

Platform Complacency: An Unrecognized Security Threat or A Positive Spillover in User Reliance on Anti-Phishing Tools?

Early stage paper

Siwei Jiang

Mississippi State University
sj1442@msstate.edu

Alaa Nehme

Mississippi State University
a.nehme@msstate.edu

Muriel-Larissa Frank

University of Luxembourg
muriel.frank@uni.lu

ABSTRACT

In 2023, the total number of phishing attacks was more than 2 billion. Especially with the prevalence of generative artificial intelligence, the urgency of combating phishing attacks is even more challenging than ever. Drawing upon the platform complacency perspective, this paper tries to explain users' reliance behavior on anti-phishing techniques based on their perceptions of the tools as well as their complacency on the platforms. Thus, this study contributes to the literature by examining users' complacency attitude, trust, and distrust to explain their reliance on phishing countermeasures. This study also provides practical implications such as the design of anti-phishing techniques should consider the impact of users' complacent state on their protective behavior.

Keywords

Platform complacency, anti-phishing tools, trust, reliance behavior.

INTRODUCTION

In a doctoral-level statistics course, students argued the advantages of ChatGPT despite its acknowledged inaccuracy. For instance, one said it provides comprehensive answers without getting lost in numerous Google answers and the answers seemed accurate enough. Although

Miller (1956) concludes that humans' information processing capacity is 7 plus or minus 2

*Proceedings of 2024 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop
Kennesaw, Georgia, USA*

items, the more precise limit is 4 according to Cowan's (2000) study. Time and attention are scarce resources for people in organizations (Pounds, 1969), which leads to the speed-accuracy tradeoff in decision-making (Larson & Hawkins, 2023). The example about ChatGPT reflects humans' reliance on technology regardless of its expenses of accuracy. Simon (1973) stated that attention management is important for organizations as humans and computers have processing limitations. Thus, information technology (IT) should improve users' attention allocated to the primary and critical tasks in organizational design (Simon, 1973). With technology advancing exponentially, IT adoption plays a crucial role in assessing innovation performance as well as business growth, and success (Baum, 2011; Pejic Bach, 2014; Yong et al., 2022).

Yet, organizations also face huge information security threats as their technology adoption increases. In 2023, the total phishing counts were over 2 billion, which was around 60% increase from 2022 (Zscaler, 2024). The Federal Bureau of Investigation (FBI) reported that phishing was the number one internet crime type regarding victim numbers and financial losses (FBI, 2023). Organizations have implemented different security policies and programs to combat increased security attacks. Meanwhile, researchers have also investigated this issue and many emphasized the importance of security awareness within organizations and some assume employees are rational (Bulgurcu et al., 2010; Ormond et al., 2016). Humans are the weakest link in the information system (IS) security chain (Warkentin et al., 2004). Organizations continually improve their information security integration and employ better security strategies. Also, IS researchers concentrate on analyzing employees' pro-security and compliance behaviors via human behaviors and cognition processes (Ormond et al., 2019). Schuetz et al. (2022) addressed the paradox between the accuracy of anti-phishing tools and people's lack of reliance on those

tools, and their user reliance model explained the three perceptions from perceived accuracy, perceived transparency, and perceived frequency that are mediated by trust and distrust in relationship with users' reliance on those tools. Particularly, the perceived frequency with perceived low accuracy together contributed to users' distrust and led to users' under-reliance on the tools. However, they did not include this relationship between perceived frequency and trust even though as their study 1 tested, the effect of perceived high frequency was mediated by perceived accuracy. Thus, in this study, we propose the following research question: how does users' platform complacency attitude impact their security behavior?

