The Role of Three Human Factors in Social Engineering Attacks

Table of Contents

1. Introduction

Information security is a critical aspect of security operations, especially for small and medium sized enterprises who may have limited security budgets and personnel for data and Cyber security (Bhaharin et al., 2019; Kovaite & Stankeviciene, 2019). One important but often overlooked aspect of information security is social engineering (SE), which focuses on the manipulation of human psychological factors rather than network or system vulnerabilities for sensitive data extraction (Cains et al., 2015).

A majority of Cyber security breaches committed against UK businesses recorded in 2023 were SE attacks, at least 20% higher than any other attack type (Figure 1; Ell & Johns, 2023). This paper thus intends to discuss three human factors which can contribute to successful SE attacks, concentrating on low-level attack psychology, common characteristics, and possible outcomes to bring attention to possible gaps in organizational security measures.

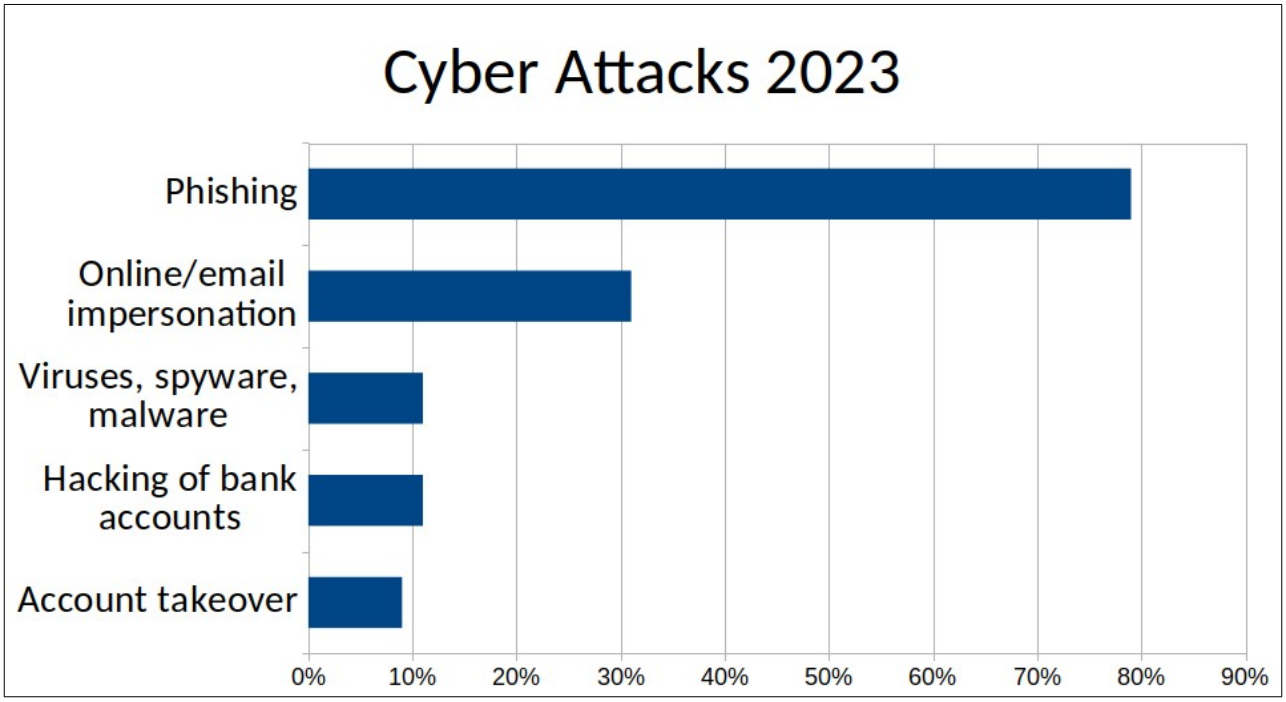

Figure 1: Rate of Cyber Attacks 2023

2. Low-Level Attack Psychology

The human psyche can be exploited in various ways to obtain sensitive information and influence behaviour. Though individuals respond to psychological factors differently, those in similar roles often have similar responses to SE exploits. *Unauthorised Access* (Allsopp, 2009) lists the fundamentals of 'guerilla psychology' which "plays on states of mind in order to" (53) complete an SE attack (Table 1).

