Social Engineering Attacks through the Lens of Routine Activity Theory: An Analysis of Crime Theory, Policy, and Prevention

Kurt J Williams

School of Cybersecurity, Old Dominion University

CRJS 215S: Introduction to Criminology

Phil Austin

4/28/2025

Social Engineering Attacks through the Lens of Routine Activity Theory: An Analysis of Crime Theory, Policy, and Prevention

Introduction

Cybercrime represents a significant and growing threat to individuals, businesses, and governments across the globe. One of the most prevalent forms of cybercrime is social engineering attacks, where perpetrators manipulate individuals into revealing confidential information, granting access to restricted systems, or performing actions that compromise security. Social engineering is "is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information" (Carnegie Melon University, 2025). Social engineering exploits human psychology rather than technical vulnerabilities, making it a unique and particularly difficult form of crime to prevent. Traditional firewalls focus on blocking unauthorized access from electronic sources, but social engineering attacks circumvent these firewalls by exploiting the human element of a computer network. There are multiple forms of social engineering attacks, and one of the most common is Phishing. Phishing is "the process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity using bulk email, SMS text messaging, or by phone. Phishing messages create a sense of urgency, curiosity, or fear in the recipients of the message" (Carnegie Melon University, 2025).

According to the FBI's Internet Crime Complaint Center (IC3) 2023 Report, social engineering tactics such as phishing, business email compromise (BEC), and tech support scams accounted for over $4.59 billion in reported financial losses (Federal Bureau of Investigation,

2024). This figure represents a significant increase from previous years and emphasizes the growing sophistication and frequency of these attacks. In addition, a Pew Research Center report from 2017 found that 64% of Americans had personally experienced a major data breach, and more than half expressed concern about their vulnerability to online attacks (Pew Research Center, 2017).

Routine Activity Theory (RAT), first introduced by Cohen and Felson in 1979, provides a useful framework for understanding the situational conditions that make social engineering possible. RAT proposes that crime occurs when three elements are present: a motivated offender, a suitable target, and the absence of a capable guardian (Cohen & Felson, 1979). In cyberspace, motivated offenders can quickly and easily find suitable targets who often lack the digital guardianship measures needed to protect themselves, such as strong passwords, multi-factor authentication, or cybersecurity training.

This paper explores how RAT applies to social engineering attacks. It first reviews relevant academic literature applying RAT to cybercrime, including both quantitative and qualitative studies. Then, it examines crime-prevention policies grounded in these theoretical insights. Finally, this paper provides a synopsis of key findings and policy recommendations.

Review of Literature

Crime Theory

Routine Activity Theory (RAT) has been widely utilized to understand cybercrime victimization, particularly social engineering attacks. Two studies — one quantitative and one qualitative — highlight how offender motivation, target suitability, and lack of capable guardianship contribute to online victimization.

Bossler and Holt (2009) conducted a quantitative study examining the relationship between online activities, guardianship behaviors, and the likelihood of malware infections. Using survey data from college students, the researchers operationalized RAT concepts by measuring time spent online, risky behaviors (such as downloading illegal software), and protective behaviors (such as using antivirus programs). Their findings indicated that individuals who engaged in more risky online behaviors without implementing protective measures were significantly more likely to become victims of malware infections. Bossler and Holt (2009) also argued that physical target hardening was less effective at preventing victimization and instead emphasized the importance of adjusting behaviors online to better protect users. This study empirically supports the idea that the convergence of a motivated offender, a suitable target, and insufficient guardianship dramatically increases the likelihood of cybervictimization.

Cross (2016) offered a qualitative perspective to cybercrime by interviewing elderly victims of cyber-fraud. Through semi-structured interviews, Cross explored victims' perceptions of how they were deceived. Many participants admitted to overlooking basic security practices, such as verifying the identity of unknown senders or double-checking the legitimacy of requests. The study also found that victims often perceived the scams as "low risk" or "only minor crimes," which contributed to their lack of vigilance. This qualitative data aligns with RAT, as it highlights how target vulnerability and weak guardianship — driven by cognitive biases and misperceptions — create ideal conditions for offenders.

Both studies reinforce the critical role of guardianship in preventing cybercrime. Where Bossler and Holt (2009) used quantitative data to show the statistical correlation between risky behaviors and victimization, Cross (2016) provided narrative accounts illustrating how victims' attitudes contribute to their vulnerability.

Crime Policy

In response to the increasing threat of cybercrime, especially social engineering attacks, crime prevention strategies have evolved to emphasize enhancing guardianship and reducing target suitability. Nobles, Reyns, Fox, and Fisher (2014) conducted a study examining formal and informal coping strategies used by victims of cyberstalking. Although their study focused specifically on cyberstalking, the policy implications are directly relevant to broader forms of cybervictimization, including social engineering attacks.

Nobles et al. (2014) found that formal interventions, such as reporting incidents to law enforcement, utilizing restraining orders, and adopting formal cybersecurity measures were underutilized compared to informal coping strategies, such as ignoring the attacker, changing email addresses, or increasing privacy settings on social media. One critical barrier to using formal resources was a lack of knowledge about available protections, and a perception that authorities were unable or unwilling to address cybercrimes effectively.

Their findings suggest that prevention efforts should prioritize increasing public awareness about cybersecurity threats, improving digital literacy, and enhancing accessibility of support resources. Programs that educate potential victims about common tactics used in social engineering — such as phishing emails, pretexting, and baiting — and that teach proactive guardianship strategies (e.g., verifying senders, using multi-factor authentication) align with RAT's focus on capable guardianship.