The purpose of this study is to explore the effect of computer users' platform complacency attitude on their reliance on security software such as anti-phishing tools. Discovered during a lab experiment on user cybersecurity behavior, Stafford (2021) proposed a new construct, platform complacency, which was users' overreliance attitudes on their computer operating system, and it was particularly manifested in Mac operating systems. Stafford (2021) classified that a computer user with platform complacency as an obviously nonsecure user, who lacks risk awareness and poses a big security threat to the systems. More importantly, this complacent attitude could be carried over into users' personal/ professional lives regardless if they use Mac or other computer systems. Thus, this conceptual paper tries to answer Stafford's call on the neglected computer security threat and propose future studies on its impact on organizational information security design.

LITERATURE REVIEW

Complacency

Raup (1926) compares complacency with equilibrium and considers complacency as the

optimum status for all live creatures. His concept of complacency is closer to a satisfactory stage of the human mind and it contains four phases, which are the formative, the quiescent, the disturbance, and the reduction phases. Thus, complacency is an ongoing process, and any subsequent changes ultimately will return to that optimum complacent condition (Raup, 1926). In contemporary literature, complacency has been one of the major studies in the aviation, artificial intelligence, and healthcare domains (Mackellar et al., 2011; Merritt et al., 2019; Parasuraman & Manzey, 2010; Parikh et al., 2019). Researchers in those disciplines usually define the term as automation-induced complacency, in which human operators' over-reliance on automation had potentially led to (fatal) incidents. Some studies used it with automation bias interchangeably (Wright et al., 2017) and some treat them as distinct constructs but both of them share some commonalities (Parasuraman & Riley, 1997; Parasuraman & Manzey, 2010). For these two automation-related issues, the potential consequence is an overreliance on automation due to automation failure (Parasuraman & Manzey, 2010). With the status of complacency, users lack the mindset of seeking other resources or information to make sound judgments to ensure their actions are accurate; rather, they tend to mindlessly follow the automation recommendations (Skitka et al., 1999). For automation-induced complacency and automation, researchers classify them as overreliance and over-compliance (Wickens et al., 2015). In this case, overreliance indicates an error of omission when the automation fails to identify errors while over-compliance indicates an error of commission when the automation incorrectly identifies an error.

Generally, complacency consists of a false assumption of a well-controlled situation (by automation) and undermining potential risks; also, the former is used in the context of alerting systems while the latter is more about decision aids (Wickens et al., 2015). Lack of situational

awareness also is one of the leading factors for complacency (Jones et al., 1996). Although one would suppose that the greater knowledge of the automation of a user process, the less the user would be less likely to have either automation bias or complacency, studies have shown a similar occurrence rate for naive and expert users (Parasuraman & Manzey, 2010). Another study (Yetgin et al., 2015) shows that the development of complacency in decision aids such as stock assistants overall is irrelevant to the accuracy of the decision aids. Although it does have a little short-term impact on users' reliance, the users ultimately become complacent and reliant. They conclude that users are not as rational as assumed in using technology such as decision-making aids; rather, System 1 thinking becomes dominant over time even when users perceive the inaccuracy of the aids (2015).

While the majority of studies define complacency as an attitude, some researchers look at complacency from another angle and test it as a behavior that is directly related to unfavorable outcomes (Wright et al., 2017). In automation disciplines, Wright et al. 's (2017) study on complacency behavior, their experiment results showed that information transparency could reduce people's Complacency behavior. Another complacency behavior study by Parasuraman et al. (1993) concludes that the state of complacency usually is induced in a highly reliable automated environment, though they assume that overconfidence alone would not be sufficient to lead to complacency rather than the result of a combination with situational factors such as fatigue. (Parasuraman et al., 1993).

In the information systems domain, similar constructs include habit, which is described as a learned response followed by automatic behavior (Limayem et al., 2007; Vedadi & Warkentin, 2018). In the context of computer security, we adopt the definition of platform complacency attitude from Stafford (2021) as an “ill-advised dependence upon specific computing

platforms and protective workplace technology implementations for protection" (p. 3814). More specifically, it indicates users' complacency attitudes with the Mac operating system (MacOS) as the result of users' perceived quality, safety, and personal preferences on MacOS. For example, from the data collecting stage to the coding phase, Stafford (2021, P. 3819) accounted for those prescriptions regarding MacOS:

After a bad exploit on [my] PC, I bought a Mac; I knew it had a potential security advantage.