In addition, malicious actors can employ 'tactical approaches' during interaction which play on low-level psychological factors to "speed up the process" (ibid: 61) of the SE attack (Table 2). Any of these low-level factors and approaches can be exploited alongside high-level factors (Section 3) for successful manipulation.

Table 1: Low-level Psychological Factors to Exploit

Exploit	Vulnerability
Trust	People trust others unless having a specific reason not to
Gullibility	Subjective claims are susceptible to manipulation
Greed	This is a fundamental human drive
Group mind	People are more likely to believe what their peers do
Desire to help	People are expected to be helpful toward colleagues
Desire to be liked	This is a fundamental human drive

Table 2: Tactical Approaches

Tactic	Utility
Impatience	Can sabotage judgment capabilities of the target
Politeness	Can put the target at ease
Inducing fear	Can impact the reasoning capabilities of the target
Faking supplication	Can inspire the target to placate
Faking authority	Can imply potential loss of employment
Ingratiation/deference	Can imply the superiority of the target

3. High-Level Human Factors

3.1 Lack of Knowledge and Memory Failure

Recognition of a website's authenticity is routinely left to the individual to parse and verify (CERT, 2014). Unintentional Insider Threats (UITs), potential marks working for targeted organizations, often rely on the expertise of features, professional look and feel, and positive assessment of a website's credentials to discern its credibility (CERT, 2014; Sharek et al., 2008).

