A Course on Social Engineering
Phishing & URL Analysis

How Social Engineers Use Persuasion Principles During Vishing Attacks

Keith S. Jones
Texas Tech University
Spring 2021

Vishing

- Vishing (voice phishing) occurs when an attacker attempts to obtain information from a victim over the phone (Maggi, 2011)
- These attacks can be launched using phone numbers and personal information mined from caller ID and social media applications that are used by millions (Gupta et al., 2015)
  - For example, a caller claiming to be from the victim's bank might say unusual charges were detected on the victim's account, and then ask the victim to confirm their credit card information

Persuasion Principles

- Social Engineering relies on an attacker being persuasive
- Thus, researchers have investigated how attackers utilize persuasion techniques, and several collections of persuasion principles have emerged
  - Gragg (2003) identified seven psychological triggers
  - Cialdini (2007) reported six principles of influence
  - Stajano and Wilson (2011) identified seven principles of general scams

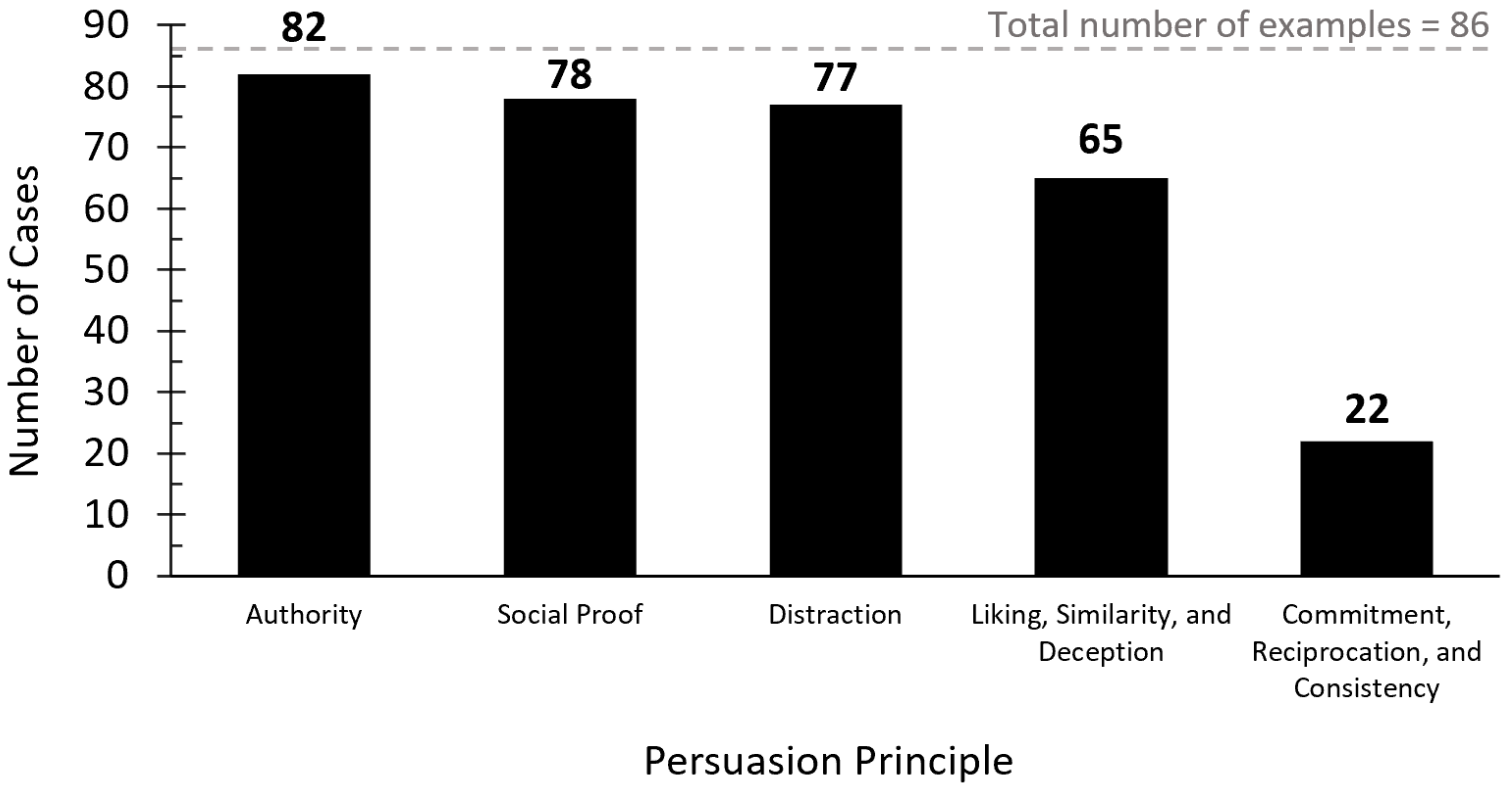
An Integrated Taxonomy of Persuasion During SE Attacks

