Cultural Attitudes Towards Trust in Technology and Their Impact on Susceptibility to Cybersecurity Scam Tactics

Samantha F. Riggs

Old Dominion University

IDS 300W: Interdisciplinary Theory and Concepts

Dr. Kat LaFever

April 25, 2025

Introduction

The FBI's Internet Crime Complaint Center (IC3) reported receiving 3.79 million complaints from 2019 to 2023. During the five-year span, an estimated $37.4 billion was lost to cyber based scams (Federal Bureau of Investigation, 2024). While there are multiple challenges that organizations face in cybersecurity, one commonly acknowledged issue is the role of human error. Many cybersecurity scams exploit flaws in human reasoning and decision-making, especially by targeting trust, which is a deeply emotional and psychological mechanism.

However, the factor of trust is not uniform across individuals or region as it is often shaped by one's culture. A person's reasoning, risk assessment, and level of trust in technology are all influenced by both the culture and social environment in which they are raised. As a result, factors that could make one cultural group more susceptible to cyber scams may not apply to another in the same way. This variability between cultures introduces a factor that is frequently overlooked in the development of cybersecurity awareness and prevention strategies. The lack of culturally informed scam prevention continues to contribute to an overall gap in global cybersecurity resilience.

In order to effectively address this issue, it is important to note that no single discipline would provide a sufficient enough solution. Scam vulnerability is not just a technological problem rooted in the cybersecurity field. It is an interdisciplinary concern that involves a combination of psychology, linguistics, cybersecurity, and anthropology. Cultural attitudes toward trust in technology significantly impacts how individuals perceive and respond to modern digital threats. Attackers often exploit psychological trust mechanisms, linguistic cues, and even culture specific communication styles. Therefore, an interdisciplinary understanding of scam

tactics and their social context is not only beneficial, but essential for developing more effective and adaptable strategies.

Literature Review

Cybersecurity Perspective

At its core, cybercrime is any unauthorized activity involving a system, equipment, or network (Li & Liu, 2021, p. 8183). While cyber-attacks take many forms and can be motivated by a variety of factors, one of the most common and damaging types involves scamming individuals into voluntarily revealing personal or sensitive information for the attacker's gain. These scams often rely on some form of social engineering, which in this case is simply the manipulation of human behavior in order to achieve a goal.

Common examples include romance scams, which aim to gain the target's affection and trust; charity scams, in which attackers ask for donations for illegitimate or nonexistent organizations; and perhaps the most well-known, phishing scams. According to the FBI's Internet Crime Complaint Center (IC3), phishing was the most commonly reported cybercrime in 2023, with 298,878 complaints submitted (Federal Bureau of Investigation, 2024).

Phishing is broadly described as "a method in which a hacker sends a seemingly legitimate email asking users to disclose confidential information (Saxena & Gayathri, 2021, as cited in Li & Liu, 2021, p. 8184)." While email is the most common vector, phishing attempts now extend to text messages, social media platforms, and even voicemail. These attacks can be non-specific or highly tailored, as in spear phishing, where the attacker goes as far as to impersonate a known or trusted individual, often someone from the victim's workplace or professional network, to increase believability.

Given the central role of human error in the success of these scams, cybersecurity experts tend to view training and education as the most effective countermeasure. Comprehensive awareness programs help both individuals and organizations recognize suspicious content, verify sources, and report any potential threats. However, the effectiveness of such training often depends on elements that technical strategies alone may miss, such as linguistic or psychological factors.

Psychology Perspective

The psychological concept of cognitive biases offers an explanation for why a person may make irrational decisions in unfamiliar or high-pressure situations. A cognitive bias is considered to be an unconscious error in thinking that can occur when people process and interpret information that is present in their surroundings that results in a distorted perception of reality, therefore directly influencing the human decision-making process (Da Silva, Gupta, & Monzani, 2023). These biases, while they can be helpful in daily life, can be exploited in cyber scams that involve trust, authority, or emotional pressure.

One of the most commonly exploited biases in scam tactics is authority bias, which is the tendency to view figures of authority as more credible or trustworthy, regardless of the presence of verification. Scammers often choose to impersonate supervisors, government officials, or corporate representatives to increase believability. In cultures where societal norms reinforce respect for authority and discourage questioning hierarchical figures, such as South Korea or Japan, this tactic can become ever more effective. When it comes to the cultural context, recipients may be less likely to question types of communication that appear to originate from someone in a superior position.

