A Course on Social Engineering
Phishing & URL Analysis

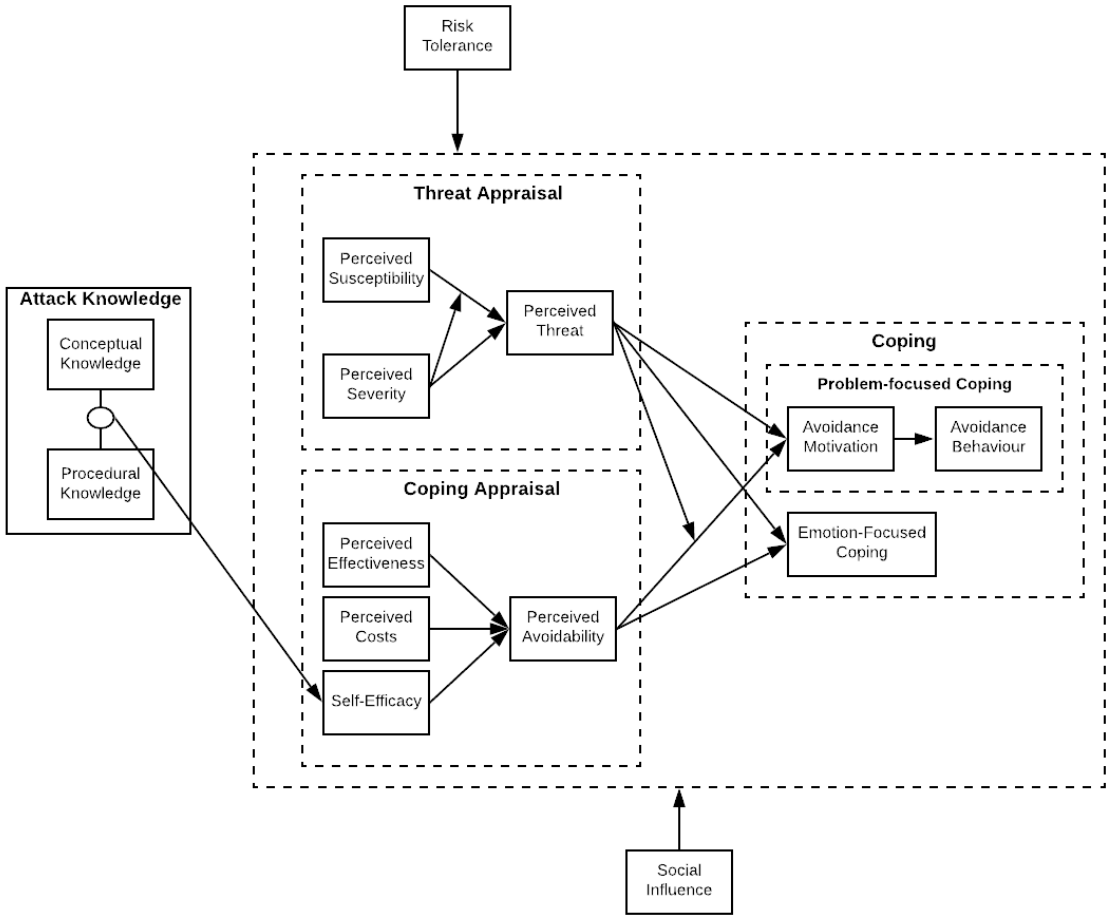
Why Certain Users Do Not Protect Themselves

Keith S. Jones
Texas Tech University
Spring 2021

Some Users Do Not Protect Themselves

- Security professionals often assume users will protect themselves if
  - They are aware of the threat
  - They know how to prevent the threat
- Sometimes non-experts consciously decide to NOT protect themselves from threats
  - Some decide against guarding their passwords (Weirich & Sasse, 2001)
  - Some decide against guarding their e-mail (Renaud et al., 2014)
  - Some decide against guarding their online privacy/cybersecurity (Kang et al., 2015; Theofanos et al., 2017)
  - Some decide against installing operating system or application updates (Ion et al., 2015; Vaniea et al., 2014)
  - Some decide against using encryption (Wu & Zappalla, 2018)
  - Some decide against using two-factor authentication (Ion et al., 2015)
- Why would they do that?
  - Such choices create major security vulnerabilities