I feel safe using a Mac, but I don't really know what's going on with it.

Those perceptions can come from personal experiences, their social interactions with others in their work or life circles, professional knowledge, or even just merely based on brand marketing strategies. According to Ajzen's (2020) theory of planned behavior, the accuracy of such perception does not matter as long as the users are influenced by their perception of the behavior. The theory of social response states that people mindlessly apply social rules and expectations when they interact with computers, so automatic processes can trigger humans' mindlessness compared to intentional processes (Nass & Moon, 2000). Similarly, Kahneman (2011) differentiates human thoughts into System 1 thinking that represents intuitive and involuntary thinking, and System 2 thinking requires deliberation and logical sensemaking to make sound judgments. For users with platform complacency attitude induced by their use of Mac, we speculate it brings the users with a superior and safer perception of Mac, which in turn reinforces their perception with their future interaction and usage with Mac. Adekotoju et al. (2020) compared different OS in the market and concluded that MacOS had the greatest reliability and negligible security threats compared to other OS. While the perception could be changed over time due to other internal or external factors such as learning new information regarding the MacOS or

experiencing information security breaches. Based on Bayes' theorem, humans' belief systems are in a spectrum, and their perceptions are conditioned on the probability of different hypotheses and the different probabilities can be changed later on (Bermiidez, 2020). Therefore, MacOS users might adjust their perception of the security or the safety of the system, leading to reduced platform complacency. However, those potential factors are outside of the scope of this study.

Trust and distrust

Across disciplines, trust is perceived and defined differently. In the IS domain, McKnight and Chervany (2001) proposed a typology of trust, namely, disposition to trust, institution-based trust, trusting beliefs, trusting intention, and trust-related behavior. Trust in IT has been operationalized in three components and the propensity to trust general technology indirectly affects trust in a specific technology (favorable features) (McKnight et al., 2011). Other studies have evidenced institution-based trust as a strong predictor of trust in technology artifacts (Vance et al., 2008). Trust in technology processes higher risk uncertainties due to the lack of social cues for trust building. With the context of human-automation interaction, trust has been conceptualized as two different facets, trust as an attitude and behavior (Hoesterey & Onnash, 2023). The former relates to the human cognition aspect (Lee & See, 2004) and the latter trust leads to reliance on automation (Hoff & Bashir, 2015). Studies have shown that interactions between humans and automation improve trust behavior, which improves users' reliance on automation.

In early studies, researchers usually treat them as two opposite ends of a single continuum (Trotter, 2002), but some view them as separate and distinct constructs (Hardin, 2002; McKnight & Choudhury, 2006; Van de Walle & Six, 2014). Distrust represents a negative expectation regarding the subject matter (Komiak & Benbasat, 2008; Van de Walle & Six, 2014). Therefore,

a clear distinction between distrust and trust is important as they process different preconditions, and ignoring their differences would lead to undermining their existences (McKnight & Chervany, 2001). In Schuetz et al. 's (2022) studies, they conclude that users' reliance on the tools is reduced by their distrust, which is caused by the high perceived frequency of the tools when the accuracy rate is not high.

Reliance

Trust regards one's attitudes toward the outside world and emphasizes the relationship, which is more of a dynamic process rather than a final decision. Our trust exists in different levels and types and it is contingent on the situation and parties involved. Though some researcher defines reliance as trust behavior, the two constructs are different on several levels based on extant literature studies, some are focused on the intention of using IT rather than assessing the actual behavior (Vance, 2008). Some view reliance on artifacts as dependable habits produced by technologies that users either choose to rely upon or not (Deley & Dubois, 2020).