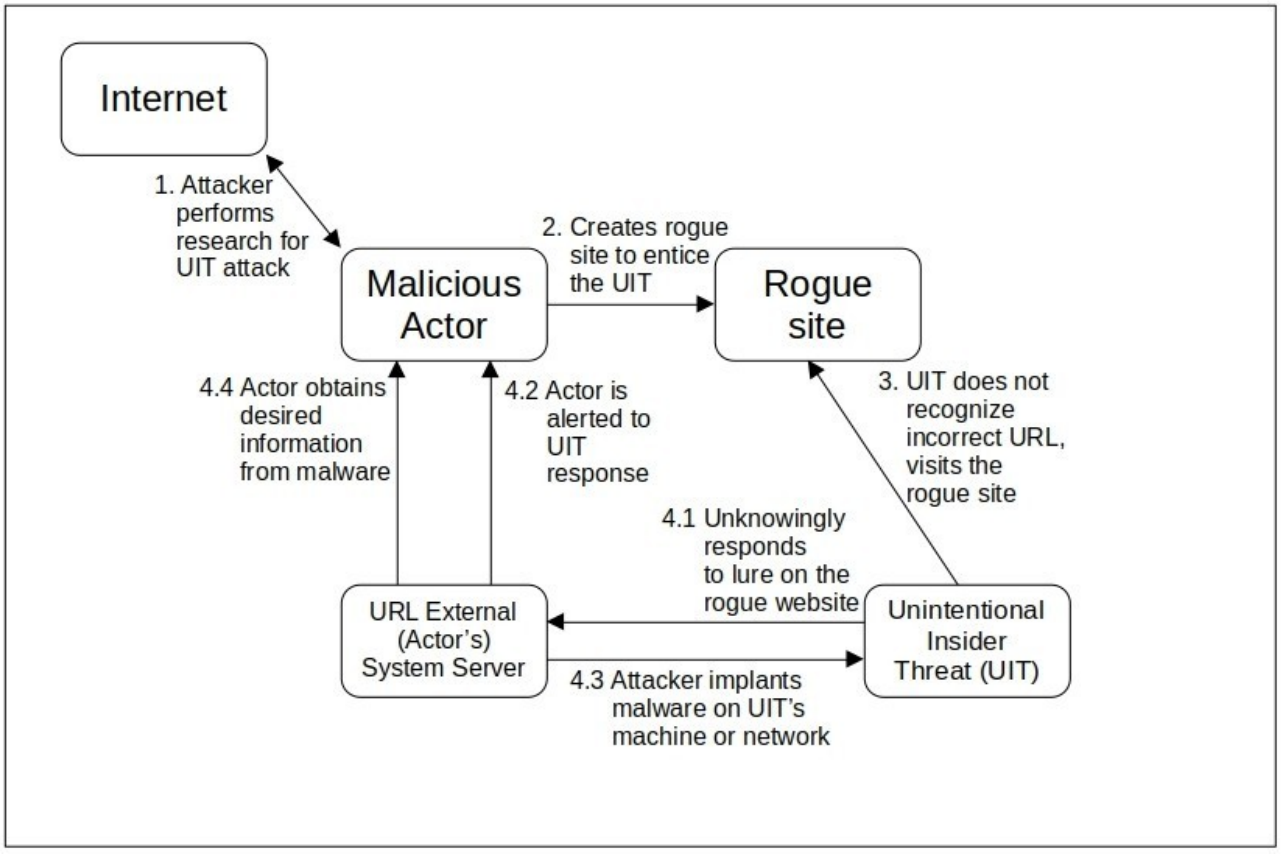

Figure 2: Man-in-the-Middle Attack

Unfortunately, users often have a suboptimal understanding of how these factors can be manipulated by malicious actors (Erkkila, 2011). Dhamija et al.'s (2006) study of phishing websites found that:

- "Good phishing websites fooled 90% of participants" (ibid: 581)
- Popup warnings about potential fraud were ineffective

- Education, age, sex, and computer experience showed no correlation to potential phishing vulnerability

As a result, if users are trusting and/or gullible and the website appears authentic, malicious actors could gain access to sensitive information through a Man-in-the-Middle attack (Figure 2; CERT, 2014).

3.2 Faulty Reasoning and Judgment

Phishing emails can be successful SE vehicles, as cognitive biases around attention show that recipients judge emails on content rather than cues for authenticity. Informative emails are a common example; UITs consider them safe even if they redirect to a website that requests