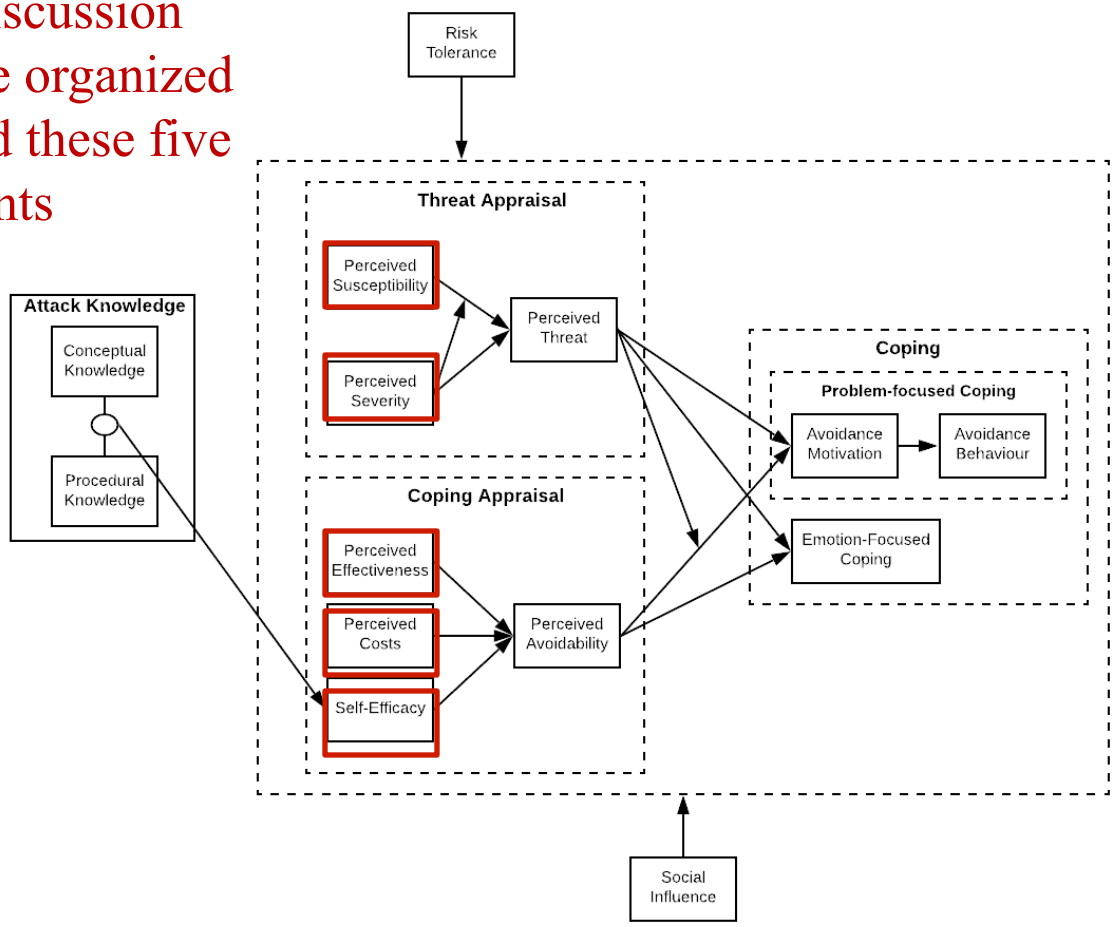
Modified Technology Threat Avoidance Model (MTTAT)



Liang and Xue (2009); Arachchilage and Love (2014)

Modified Technology Threat Avoidance Model (MTTAT)

Our discussion will be organized around these five elements



Liang and Xue (2009); Arachchilage and Love (2014)

Key Elements

- Perceived Susceptibility
  - How likely is that I am being attacked?
- Perceived Severity
  - How severe are the consequences if the attack is successful?
- Perceived Effectiveness
  - Are known threat countermeasures effective?
- Perceived Costs
  - How much time and/or money is required to execute the threat countermeasures?
- Self-Efficacy
  - Can I successfully implement the threat countermeasures?