Reliance also differs from complacency as reliance is a result of expectation when the technology fulfills its alleged purpose (Campbell et al., 2007). Early studies compared interpersonal trust and trust between humans and machines, and by drawing literature on the formal, those studies concluded that trust in machines has an impact on human's reliance on machines (Muir, 1987). Some studies tested the relationship between trust and reliance on automated systems, and their study results indeed demonstrated there is a positive effect (Parasuraman et al., 2008; Wang et al., 2009). In this study, users' reliance behavior on the tools are defined as their actual reliance on phishing website detection tool-based security warnings, and

this behavior will be measured as whether they ignore such warnings and click phishing websites or not.

The previous literature review concentrates on the cognitive aspects of the constructs of the study, the rest of the literature review focuses on phishing attacks and anti-phishing tools.

Phishing and anti-phishing tools

There are numerous definitions of phishing but some common terms define this as a form of social engineering or fraudulent activity by disguising as a legit email or website in order to trick victims into revealing any sensitive information (CISA, 2021; Merwe et al, 2005; Schuetz et al., 2022). The most common phishing methods include link manipulation or filter evasion insert in an email or website forgery (Bhuvana et al., 2021), and spear phishing techniques are used to target specific employees or companies (Sharma et al., 2022).

Extant literature showed that certain attributes that appear more prevalent among phishing attack victims. For example, one study shows that self-efficacy, web experience, security awareness, trust, perceived risk and suspicion of humanity (Vishwanath et al., 2011; Wright & Marett, 2010) are all associated with vulnerability to phishing attacks. Surprisingly, other studies show that phishing knowledge and awareness are negatively correlated with detecting phishing emails (Diaz et al., 2018), which could be due to users' overconfidence and/ or underestimation of phishing risks. Studies show that domain knowledge affects users' perceived self-efficacy and induces two coping behaviors (Arachchilage & Love, 2014). Problem-solving approach for users with high self-efficacy who see phishing attacks as a challenge that needs to be solved; in contrast, users with low self-efficacy take an emotion-focused approach since they see phishing attacks as a threat and prefer to avoid it (Arachchilage & Love, 2014).

According to Schuetz et al. (2022), anti-phishing tools are protective software that is used for preventing and detecting phishing attacks, and it has two types of approaches. The first approach is lookup, in which the program lookup received emails and checks whether the senders match with the existing blacklist; however, this approach cannot detect novel attacks since it takes more than 48 hours for a novel attack to be identified by a blacklist. On the other hand, the classification approach is based on the existing information and knowledge of the phishing attacks and then uses heuristics to analyze the emails and evaluate the odds of an email being fraudulent. Thus, this approach is also called the probability approach and usually can achieve over 90% accuracy in its predictions.

THEORETICAL FOUNDATIONS

In social psychology studies, several dual process theories focus on cognitive processes regarding different kinds of thinking. The heuristic-systematic model contains two modes that represent humans' information processes, whereas the heuristic model suggests simple decision rulemaking that requires less cognitive effort and resources while the systematic model uses comprehensive and analytical thinking for logical decision-making (Chaiken & Ledgerwood, 2012). Similarly, Kahneman (2008) categorizes human thinking as System 1 and System 2 which serve different functions, where daily routine types tasks are usually conducted by System 1 thinking, but more complex situations require System 2 thinking as more logical reasoning and reflective thinking to achieve desired and less biased outcomes. When users have multiple tasks on hand and especially if security is not their primary concern for their job, and their complacency level is the highest, they would just rely on heuristic or System 1 thinking to guide their actions such as whether to trust the anti-phishing tools and then rely on relevant recommendations/ warnings or not. Studies

in different disciplines have shown that people, in general, are less likely to notice issues with

reliable systems especially related to the decision-making process when their workload is excessive (Challen et al., 2018).

The anti-phishing tool interrupts the equilibrium status of complacency, which forces one to enter the disturbance phase of complacency (Raup, 1926). With the natural tendency to return to equilibrium status. In this situation, they would follow the recommendations/ warnings, which eliminates the security concerns. As a result, the security of the computer system returns to its equilibrium status.