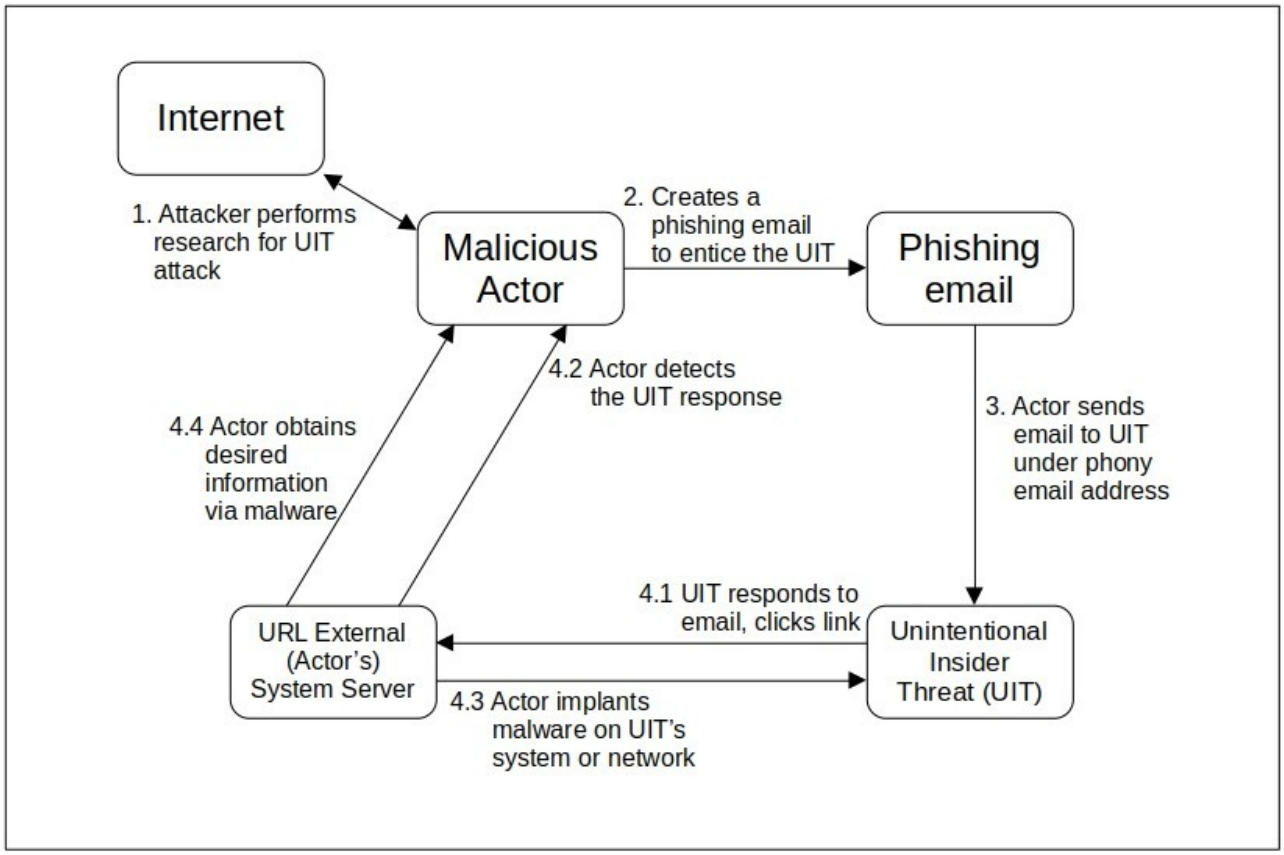

Figure 3: Phishing Email Attack

credentials or other information (CERT, 2014). The appearance of authority is a reliable tactic to convince UITs that such an email link is safe. Butavicius et al. (2015) found that even with explicit instructions to avoid bogus email links, users were unable to distinguish between real and fake links "when the email contained reference to an authority figure" (7). Thus, fabricating authority may induce fear or the desire to be liked or helpful, and compel a UIT to disregard security policies and click a link provided by a suspicious email (Figure 3; Hadnagy, 2018).