Perceived Susceptibility

- Some non-experts do not think they are very susceptible to threats

- Some non-experts think they are not likely to be targeted because
  - They are not wealthy or important enough to warrant being attacked, i.e., they are not "big fish" (Kang et al., 2015; Kauer et al., 2013; Prettyman et al., 2015; Renaud et al., 2014; Sasse et al., 2001; Theofanos et al., 2017; Ur et al., 2016; Wash, 2010; Wash & Rader, 2015; Weirich & Sasse, 2001)
  - They think threats do not target individuals, just organizations (Kauer et al., 2013; Wash, 2010)
- Some non-experts think they do not have to protect themselves because
  - The systems with which they interact (e.g., email) are inherently secure (Renaud et al., 2014).

Perceived Severity

- Some non-experts do not think cybersecurity threat consequences are severe
- Some non-experts do not care whether someone violates their privacy (Kang et al., 2015)
- Some non-experts think they have nothing to hide (Kang et al., 2015; Renaud et al., 2014; Wu & Zappalla, 2018), so cybersecurity threats could not harm them (Renaud et al., 2014; Sasse et al., 2001; Viseu et al., 2004; Weirich & Sasse, 2001)
- On a related note, there is evidence that in the absence of information about perceived severity, non-experts may not think about potential consequences of a threat (Kauer et al., 2012)

Perceived Effectiveness

- Some non-experts do not consider cybersecurity threat countermeasures to be particularly effective, and have a generally fatalistic attitude

- Some non-experts think that they have no real control over their privacy or security (Prettyman et al., 2015).
- Some non-experts think that attackers will always be one step ahead of them (Dourish et al., 2003) and can always find a way to access what they want (Weirich & Sasse, 2001)

Perceived Costs

- Some experts think threat countermeasures are costly

- Some non-experts think actions to protect themselves are an inconvenient distraction from the task at hand (Dourish et al., 2003; Hardee et al., 2006; Kang et al., 2015; Sasse et al., 2001) and negatively affect their productivity (Vaniea et al., 2014)
- Some non-experts think tools that they would use to protect themselves are not effective and have poor usability (Kang et al., 2015)

Self-Efficacy

- Some non-experts' self-efficacy regarding executing cybersecurity threat countermeasures is probably quite low

- Some non-experts times think they do not know much about cybersecurity (Theofanos et al., 2017) or, more specifically, that they do not know how to protect their cybersecurity (Kang et al., 2015)

Not My Job

- Some non-experts think it is someone else's job to protect their cybersecurity (Dourish et al., 2003; Gross & Rosson, 2007; Prettyman et al., 2015; Renaud et al., 2014; Theofanos et al., 2017), which has come to be known as the "Not My Job" perspective in the literature (Prettyman et al., 2015)
- They point to another individual, such as a knowledgeable friend, family member, colleague, or roommate, who ensures their security by, for example, setting up their computer in a secure manner (Dourish et al., 2003)
- They point to organizations, e.g., they argued that it was their e-mail service provider's job to keep others out of their e-mail (Renaud et al., 2014), a Web site's responsibility to ensure its users' online privacy (Prettyman et al., 2015; Theofanos et al., 2017), or an online bank's responsibility to ensure its customers' security (Dourish et al., 2003)

Thought Co-Occurence

- It is important to note that the thoughts described earlier often occur together (Renaud et al., 2014; Vaniea et al., 2014)
- For example, non-experts who decided against encrypting their e-mails noted they were not important enough to attack, e-mail systems are secure, they have nothing to hide, no harm would come to them if someone did access their e-mail, private e-mails are not particularly critical, and it was not their job to secure their e-mail

- That suggests non-experts have multiple reasons why they they decide against protecting themselves from cybersecurity threats
- That likely makes it even more likely that they will decide against protecting themselves

Summary

- Certain non-experts think in ways that undermine cybersecurity
  - They think they will not be attacked
  - They think attack consequences are not serious
  - They think threat countermeasures are not effective
  - They think threat countermeasures are expensive/disruptive
  - They think they do not know how to execute threat countermeasures
  - They think it is not their job to protect their cybersecurity

- According to MTTAT, such thoughts should result in very low motivation to do anything to prevent the attack
- Users who hold these views are the weakest links in your cybersecurity systems

Implications

- This research helps to dispel the idea that users will protect themselves if they are made aware of the threat and told how to prevent it
  - Unfortunately, the situation is much more complicated than that

- This research illuminates some of the challenges that will have to be overcome to convince users who hold these views to protect their cybersecurity
  - Addressing this issue will not be as simple as telling users they are susceptible, attack consequences are severe, etc.
  - Rather, addressing this issue will take a sustained effort that convinces user to change their views about this topics