HYPOTHESIS DEVELOPMENT

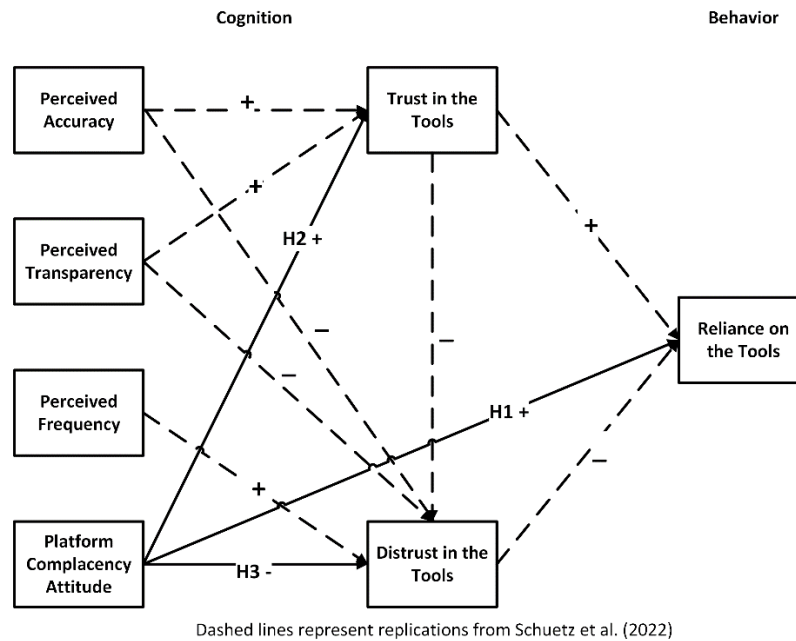


Figure 1. Conceptual model (adapted from Schuetz et al, 2022)

Schuetz et al. 's (2022) study, we propose that users' platform complacency is associated with users' trust in the anti-phishing tools. With a complacent attitude towards computer systems, a user would have a higher tendency to trust the application installed in the system. Also, the antecedents of perceived accuracy and transparency in the user reliance model act as the cues in the decision-

making process regarding the transaction-specific uncertainties that users would normally hold (Grabner-Kräuter, 2002). For the system-dependent uncertainties, a platform complacency attitude will reduce those uncertainties derived from hardware and software. Normally, people will proactively seek more information about something that they are not certain about according to the uncertainty reduction theory.

However, Mac users hold the belief that Mac is simple to use and its system is safer and more secure compared to other OS. According to Stafford (2021), platform complacency is not only about the system but also the software within the system. The theory of planned behavior suggests that accuracy of users' certain beliefs is not of concern when the determinant is whether their beliefs will influence their behaviors (Ajzen, 2020). Extant literature on complacency is more concerned about the negative effects such as the omission of errors of complacency. This study is more interested in exploring how users' complacency with the computer operating system as a whole would improve their trust in the anti-phishing software that is used to protect the system and sensitive data. As such, Mac users' complacent attitude will lead to a higher trust attitude and then to the anti-phishing tools. Studies also provide evidence that trust has an impact on users' reliance on automated systems (Lee & See, 2004; Dzindolet et al., 2001; Muir, 1987; Wang et al., 2009). Therefore, we hypothesize the following:

H1: Platform complacency increases users' reliance on the tools.

According to Grabner-Kräuter (2002), two types of uncertainties are related to consumer online behavior. The system-based behavior is concerned with computer systems and software. Under the premise of platform complacency, MacOS users possess much less system-based uncertainty with high trust in the computer systems, therefore, we hypothesize:

H2: Platform complacency increases users' trust in the tools.

H3: Platform complacency decreases users' distrust of the tool.