3.3 Casual Values and Attitudes about Compliance

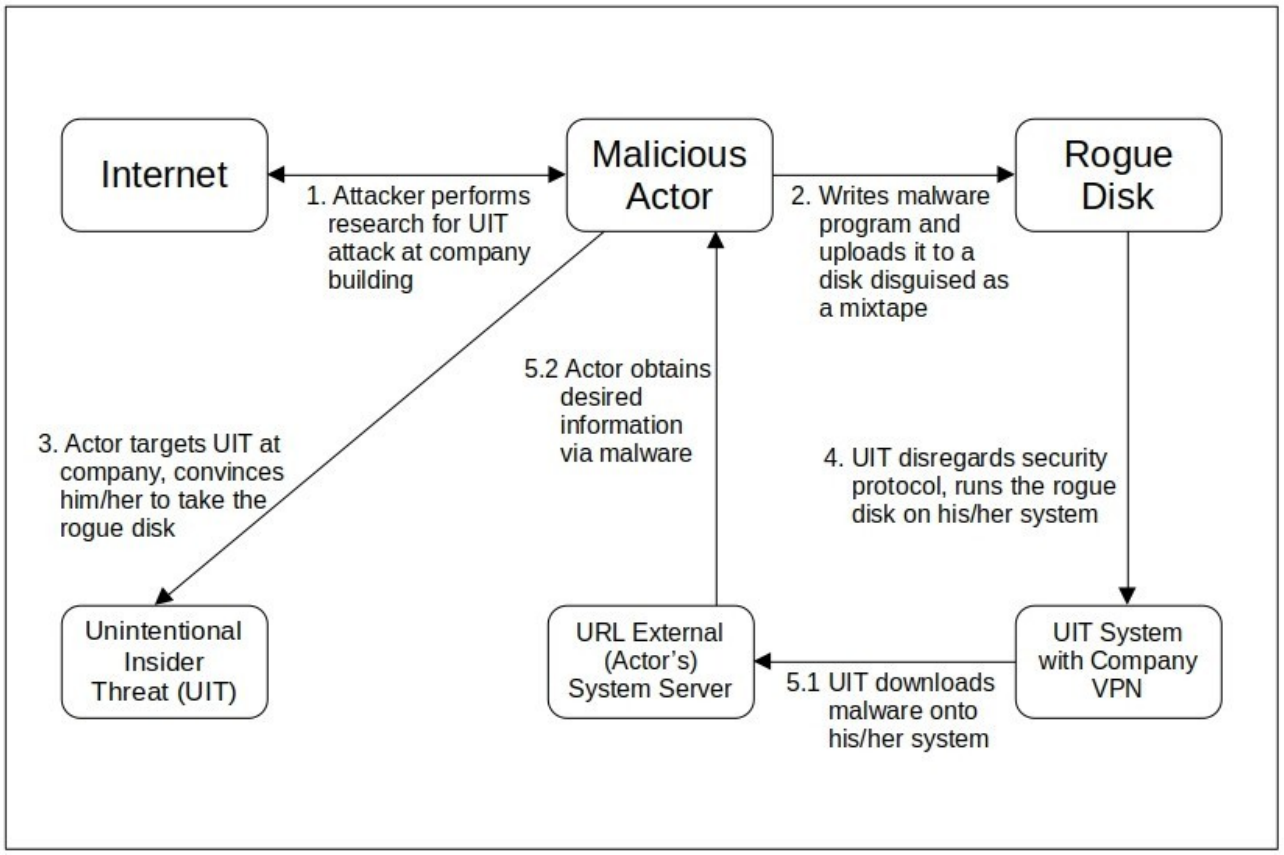

Figure 4: Physical Artifact Attack

UITs' attitudes towards compliance with security policies can be traced back to pre-existing beliefs (CERT, 2014), and though a company may implement security policies to prevent SE attacks, UITs' adherence often depends on their "motivation to conform" (Lee et al., 2021: 2). The threat of

sanctions are not found to be “an effective motivator” (Carter et al., 2012: 14) for those with a desire to be liked, a desire to help, or who do not take the threat of sanctions seriously. Interestingly, rewards for compliance are also not significant motivators if non-compliance is perceived as more beneficial (Barki & Khatib, 2021).

Such attitudes could manifest in SE attacks that would otherwise be unusual. One example is a UIT receiving a rogue disk from a malicious actor. If the disk has a sufficient disguise and the UIT is sufficiently motivated, either by greed, trust, or indifference, the company network could be compromised (Figure 4; Esmail, 2015; UIC, 2021).

4. Conclusion

Social engineering is a popular and effective form of Cyber attack, though it is often overlooked as an aspect of information security. Three high-level human factors along with low-level psychological factors and tactical approaches have been discussed with a concentration on common characteristics and possible outcomes to bring attention to possible gaps in organizational security measures.

5. References

Allsopp, W. (2009) *Unauthorized Access: Physical Penetration Testing for IT Security Teams*. West Sussex, UK. Wiley: 53 – 70.

Barkhi, H. & Khatib, R. (2021) How Different Rewards Tend to Influence Employee Non-Compliance with Information Security Policies. *Information & Computer Security,* 2(1): 97 – 116.

