, or even human failure. The human factor in cybersecurity needs to have the same priority as technical factors.

This is where cybersecurity starts relating to social sciences. Psychology can help us explain why social engineering attacks work and sociology can help us understand how to protect ourselves and our systems from these attacks.

Source: Verizon 2026 DBIR Report

Common Social Engineering Tactics

Phishing

Fake emails can impersonate trusted sources, such as a “bank” or a platform and they can attempt to get you to click a link or provide confidential information. Variants of phishing include
Spear Phishing: targeting specific individuals
Whaling: targeting high profile individuals ex. CEO
Vishing: voice phishing ex. Voicemail or call
Smishing: SMS phishing

Pretexting

An attacker can create a believable scenario or identity such as an IT support technician, a vendor, or a police officer to get information or even physical access. An example could be an attacker impersonating your companies IT department and asking for your login details to “fix a problem.”

Baiting

Baiting exploits a person's curiosity by leaving “bait” such as a USB device or mislabeled file like “confidential” or offering an opportunity to receive something for free. When the USB device is accessed or the file is opened, malware spreads through the computer and system.

Quid Pro Quo

A reward if offered in exchange for access or data. This reward can have monetary value such as a gift card or it can take the form of a service such as free tech support. This social engineering tactic exploits our sense that a favor should be returned.

Source: Singh, Ch. 8; Aldabagh et al. (2025), p. 156; Social Engineering PPT (Diwakar Yalpi)

Real World Cases

Real examples of social engineering attacks causing serious damages

Bangladesh Bank, 2016	$81 Million dollars stolen via fraudulent transfers	Pretexting and Authority
Google and Facebook, 2017	Fake invoices and contracts tricked employees into transferring over $100 Million	Business Email Compromise and Authority
DNC Email Hack, 2016	Fake security alerts tricked employees into leaking credentials and confidential information	Phishing and Urgency
Twitter Hack, 2020	Multiple high profile accounts were compromised and used by hackers to spread crypto scams, stealing over $100,000	Trust Exploitation

Source: Singh, Ch. 8, Case Studies 1, 5, 6, and 9

The Human Factor: Three Lenses

Psychological

Social engineering exploits a person's psychology, trust, or ignorance. Creating a false sense of urgency or fear like a scary “ACCOUNT COMPROMISED!” message targets a person's emotions. This creates a situation where a person acts illogically and gets them to do something they wouldn't do under normal circumstances.

Social

Convenience often beats out caution. People reuse passwords across multiple accounts because unique ones are harder to remember. This means one stolen password can be the key to many doors. Wishful thinking like “it won't happen to me” makes social engineering attacks easier to carry out.

Organisational

Whaling and fake vendor scams work when staff carry out actions they might believe came from their higher ups. Insider threats can happen when attackers “trick workers or contractors into selling or sharing system access or information with unapproved parties” (Aldabagh).

Source: Singh, Ch. 8; Aldabagh et al. (2025), pg. 79

The Attack Cycle

01 Information Gathering:

The most time intensive portion of a social engineering attack. Information is gathered on potential victims and vectors of attack

02 Relationship & Rapport:

The attacker builds a relationship and trust with the victim. The relationship quality will determine the level of cooperation the victim will have with the attacker (Amade Nyirak)

03 Exploitation:

This is when the attacker actively infiltrates the target. This can be handing over information like credentials or granting physical access to restricted areas.

04 Execution:

The final step, where the attacker finally gets access to the information or systems they were targeting. Typically, this step concludes before the victim realizes it's an attack.

Source: Social-Engineer.org

Mitigating Social Engineering Threats

People	Process	Technology
The easiest and cheapest option is to educate. Spreading awareness of social engineering tactics attackers may use can significantly decrease risk of becoming a victim. Tips like: do not open links from unknown senders and verify before helping unfamiliar personal are examples of basic educational advice. Pairing this with a culture that rewards reporting, and you can easily mitigate your risk to social engineering attacks.	Verifying unusual activity like wire transfers or requests for confidential information through another person before authorizing. Getting a second opinion is always helpful because social engineering tactics specifically try to get you to act irrationally. Preventative measures like documenting policies and constantly watching for unusual behavior are important steps to take too.	Security measures can be put in place to stop social engineering tactics from succeeding. Multi factor authentication, email filtering, and one click reporting of suspicious mail can all help to deter or predict attackers actions. The most damaging vulnerability, password reusing across multiple accounts, can be completely avoided with password managers to ensure each account has secure and unique passwords.

Source: Singh, Ch. 8; Aldabagh et al. (2025), pg. 100–102

Conclusion

Social engineering exploits psychology, not code.

Authority, urgency, and trust are predictable levers attackers may use to manipulate us. Convenience and emotion make us susceptible targets.

Social Engineering threats are measurable and persistent.

62% of all breaches involve the human factor. This can be tricked staff or recruited insiders all the way to specifically targeted high value individuals.

Defense must be layered and cultural

Education, verification/reporting processes, and technically strong security systems need to work in unison, not separately. A chain is only as strong as its weakest link, and social engineering targets that link.

References

Aldabagh, H., Bowman, C., Kirkpatrick, C., Oesteraas, I. & Yalpi, V. L. D. (2025). Cybersecurity, technology & society: An interdisciplinary look at the field of cybersecurity. Old Dominion University.

Singh, T. Chapter 8: Case Studies: Social Engineering Tactics.

Verizon. (2026). 2026 Data Breach Investigations Report. Verizon Business.

Social-Engineer, LLC. The attack cycle. Security Through Education. https://www.social-engineer.org/framework/attack-vectors/attack-cycle/

Course Materials: CYSE 201S Social Engineering PPT (Module 6)