Another key psychological mechanism involved in scam susceptibility is the manipulation of fear and urgency. Phishing schemes frequently invoke scenarios such as missed court dates, bank account lockouts, or legal threats to create a sense of time-sensitivity. When presented with a threat in this manner, people are more likely to act quickly without carefully evaluating the legitimacy of the message. The urgency that these situations present reflects the tendency for an individual to engage in potentially risk-taking decisions in response to strong negative and positive emotions (Fisher Fox, Prestigiacomo, & Cyders, 2024)

Together, psychological vulnerabilities such as these highlight why scam tactics are not just technical issues but deeply human ones. Scammers rely on pre-existing cognitive biases, emotional appeals, and perceived authority to manipulate targets. These factors vary not only from person to person, but from culture to culture.

Linguistics Perspective

As Johnstone (1989) notes, any persuader has access to a range of persuasive strategies, and his or her choices of persuasive strategies, like his or her choices of words or grammatical structures, are made in the context at hand" (p. 153). This concept is particularly relevant in the context of cyber scam tactics, where the language used is rarely accidental. Scammers intentionally select words, sentence structures, and tones designed to produce a specific response. The use of certain grammatical structures, such as passive voice ("Your account has been compromised") or imperative commands ("Click the link below"), can play a persuasive role, especially when paired with emotional cues or claims of authority. These linguistic choices, which may seem neutral or routine to recipients, are often part of carefully crafted or algorithmically generated rhetorical strategies that can shape perception and action. As with psychological manipulation, the success of linguistic persuasion is deeply intertwined with the

target's cultural and communicative expectations, making language one of the more subtle tools utilized by scammers.

The language used in phishing emails is such a meaningful factor that many spam filters currently in place rely heavily on recognizing specific red flags found in these messages. This is done by implementing technical checks such as URL content or HTML link structures. However, with the rapid advancement of modern technology, detection systems have become more sophisticated. Natural Language Processing (NLP) now enables machine learning algorithms to analyze an email's content for signs of deception, evaluating its semantics, syntax, and structure to determine whether it is likely to be a phishing attempt or a legitimate message. Machine learning-based anti-phishing algorithms trained on both legitimate and scam messages can assess not just content, but also perceived intent and behavioral patterns (Salloum, Gaber, Vadera, & Shaalan, 2021).

Anthropological Perspective

Hofstede, a prominent figure in social psychology and cross-cultural studies, identified several cultural dimensions that contribute to national diversity in communication, behavior, and perceptions of technology. These dimensions include:

- Power Distance: the degree of inequality that members of a culture accept as normal.
- Uncertainty Avoidance: The extent to which individuals prefer structured over unstructured situations.
- Individualism: The degree to which people are integrated into groups or encouraged to act as individuals.

- Masculinity: The extent to which assertiveness, competition, and achievement are valued over qualities like nurturing, cooperation, and quality of life (Hofstede, 1989).

These dimensions help explain how people from different cultures interpret factors that influence scam susceptibility such as authority, risk, and digital communication. For example, individuals in high power distance cultures may be more likely to trust messages from figures perceived to hold authority, even in online spaces. Similarly, cultures with high uncertainty avoidance may response more impulsively to fear-based scam messages that introduce a sense of instability or urgency.

Cultural values also shape attitudes toward technology itself. A study on technology acceptance found that cultural background significantly influences an individual's readiness to adopt to new technologies, particularly in organizational settings (Sun, Lee, & Law, 2019, as cited in Al-Gahtani, Hubona, & Wang, 2007).

Another key consideration is the digital divide, defined as the disparity between socio-economic groups in terms of their access to digital communication technologies (Korupp & Szydlik, 2005). While public access programs have been implemented to reduce this divide, notable gaps persist, particularly between low- and high-income nations and across generational lines. This generational gap is especially relevant to scam vulnerability. A study on scam susceptibility in older adults found that the oldest participants were at the highest risk, even after adjusting for variables such as cognitive function or socio-economic status (James, Boyle, & Bennett, 2014). These findings suggest that technological literacy, influenced by both cultural and generational factors, plays a critical role in determining how individuals interpret and respond to scam messages.

Interdisciplinary Synthesis and Analysis

While each discipline presented provides valuable insights into the inner workings of scam tactics, a comprehensive understanding of how cultural attitudes towards trust in technology shapes scam susceptibility requires a synthesis of cybersecurity, psychology, linguistics, and anthropology. When considered together, the perspectives these disciplines provide offer a more complete explanation of how scams succeed as well as how prevention efforts might become more effective through interdisciplinary collaboration.