Bhaharin, S. H., Mokhtar, U. A., Sulaiman, R., & Yusof, M. M. (2019) Issues and Trends in Information Security Policy Compliance. In: *6th International Conference on Research and Innovation in Information Systems (ICRIIS).* IEEE: 1 – 6.

Butavicius, M., McCormac, A., Parsons, K., & Pattinson, M. (2015) Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails. In: *Australasian Conference on Information Systems*. Adelaide, AUS: 1 - 10

Cains, G., Henshel, D., Hoffman, B., & Kelley, T. (2015) Trust as a Human Factor in Holistic Cyber Security Risk Assessment. In: *6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015)*: 1117 – 1124.

Carter, L., McBride, M., Warkentin, M. (2012) Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies. Triangle Park, North Carolina. RTI International–Institute for Homeland Security Solutions: 1 – 36. [online] Available at: https://d1wqtxts1xzle7.cloudfront.net/72231033/CyberSecurityFinalReport-Final_mcbride-2012-libre.pdf?1633979473=&response-content-disposition=inline%3B+filename%3DExploring_the_Role_of_Individual_Employe.pdf&Expires=1684764528&Signature=HNnB4eqZ4RfKK4Z2AHJJmLpXRXWLLAkox9qs8kOakqxW7fP9Jl1LWj20AOwSYRvj3HRVRDFn9jsYdF~ESek8n5cjHlG4WfcO2HvT3X8zgm~xz0yFebgj6nZxWOSKlDIMPzpnCh6Dh-rtXLefFZ8WpdhhIzbLw5RoSV9LjsLlKi1l7tVcWVs7qFAqpS93mkrA0ghztseCQ0twvYgFYLxOXU8YvhWlEhPZKdZeN3dWM0AaybGT8-d1v3PTpJdByFhvTyJbc6RYhWO8mGlI2130JQ-wllRn~5yNJQr~GPlw9tLWH1vfZvQhRKppaOgwxxmQkJyl5kR4mSp1EmbUsEFg3A__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

CERT Insider Threat Center (2014) Unintentional Insider Threats: Social Engineering. Pittsburgh, USA. Carnegie Mellon University: 11 – 38.

Dhamija, R., Hearst, M., & Tygar, J. D. (2006) Why Phishing Works. In: *CHI 2006 Conference on Human Factors in Computing Systems*. Montreal, Quebec: 581 – 590.

Ell, M. & Johns, E. (2023) *Cyber Security Breaches Survey 2023* | gov.uk. Government of the United Kingdom. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023#chapter-4-prevalence-and-impact-of-breaches-or-attacks

Erkkila, J-P. (2011) Why We Fall for Phishing. In: *CHI 2011 Conference on Human Factors in Computing Systems*. Vancouver, British Columbia: 1 – 8.

Esmail, S. (2015) 'eps1.1_ones-and-zer0es.mpeg', *Mr. Robot*. USA.

Hadnagy, C. (2018) *Social Engineering: The Science of Human Hacking*. Indianapolis, IN. Wiley.

Kovaite, K. and Stankeviciene, J. (2019) Risk of Digitalisation of Business Models. In: *International Scientific Conference*. Vilnius, Lithuania. VGTU Press: 380-387.

Lee, V-H., Ooi, K-B., Sohal, A., Tan, G. W-T., Wong, L-W. (2021) The Role of Cybersecurity and Policy Awareness in Shifting Employee Compliance Attitudes: Building Supply Chain Capabilities. *International Journal of Information Management*: 1 – 15.

Sharek, D. Swofford, C., & Wogalter, M. (2008) Failure to Recognize Fake Internet Popup Warning Messages. In: *Human Factors and Ergonomics Society 52nd Annual Meeting*: 557 – 590

UIC (2021) *Phishing & Social Engineering: Don't Fall for a Nasty Guise!* | Information Technology @ UIC. [online] Available at: https://it.uic.edu/news-stories/phishing-social-engineering-dont-fall-for-a-nasty-guise/