- Ferreira, Coventry, and Lenzini (2015) integrated principles mentioned in Gragg (2003), Cialdini (2007), and Stajano and Wilson (2011) (see Ferreira et al., 2015 for detailed method)
- Their five Principles of Persuasion in Social Engineering (PPSEs)
  - Authority. People are conditioned to respond to authority and tend to follow those they think are experts or authority figures
  - Commitment, reciprocation, and consistency. People have more confidence in decisions after publicly committing to following through with a given action. People also tend to believe others, desire to appear consistent in their actions, and reciprocate the acts of others
  - Distraction. People singularly focus attention on their needs, potential gains or losses, time pressure, etc. while ignoring other things that might be happening around them.
  - Liking, similarity, and deception. People prefer and listen to others that they know or like, are similar to or familiar with, and/or are attracted to
  - Social proof. People tend to go along with the crowd and want to be included. They feel diminished responsibility for their actions and let their guard down when others appear to be involved in the same behaviors and risks

What PPSEs Do Vishers Use?

- Jones, Armstrong, Tornblad, and Namin (2021) examined 86 examples of real-world vishing attacks, which were coded using questions derived from Gragg (2003), Cialdini (2007), Stajano and Wilson (2011), and Mouton et al. (2014) according to Ferreira and colleagues' (2015) five PPSEs
- They answered the following questions:
  - How frequently were the various PPSEs utilized in the vishing attacks?
  - Were certain PPSEs utilized in the vishing attacks more often than others?
  - Which PPSEs were utilized in the majority of the vishing attacks?
  - How frequently did certain PPSEs co-occur in the vishing attacks?
  - Were certain sets of PPSEs utilized more often than others?
  - How were those sets of PPSEs implemented (i.e. what specific elements of the attack contributed to the presence of each PPSE)?

How Frequently Were PPSEs Utilized in the Vishing Attacks?



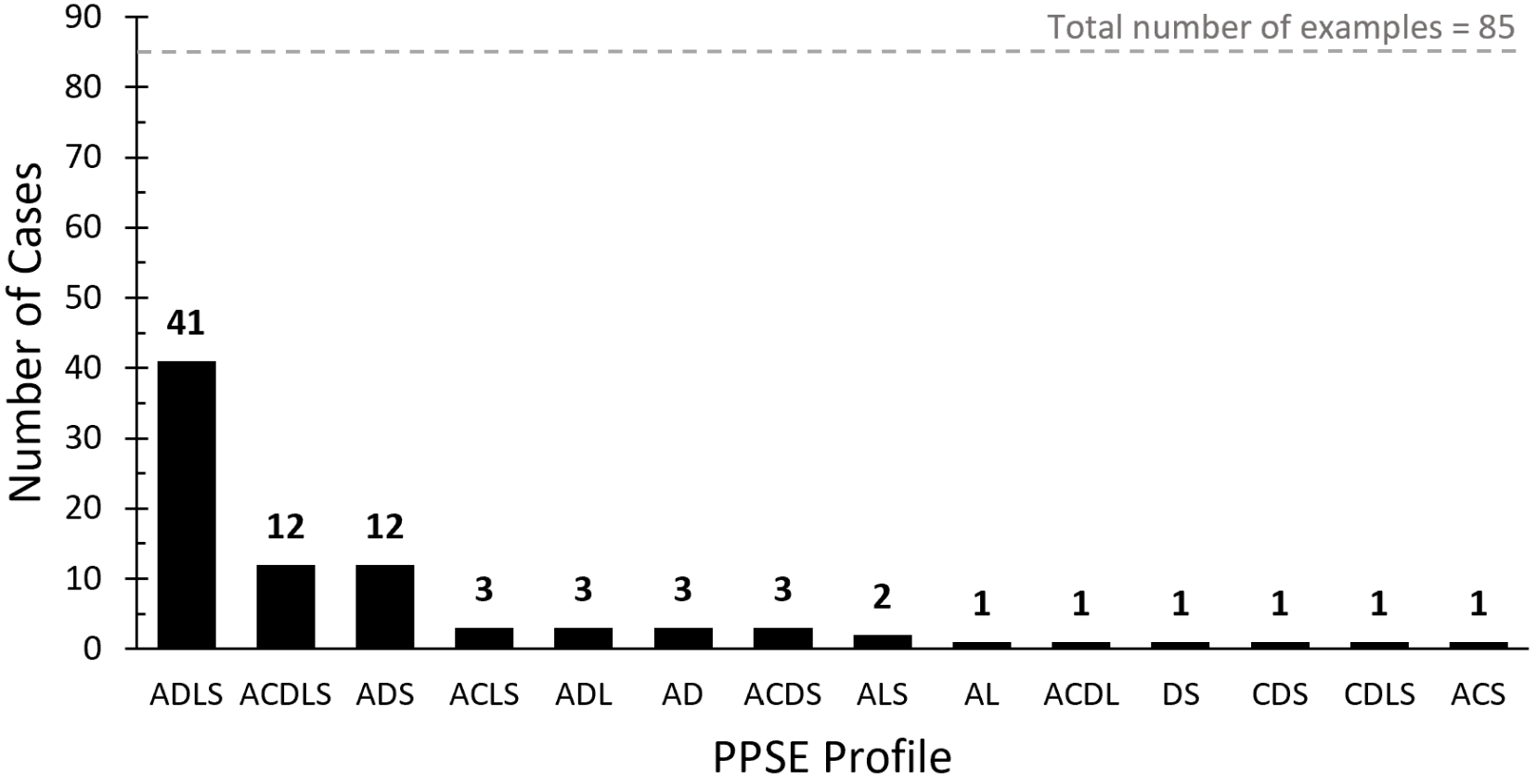
Were Certain PPSEs Utilized More Often Than Others?