References

- Dourish, P., De La Flor, J. D., & Joseph, M. (2003). Security as a practical problem: Some preliminary observations of everyday mental models. In Proceedings of CHI 2003 workshop on HCI and security systems. ACM.
- Gross, J. B., & Rosson, M. B. (2007). Looking for trouble: Understanding end-user security management. In Proceedings of the 2007 symposium on computer human interaction for the management of information technology (CHIMIT '07). ACM. https://doi.org/10.1145/1234772. 1234786
- Hardee, J. B., West, R., & Mayhorn, C. B. (2006, May). To download or not to download: An examination of computer security decision making. Interactions, 13(3), 32–37. https://doi.org/10.1145/1125864. 1125887
- Ion, I., Reeder, R., & Consolvo, S. (2015). "... No one can hack my mind": Comparing expert and non-expert security practices. In Eleventh symposium on usable privacy and security (SOUPS) (pp. 327–346). ACM Press.

References

- Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). “My data just goes everywhere:” user mental models of the internet and implications for privacy and security. In Symposium on Usable Privacy and Security (SOUPS) (pp. 39–52). USENIX Association.
- Kauer, M., Günther, S., Storck, D., & Volkamer, M. (2013). A comparison of American and German folk models of home com- puter security. In International conference on human aspects of infor- mation security, privacy, and trust (pp. 100–109). Springer.
- Kauer, M., Pfeiffer, T., Volkamer, M., Theuerling, H., & Bruder, R. (2012). It is not about the design-it is about the content! Making warnings more efficient by communicating risks appropriately. GI- Edition – Lecture Notes in Informatics (LNI).
- Liang, H., & Xue, Y. (2009, March). Avoidance of information technol- ogy threats: A theoretical perspective. MIS Quarterly, 33(1), 71–90. https://doi.org/10.2307/20650279

References

- Prettyman, S. S., Furman, S., Theofanos, M., & Stanton, B. (2015). Privacy and security in the brave new world: The use of multiple mental models. In International conference on human aspects of infor- mation security, privacy, and trust (pp. 260–270). Springer International Publishing.
- Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014). Why doesn't Jane protect her privacy? In E. De Cristofaro & S. J. Murdoch (Eds.), Privacy enhancing technologies (PETS). Lecture notes in computer science (pp. 8555). Springer.
- Sasse, M. A., Bronstoff, S., & Weirich, D. (2001, July). Transforming the "Weakest Link": A human-computer interaction approach for usable and effective security. BT Technology Journal, 19(3), 122–131. https:// doi.org/ 10.1023/A:1011902718709

References

- Theofanos, M. F., Stanton, B., Furman, S., Prettyman, S. S., & Garfinkel, S. (2017). Be prepared: How US government experts think about cybersecurity. In Network and distributed system security symposium (NDSS) (pp. 1–11). Information Society. https://doi.org/ 10.14722/usec.2017.23006
- Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016). Do users' perceptions of password security match reality?. In Proceedings of the 2016 CHI conference on human factors in computing systems (pp. 3748–3760). ACM.
- Vaniea, K. A., Rader, E., & Wash, R. (2014). Betrayed by updates: How negative experiences affect future security. In Proceedings of the SIGCHI conference on human factors in computing systems (pp. 2671–2674). ACM. https://doi.org/10.1145/2556288.2557275

References

- Viseu, A., Clement, A., & Aspinall, J. (2004). Situating privacy online: Complex perceptions and everyday practices. Information, Communication & Society, 7(1), 92–114. https://doi.org/10.1080/ 1369118042000208924
- Wash, R. (2010). Folk models of home computer security. In Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS) (1–11). ACM Press.
- Wash, R., & Rader, E. J. (2015). Too much knowledge? Security beliefs and protective behaviors among United States internet users. In Proceedings of the symposium on usable privacy and security (SOUPS) (pp. 309–325). ACM.
- Weirich, D., & Sasse, M. A. (2001). Pretty good persuasion: A first step towards effective password security in the real world. In Proceedings of the 2001 workshop on new security paradigms (NSPW ’01) (pp. 137–143). ACM.

References

- Wu, J., & Zappalla, D. (2018). When is a tree really a truck? Exploring mental models of encryption. In Proceedings of the fourteenth sympo- sium on usable privacy and security (SOUPS) (pp. 395–409). USENIX Association.