METHODOLOGY PROPOSAL

Platform complacency is a multidimensional construct with three factors - better performance, safer security protection, and general preference based on the qualitative study by Stafford (2021). For study 1, a two-step construct validation study would be used to assess measurement properties tests by conducting a confirmatory factor analysis via AMOS (Anderson & Gerbing, 1988). Discriminant validity would be very critical for the subsequent study to establish the distinction between platform complacency with other constructs, especially trust. Once the reliability and validity of the construct platform complacency are established based on current criteria (Hu & Bentler, 1999), the structural relationships including the second-order construct, platform complacency as well as the interrelationships among other constructs in the model would be carried out by using AMOS for a structural equation model. Control variables included in the original study will also be tested (Schuetz et al., 2022). Two groups of participants are needed for the studies, one group for MacOS users and another group for other PC users.

CONCLUSION

For future studies, cognitive theories such as the theory of self-perception (Bern, 1972) could be incorporated into the model to explain the underlying cognitive aspect of the complacent attitude in users' security behaviors according to Stafford (2023). Alternatively, it would be reasonable to assume that MacOS users who hold high beliefs in Mac, which leads them to the status of complacency, would be able to ignore the anti-phishing recommendations/ warnings. Especially, as MacOS users believe that the Mac "itself, is a palliative to security threats" (Stafford, 2021). By holding firm to their original beliefs, they choose self-affirmation, which causes them to be complacent about the security feature and no-virus of Mac, and rely on the MacOS rather than the additional anti-phishing tools. As a result, users are more likely to distrust the tools and subsequently rely less on the tools.

REFERENCES

- Adekotujo, A., Odumabo, A., Ademola, A. & Aiyeniko, O. (2020). "A comparative study of operating systems: Case of Windows, UNIX, Linux, Mac, Android and iOS," *International Journal of Computer Applications* (176), pp. 16-23. 10.5120/ijca2020920494.
- Ajzen, I. and Fishbein, M. 1980. Understanding attitudes and predicting social behavior. Prentice-Hall.
- Ajzen, I. 2020. "The theory of planned behavior: Frequently asked questions," *Human Behavior and Emerging Technologies* (2:4), pp. 314–324. 10.1002/hbe2.195
- Anderson, J. C., & Gerbing, D. W. 1988. "Structural equation modeling in practice: A review and recommended two-step approach," *Psychological Bulletin* (103:3), pp. 411–423. 10.1037/0033-2909.103.3.411
- Arachchilage, N. & Love, S. 2014. "Security awareness of computer users: A phishing threat avoidance perspective," *Computers in Human Behavior* (38), pp. 304–312. 10.1016/j.chb.2014.05.046.
- Bermúdez, J.L. 2020. Cognitive science: An introduction to the science of the mind, Cambridge University Press.
- Bhuvana, B. A., Shetty, T. & Naik, P. 2021. "A study on various phishing techniques and recent phishing attacks," *International Journal of Advanced Research in Science, Communication and Technology* pp. 142-148. 10.48175/IJARSCT-2094.

