Social engineering

Christine Potthast, Patrick Berry, and Hamad Al-Naimi

Abstract: The realm of cybersecurity is replete with challenges, not least among them being the art of social engineering. This form of attack leverages human tendencies such as trust, leading to potential breaches. Though more covert than brute force or technical hacks, social engineering can be insidiously effective. Within this exposition, we probe various manifestations of social engineering: from phishing to pretexting, baiting to tailgating, and the subtle act of shoulder surfing, concluding with mitigation strategies.

Keywords: cybersecurity, social engineering, phishing, pretexting, baiting, tailgating

1. Phishing: Unmasking the facade

Phishing, at its essence, is the act of digital deception wherein malefactors don a trustworthy guise to exploit the unwary. Subtypes like spear-phishing and whaling refine this technique with a more targeted approach, while vishing introduces auditory elements to the subterfuge. For instance, the 2018 Airbnb masquerade leveraged the European Union's GDPR transition, ensnaring unsuspecting users. Counteractions encompass a spectrum: user education, public cognizance, robust login protocols, technological countermeasures, and punitive legal actions.

2. Quid pro quo: A deceptive exchange

Quid Pro Quo, translated as "something for something", in the context of social engineering, is a sinister barter of services for access. The modus operandi often involves a trifold strategy: initiate a problem, pose as the solution, and extract the prize. Proper user education can vitiate the impact of these tactics.

3. Baiting: The allure of forbidden fruit

Drawing from the age-old paradigm of curiosity killing the cat, baiting relies on human inquisitiveness. A seemingly innocuous device, laden with malicious intent, is left for the unsuspecting. Once engaged, the device delivers its payload, often to calamitous effect. Preventative strategies chiefly revolve around awareness and education.

4. Pretexting: Crafting an illusion

Delving into the art of pretexting, one enters the domain of elaborate narratives and impersonation. Adept attackers fashion intricate, believable personas, becoming chameleons in their quest for unauthorized data. Hewlett-Packard's notorious escapade provides a case in point. A fortified system of identification and verification stands as a bulwark against such ruses.

5. Tailgating: Breaching the physical gateway
Beyond the digital, lies the tangible threat of tailgating, where unauthorized entities slip through security perimeters by piggybacking on legitimate entries. The breach, in this instance, is as much a physical space as a virtual one. Countermeasures include hierarchical badge systems, vigilant security personnel, and surveillance apparatuses.

6. Shoulder surfing: Espionage in plain sight
This variant of attack is simplicity personified: the mere act of observation. Whether one is keying in an ATM PIN or entering a system password, prying eyes could be lurking. The act is brazen, yet its simplicity makes it pernicious. A combination of user mindfulness and spatial design can offer deterrence.

6.1 Phishing
Phishing is one of the most prevalent forms of social engineering. As the digital realm expands, the tactics and methods employed in phishing attacks have evolved (Whitman & Mattord, 2018). Spear-phishing and whaling are specialized versions of phishing targeting specific individuals or high-ranking officials within organizations, respectively.

6.1.1 Example: The Airbnb phishing incident in 2018 is a testament to the level of sophistication in recent attacks. With the introduction of GDPR, many businesses were adjusting their policies and practices, which provided attackers a chance to exploit the situation (Bisson, 2018).

6.1.2 Countermeasures: Organizations should use multi-factor authentication (MFA) systems to provide an extra layer of security. Regular employee training sessions to identify suspicious emails can substantially reduce the risk (Hadnagy, 2011).

6.2 Quid pro quo
This tactic leverages human nature to reciprocate. By offering help or services, attackers trick their victims into providing sensitive data or access (Ivaturi, and Janczewski, 2011).

6.2.1 Countermeasures: Ensuring that employees understand protocols related to tech issues can prevent this. If an unknown individual offers assistance, employees should be trained to immediately notify their IT department (Whitman & Mattord, 2018).

6.3 Baiting
Baiting preys on human curiosity. By leaving malware-infected devices in easily accessible locations, attackers wait for unsuspecting victims to plug them in, granting unauthorized access (Arfuso, 2015).

6.3.1 Countermeasures: Implement strict policies about using unknown external devices on company hardware. Regularly educating employees about the risks can also deter them from falling prey (Hadnagy, 2011).

6.4 Pretexting
Pretexting involves a fabricated scenario to gain information or access. Deep research is usually conducted by the attacker to make their story more believable (Hadnagy, 2011).

6.4.1 Countermeasures: Implement strict data access protocols and ensure that sensitive data requests are always cross-verified through multiple channels (Whitman & Mattord, 2018).

6.5 Tailgating
Tailgating is a physical security breach where unauthorized individuals gain entry by following an authorized person (Whitman & Mattord, 2018).

6.5.1 Countermeasures: Install security cameras at entry and exit points and train employees not to hold doors open for strangers. Employ security personnel at vital access points to ensure protocol adherence.

6.6 Shoulder surfing
Shoulder surfing is the act of gaining unauthorized information by literally looking over someone's shoulder (Whitman & Mattord, 2018).

6.6.1 Countermeasures: Utilize privacy screens on computer monitors, especially in high-traffic areas. Encourage employees to be aware of their surroundings when entering sensitive data.

Table 1: Social engineering attacks and preventive measures

Attack Type	Description	Preventive Measures
Phishing	Attackers imitate trustworthy entities via emails.	Multi-factor authentication, employee training.
Quid Pro Quo	Attackers offer services in exchange for data/access.	Strict IT protocols, employee awareness.
Baiting	Uses malware-infected devices to lure victims.	Restrict unknown device usage, regular education.
Pretexting	Uses a fabricated scenario to extract information.	Strict data access protocols, cross-verification.
Tailgating	Unauthorized entry by following an authorized person.	Cameras at entry/exit, security personnel.
Shoulder Surfing	Gaining data by looking over someone's shoulder.	Privacy screens, employee spatial awareness.

7. Conclusion:
The digital age, with all its advancements, brings forth unique challenges. The realm of social engineering underscores the ever-present tension between technology and human fallibility. As evinced through various attack vectors, the human element often emerges as the weakest link. Mitigation, then, requires a holistic approach, fusing technological safeguards with rigorous user education and awareness.

References

[1] Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. Wiley.
[2] Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley.

[3] Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security*. Cengage Learning.
[4] Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610-613.
[5] Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94-100.
[6] Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4), 662-674.
[7] Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cybersecurity risk. *Computers & Security*, 31(4), 597-611.
[8] Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73-80.
[9] Alseadoon, I., Chan, T., & Foo, E. (2012). Who is more susceptible to phishing emails? A Saudi Arabian study. *Information Management & Computer Security*.
[10] Stajano, F., & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM*, 54(3), 70-75.
[11] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66, 40-51.
[12] Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI conference on Human Factors in computing systems*.
[13] Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys (CSUR)*, 48(3), 1-39.
[14] Finn, P., & Jakobsson, M. (2007). Designing ethical phishing experiments: A study of (ROT13) rOnl query features. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.
[15] Florencio, D., & Herley, C. (2006). A large-scale study of web password habits. *Proceedings of the 16th international conference on World Wide Web*.