Cyber scams often rely heavily on the exploitation of psychological mechanisms, which serve as entry points for attackers. One of the most effective of these is authority bias, which is the tendency to place greater trust in individuals perceived to hold positions of power. In scam contexts, this often manifests through impersonations of bosses, government officials, or law enforcement. When such figures deliver a seemingly urgent message concerning serious matters such as the law or late payments, the combination of perceived authority and fear can trigger panic, especially in individuals unfamiliar with common scam tactics. This emotional response has the potential to override skepticism and lead victims to disclose sensitive information or click on malicious links without questioning their legitimacy.

From a technical standpoint, cybersecurity defenses that focus solely on tools such as firewalls, anti-virus software, and spam filters are inherently limited in their ability to counteract these human vulnerabilities. While these systems are essential for filtering and blocking known threats, they cannot fully account for the human element, which is precisely where many scams succeed. Most phishing attempts, for example, only work when the intended target interacts with the message. If the recipient doesn't respond, download the malicious software, or click the suspicious link, the scam fails. But because these attacks are oftentimes carefully designed to

provoke emotional and psychological triggers, even systems that are well-defended on a technical level can be compromised by a single human mistake.

Furthermore, the psychological predictability of certain responses makes scam more scalable. Attackers do not have the need to tailor messages to every individual as they can simply rely on broadly applicable emotional cues that have a high chance of success across large populations. This further exemplifies the need to treat cybersecurity not just as a technical issue, but as a behavioral and psychological one as well. Training and educating users to recognize manipulation tactics and understand their own cognitive biases is just as critical as developing stronger technical defenses.

While psychological mechanisms and biases create the foundation for scam success, it is often the language used in these messages that can evoke these responses. Linguistic choices such as tone, sentence structure, and word selection serve as the delivery system for psychological manipulation, shaping how messages are interpreted and whether they are trusted. Understanding how these linguistic strategies are shaped by context and audience is essential for recognizing how scams adapt to different communicative expectations.

Word choice, sentence structures, and tone are powerful linguistic tools, especially for attackers who are building and optimizing the delivery of their phishing attempt. For example, if a person wanted to come across as authoritative, they would use direct, formal, sometimes even threatening language to further evoke an emotional response in their victim. Contrast this kind of language with a phishing message that has grammatical errors or does not attempt to invoke any kind of emotional response. The latter would more than likely not be taken as seriously.

These linguistic strategies are most effective when tailored to the psychological expectations of the recipient. The use of imperative commands asking for the target to act quickly or confirm an account immediately, for example, taps into urgency bias, prompting the victim to respond quickly without questioning the legitimacy of the message. Sentences that involve passive voice, such as indicating an account has been suspended, shift focus away from the source of the message, making it seem like an official, routine process rather than a simple personal request. This approach further reinforces perceived legitimacy.

Cultural linguistic expectations also influence how these messages are received. In high-context cultures, where indirect communication and politeness are the social norm, a phishing email that uses formal, deferential language may come across as more credible. Conversely, in low-context cultures, where clarity and directness are valued, a message that is vague or overly elaborate may arouse suspicion. These differences demonstrate how language must be carefully constructed not just for emotional effect, but for cultural appropriateness as well. This highlights the need for scam detection tools and public awareness campaigns to consider both linguistic and cultural nuance.

While psychological mechanisms and linguistic strategies provide insight into how scam messages manipulate individuals on a personal level, anthropology offers critical insight into the cultural frameworks that shape how those messages are received and further interpreted. Cultural norms influence not only how people communicate and process authority, but also how they perceive technology, trust digital systems, and respond to risk. These factors play a significant role in whether an individual is more or less likely to fall victim to a cyber based scam. By examining scam susceptibility through an anthropological lens, it becomes clear that cultural

attitudes towards factors like hierarchy, uncertainty, and technology adoption deeply affect how persuasive a scam message appears.

Cultural norms significantly shape how individuals interpret and respond to digital communications, especially in the context of phishing and other scam tactics. One important cultural factor is power distance, which refers to how members of a society that are less powerful than others accept hierarchical structures and authority figures. In high power distance cultures, individuals are more likely to comply with perceived authoritative figures without question. As a result, phishing messages that impersonate government agencies or law enforcement tend to be more persuasive, particularly when combined with authoritative tone and formal language. This effect is further reinforced by psychological biases such as authority bias and linguistic cues that signal status or urgency. In contrast, individuals in low power distance cultures are more likely to hold some level of suspicion due to the cultural norm surrounding trust in sources of authority.