- Campbell, E., Sittig, D., Guappone, K., Dykstra, R. & Ash, J. 2007. "Overdependence on technology: An unintended adverse consequence of computerized provider order entry," *AMIA. Annual Symposium proceedings / AMIA Symposium* (9), pp. 94-8.
- Diaz, A., Sherman, A. & Joshi, A. 2019. "Phishing in an academic community: A study of user susceptibility and behavior," *Cryptologia* (44), pp. 1-15. 10.1080/01611194.2019.1623343.
- Deutsch, M. 1958. "Trust and suspicion," *Journal of Conflict Resolution* (2), pp. 265-279. 10.1177/002200275800200401
- Dzindolet, M. T., Pierce, L. G., Beck, H. P., Dawe, L. A., & Anderson, B. W. 2001. "Predicting misuse and disuse of combat identification systems," *Military Psychology* (13:3), pp. 147–164. 10.1207/S15327876MP1303_2
- Deley, T. & Dubois, E. 2020. "Assessing trust versus reliance for technology platforms by systematic literature review," *Social Media + Society* (6) 205630512091388. 10.1177/2056305120913883.
- FBI. (2023, March 22). *Internet crime complaint center releases 2022 statistics*. FBI. Retrieved from <https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crimecomplaint-center-releases-2022-statistics>
- Festinger, L. 1957. *A theory of cognitive dissonance*. Stanford University Press.
- Furnell, S. 2010. "Mac security: An Apple that can't be bitten?" *Network Securit* pp. 7-11. 10.1016/S1353-4858(10)70014-3.
- Garber, M. (2012, June 24). "It's official: Apple Computers are no longer virus-free," *The Atlantic*. Retrieved from <https://www.theatlantic.com/technology/archive/2012/06/its-officialapple-computers-are-no-longer-virus-free/258902/>
- Grabner-Kräuter, S. 2002. "The role of consumers' trust in online-shopping," *Journal of Business Ethics* (39), pp. 43-50. 10.1023/A:1016323815802.
- Guo, K.H., Yuan, Y., Archer, N.P., & Connelly, C.E. 2011. "Understanding nonmalicious security violations in the workplace: A composite behavior model," *Journal of Management Information Systems* (28), pp. 203 - 236.
- Hardin, R. 2002. *Trust and trustworthiness*. Russell Sage Foundation.
- Hoesterey, S. & Onnasch, L. 2023. "The effect of risk on trust attitude and trust behavior in interaction with information and decision automation," *Cogn Tech Work* (25), pp. 15–29 10.1007/s10111-022-00718-y
- Kahneman, D. 2011. *Thinking, fast and slow*. Farrar, Straus and Giroux.
- Komiak, S. & Benbasat, I. 2008. "A two-process view of trust and distrust building in recommendation agents: A process-tracing study," *J. AIS* (9). 10.17705/1jais.00180.
- Lee, J. & See, K. 2004. "Trust in automation: Designing for appropriate reliance," *Human Factors* (46), pp. 50-80. 10.1518/hfes.46.1.50.30392.
- Luhmann, N. 2000. Familiarity, confidence, trust: Problems and alternatives in Gambetta, Diego (ed.) *Trust: Making and Breaking Cooperative Relations, electronic edition*, Department of Sociology, University of Oxford, chapter 6, pp. 94-107
- Merwe, A. v. d., Marianne, L., & Marek, D. 2005. "Characteristics and responsibilities involved in a phishing attack," in *WISICT '05: Proceedings of the 4th international symposium on information and communication technologies*. Trinity College Dublin, pp. 249–254.
- Muir, B. 1987. "Trust between humans and machines, and the design of decision aids," *International Journal of Man-Machine Studies* (27), pp. 527-539. 10.1016/S0020-7373(87)80013-5.