Based on Nobles et al.'s (2014) results, effective crime policy should combine technical solutions (like improved software protection) with educational campaigns designed to change risky behaviors and promote vigilance among potential victims. The 2023 MGM Resorts cyberattack is a prime example of how lapses in capable guardianship and human-centered

vulnerabilities can enable social engineering attacks that lead to security breaches despite robust cybersecurity infrastructures.

Current Example of Social Engineering

A recent example of a social engineering attack occurred during the 2023 MGM Resorts cyberattack. In this case, attackers from the "Scattered Spider" groups social engineering techniques to breach MGM's internal systems (Gupta, 2023). According to an in-depth analysis by Gupta (2023), the attackers impersonated a senior MGM employee and contacted the company's IT help desk through vishing (voice phishing) attacks. By using publicly available information from LinkedIn to better impersonate their victim, the attackers successfully convinced help desk personnel to reset login credentials and gained privileged access to critical systems.

This attack highlights how RAT applies in real-world cyber incidents. The motivated offender (the "Scattered Spider" group) identified a suitable target (an organization with accessible employee information and standard help desk protocols) and exploited a situation with an absence of capable guardianship (inadequate verification procedures). Despite MGM's investment in cybersecurity infrastructure, the attack succeeded because the human element — the help desk staff — became the weak link in the guardianship chain.

The MGM attack emphasizes the need for not just technical defenses, but also rigorous social engineering awareness training for employees. It demonstrates that even highly secure organizations remain vulnerable when situational guardianship lapses occur.

Synopsis/Discussion

This paper has examined the relevance of RAT to understanding and preventing social engineering attacks. Both quantitative and qualitative research confirm that the convergence of a

motivated offender, a suitable target, and a lack of capable guardianship creates prime conditions for victimization. Crime prevention strategies should therefore prioritize strengthening guardianship — not only by deploying advanced cybersecurity technologies but also by educating individuals about the psychological manipulation tactics employed by social engineers.

However, enhancing capable guardianship alone may not be sufficient. In addition to improving guardianship, it is critical to address target hardening and reducing target attractiveness. Target hardening involves making it more difficult for offenders to access victims by implementing more stringent verification processes, improving security protocols, and requiring multiple layers of authentication before sensitive actions (like password resets) are completed. These measures were notably absent in the MGM cyberattack, where the attackers successfully bypassed safeguards by exploiting procedural weaknesses.

Reducing target attractiveness is another essential strategy. For example, limiting the amount of personal and organizational information available online can make it harder for attackers to craft convincing pretexts. Training individuals to be cautious about oversharing on social media and ensuring organizations conduct regular audits of publicly available employee information are critical steps toward decreasing the visibility and accessibility of potential targets.

The MGM cyberattack serves as a stark reminder that even well-funded organizations can be victimized through social engineering attacks when procedural and human vulnerabilities are exploited. It demonstrates that technical defenses alone are insufficient if human elements remain untrained or unaware. Future policy initiatives must therefore combine technical

hardening with widespread, ongoing digital literacy campaigns targeted at all levels of society — from individual users to corporate IT departments.

Despite significant advances in cybersecurity tools, the human factor remains a critical vulnerability. Social engineering attacks, by their very nature, bypass firewalls and encryption by tricking people rather than defeating machines. In line with RAT, preventing victimization in the digital age will require multi-layered approaches: enhancing capable guardianship, hardening potential targets, minimizing visibility to motivated offenders, and raising public awareness about emerging cyber threats.

Addressing social engineering attacks must be prioritized at a societal level. Just as government conducted campaigns to raise awareness for public health (anti-smoking or seatbelt use) have shifted cultural behavior over time, so too there should be campaigns to raise awareness about social engineering attacks. Introducing cybersecurity education into schools, workplaces, and media campaigns could help normalize cautious digital habits from a young age. Furthermore, businesses should shift away from viewing cybersecurity as purely a technical IT responsibility and recognize it as a holistic organizational risk that requires engagement at every level — from entry-level employees to senior executives. Without broad, systemic cultural change that emphasizes digital responsibility and awareness, social engineering attacks will remain a persistent and growing threat.

References

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of Routine Activity Theory. *International Journal of Cyber Criminology, 3*(1), 400–420. https://www.researchgate.net/publication/228929213_On-line_Activities_Guardianship_and_Malware_Infection_An_Examination_of_Routine_Activities_Theory

Carnegie Mellon University. (2025). Social engineering. Information Security Office. Retrieved April 28, 2025, from https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589

Cross, C. (2016). 'They're Very Lonely': Understanding the Fraud Victimisation of Seniors. *International Journal for Crime, Justice and Social Democracy*, *5*(4), 60-75. https://doi.org/10.5204/ijcjsd.v5i4.268

Federal Bureau of Investigation. (2024). *Internet Crime Report 2023.* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Gupta, S. (2023). *In-depth analysis of the 2023 MGM Resorts cyberattack*. Industrial Software Community. https://industrial-software.com/community/news/in-depth-analysis-of-the-2023-mgm-resorts-cyberattack-virsec-systems-blog/

Nobles, M. R., Reyns, B. W., Fox, K. A., & Fisher, B. S. (2012). Protection Against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking Victimization

Among a National Sample. *Justice Quarterly*, *31*(6), 986–1014.

https://doi.org/10.1080/07418825.2012.723030

Pew Research Center. (2017). *Americans and cybersecurity.*

https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/