Beyond attitudes towards authority, technology access and digital literacy also vary widely across cultures and further contribute to scam vulnerability. In communities with limited access to communication technology, users often have less exposure and less experience with phishing tactics, which makes it more difficult to detect red flags in a scam message. These individuals may not recognize the emotional manipulation or suspicious tone that would stand out to more digitally literate users. This gap in awareness illustrates how cultural and economic factors amplify the linguistic and psychological tactics scammers often employ. In this sense, anthropological perspectives help provide an explanation as why cultural adaptation of scam prevention strategies is necessary. The strategies and methods that may work in one region may not be as effective in another.

Conclusion

Understanding why cybersecurity scams succeed requires far more than a technical explanation as it requires an examination of how people think, how they use language, and how they are shaped by their cultural environments. Cultural attitudes toward trust in technology significantly influence a person's susceptibility to scam tactics, and that these influences can only be fully understood through an interdisciplinary lens.

Through the lens of cybersecurity, it is shown how phishing and social engineering attacks exploit human behavior rather than technical weakness. Psychological perspectives reveal the cognitive biases, such as authority bias and urgency response, that scammers manipulate to provoke action. The discipline of linguistics illustrates how these psychological exploits are delivered, using tone, structure, and wording designed to evoke trust or fear. Finally, anthropology provides critical context, showing how cultural norms, levels of digital literacy, and communication styles shape the effectiveness of these tactics across different populations.

Each of these disciplines offers a piece of the puzzle, but no one discipline can fully explain the complexity of scam susceptibility on its own. A purely technical solution would overlook the emotional manipulation that makes these scams effective. A psychological approach alone would fail to account for how language constructs meaning and how culture shapes communication. By integrating these perspectives, both the development of more effective, culturally informed prevention strategies and an increase in global cybersecurity awareness can take place.

References

Al-Gahtani, S., S., Hubona, G., S., & Wang, J., (2007). Information technology (IT) in Saudi Arabia: Culture and the acceptance and use of IT. *Information & management, 44*(8), 681-691. https://doi.org/10.1016/j.im.2007.09.002

Da Silva, S., Gupta, R., & Monzani, D., (2023). Editorial: Highlights in psychology: cognitive bias. *Frontiers in Psychology*. *14*. https://doi.org/10.3389/fpsyg.2023.1242809

Federal Bureau of Investigation. (2024, March 6). *Federal Bureau of Investigation Internet Crime Report 2023.* https://www.ic3.gov/AnnualReport/Reports

Fisher-Fox, L., Prestigiacomo, C., J., & Cyders, M., A., (2024) Urgency Theory in the context of broader emotion theories: a conceptual review. *Frontiers in Psychiatry. 15.* https://doi.org/10.3389/fpsyt.2024.1403639

Hofstede, G., (1989). Organising for cultural diversity. *European Management Journal. 7*(4). 390-397. https://doi.org/10.1016/0263-2373(89)90075-3

James, B., D., Boyle, P., A., & Bennett, D., A., (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of elder abuse & neglect. 26*(2). 107-122. https://doi.org/10.1080/08946566.2013.821809

Johnstone, B., (1989). *Linguistic strategies and cultural styles for persuasive discourse*. Sage. 138-156.

Korupp, S., & Szydlik, M., (2005). Causes and Trends of the Digital Divide. *European Sociological Review. 21.*(4). 409-422. https://doi.org/10.1093/esr/jci030

Lu, Y., & Liu, Q., (2021). A comprehensive review study of cyber-attacks and cybersecurity; emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Repko, A. F., & Szostak, R, (2021). *Interdisciplinary research: process and theory.* Sage.

Salloum, S., Gaber, T., Vadera, S., & Shaalan, K., (2021). Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey. *Procedia Computer Science.* 189. 19-28. https://doi.org/10.1016/j.procs.2021.05.077

Saxena, R., & Gayathri, E. (2022). Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution. *Materials Today: Proceedings.* 51. (2022). 682-689. https://doi.org/10.1016/j.matpr.2021.06.204

Sun, S., Lee, P., & Law, R., (2019). Impact of cultural values on technology acceptance and technology readiness. *International Journal of Hospitality Management. 77.* 89-96. https://doi.org/10.1016/j.ijhm.2018.06.017