- Mcknight, D. & Chervany, N. 2001. "Trust and distrust definitions: One bite at a time," 10.1007/3-540-45547-7_3.
- Mcknight, D. & Choudhury, V. 2006. "Distrust and trust in B2C e-commerce: Do they differ?" *Proceedings of the ACM Conference on Electronic Commerce*. pp. 482-491. 10.1145/1151454.1151527.
- Mcknight, D., Carter, M., Thatcher, J. & Clay, P. 2011. "Trust in a specific technology: An investigation of its components and measures," *ACM Transactions on Management Information Systems* (2), pp. 12-32. 10.1145/1985347.1985353.
- Nass, C., & Moon, Y. 2000. "Machines and mindlessness: Social responses to computers," *Journal of Social Issues* (56:1), pp. 81–103. 10.1111/0022-4537.00153
- PC pain persists in Q1 2023 due to excess inventory and poor demand, according to IDC tracker. IDC. (2023, April 9). Retrieved from <https://www.idc.com/getdoc.jsp?containerId=prUS50565723>
- Parasuraman, R., Molloy, R., and Singh, I. L. 1993. "Performance consequences of automation induced 'complacency'," *Int. J. Aviat. Psychol* (3), pp. 1–23. 10.1207/S15327108ijap0301_1
- Parasuraman, R. & Manzey, D. 2010. "Complacency and bias in human use of automation: An attentional integration," *Human Factors* (52), pp. 381-410. 10.1177/0018720810376055.
- Parasuraman, R., & Riley, V. 1997. "Humans and automation: Use, misuse, disuse, abuse," *Human Factors* (39:2), pp. 230–253. 10.1518/001872097778543886
- Pounds, W. F. 1965. "The process of problem finding," *Industrial Management Review* (11:1): p.1.
- Raup. 1926. *Complacency: the foundation of human behavior*. Macmillan.
- Schneider, S., Liu, Y., Tomita, K. & Kanda, T. 2022. "Stop ignoring me! On fighting the trivialization of social robots in public spaces," *ACM Transactions on Human-Robot Interaction* (11), pp. 1-23. 10.1145/3488241.
- Schuetz, S., Steelman, Z., & Syler, R. 2022. "It's not just about accuracy: An investigation of the human factor in users' reliance on anti-phishing tools," *Decision Support Systems* (163). 113846. 10.1016/j.dss.2022.113846.
- Sharma, P., Dash, B. & Ansari, M. F. 2022. "Anti-phishing techniques -A review of cyber defense mechanisms," *IJARCCCE* (11). 10.17148/IJARCCCE.2022.11728.
- Simon, H.A. 1973. "Applying information technology to organization design," *Public Administration Review* (33), p. 268.
- Simon, L., Greenberg, J. & Brehm, J. 1995. "Trivialization: The forgotten mode of dissonance reduction," *Journal of Personality and Social Psychology* (68:2), pp. 247–260. 10.1037/0022-3514.68.2.247
- Stafford, T. 2021. "Platform-dependent computer security complacency: The unrecognized insider threat," *IEEE Transactions on Engineering Management* pp. 1-12. 10.1109/TEM.2021.3058344.
- Trotter, A. 2002. "Plagiarism controversy engulfs Kansas school," *Education Week* (5).
- van Dongen, K., & van Maanen, P.-P. 2013. "A framework for explaining reliance on decision aids," *International Journal of Human-Computer Studies* (71:4), pp. 410–424. 10.1016/j.ijhcs.2012.10.018
- Van de Walle, S. & Six, F. 2014. "Trust and distrust as distinct concepts: Why studying distrust in institutions is important," *Journal of Comparative Policy Analysis* (16). 10.1080/13876988.2013.785146.

- Vance, T. & Elie-Dit-Cosaque, C. & Straub, D. 2008. "Examining trust in information technology artifacts: The effects of system quality and culture," *Journal of Management Information Systems* (24). 10.2753/MIS0742-1222240403.
- Vedadi, A., & Warkentin, M. 2018. "Secure behavior over time: Perspectives from the theory of process memory," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, (49:SI), pp. 39-48. 10.1145/3210530.3210534
- Wickens, C., Clegg, B., Vieane, A. & Sebok, A. 2015. "Complacency and automation bias in the use of imperfect automation," *Human Factors* (57). 10.1177/0018720815581940.
- Wright, J., Chen, J., Barnes, M. & Hancock, P. 2017. "Agent reasoning transparency: The influence of information level on automation-induced complacency."
- Wang, L., Jamieson, G. & Hollands, J. 2009. "Trust and reliance on an automated combat identification system," *Human Factors* (51). pp. 281-91. 10.1177/0018720809338842.
- Yetgin, E., Jensen, M. & Shaft, T. 2015. "Complacency and intentionality in IT use and continuance," *AIS Transactions on Human-Computer Interaction* (7). pp. 17-42. 10.17705/1thci.00064.
- Zscaler. 2024. *Zscaler threatlabz 2024 phishing report*.
<https://www.zscaler.com/campaign/threatlabz-phishing-report>