- Authority, Social Proof, and Distraction were employed equally often
- They were employed more often than Liking, Similarity, and Deception
- Liking, Similarity, and Deception was employed more often than Commitment, Reciprocation, and Consistency

Which PPSEs Were Utilized in the Majority of the Vishing Attacks?

- Authority, Distraction, and Social Proof were utilized in the vast majority of vishing attacks
- Liking, Similarity, and Deception was utilized in the majority of attacks
- Commitment, Reciprocation, and Consistency was not utilized in the majority of attacks

How Frequently Did Certain PPSEs Co-Occur in the Vishing Attacks?



Were Certain Sets of PPSEs Utilized More Often Than Others?

- Vishers utilized three PPSE sets – ADLS, ACDLS, and ADS – more frequently than other sets of persuasion techniques

How Were Those Sets of PPSEs Implemented?

- ADLS
  - Vishers implied they had authority to access the requested information (A)
  - Vishers claimed to be from a reputable institution (A)
  - Visher expressed to the victim that there are potential benefits involved if they comply (D and S)
  - Vishers mentioning negative consequences if they do not comply (D)
  - Interestingly, no elements related to Liking, Similarity, and Deception occurred in a majority of ADLS-type attacks, which suggests how exactly Liking, Similarity, and Deception was implemented in ADLS-type attacks varied from attack to attack

How Were Those Sets of PPSEs Implemented?

- ACDLS
  - Vishers claimed to be from a reputable institution (A)
  - Vishers claimed to have the authority to access the requested information (A)
  - Vishers emphasized that the victim is committed to helping them (C)
  - Vishers gave the impression that the requested information is time-sensitive (D)
  - Vishers distracted the victim from thinking about potential consequences (D)
  - Vishers stressed the benefits (S) and social correctness (S) of compliance
  - Vishers provided some kind of "proof" of their credibility (L)

How Were Those Sets of PPSEs Implemented?

- ADS
  - Vishers claimed to be a member of a reputable institution (A)
  - Vishers heightening the victim's emotional state (D)
  - Vishers expressed the potential benefits of compliance (D & S)

Summary

- Authority (A), Social Proof (S), and Distraction (D) were the most widely utilized PPSEs, followed by Liking, Similarity, and Deception (L)
- All four of those PPSEs occurred in a majority of vishing attacks, while Commitment, Reciprocation, and Consistency (C) did not.
- Certain sets of PPSEs were utilized more than others, with each set implementing persuasion elements in different ways
  - ADLS: Vishers claim to be from known institutions and aim to convince the victim that there are personal benefits if the victim complies
  - ACDLS: Vishers incorporated more persuasion elements overall, especially distraction, and tried to convince the victim that they are committed to helping the visher. Vishers also gave some kind of "proof" that they are legitimate
  - ADS: Vishers used threats of negative consequences, in addition to describing benefits, and used emotional states to distract their victim
- Two elements were used in a majority of attacks: claiming to be a member of a reputable institution (A) and stressing the benefits of compliance (S)

What Was Not Observed

- Two notable elements were not present in many vishing examples
  - Does the scammer claim to have authority over the victim?
  - Does the scammer state or imply that they are in a hurry or otherwise have limited time to converse with the victim?
- One might expect these to be commonplace
- Instead, vishers established authority by claiming to be from a reputable institution and suggesting they have authority to access the requested information
  - This may be because the hierarchy within the victim's own company is quicker and easier for the victim to verify compared to an outside institution
- Also, vishers applied time pressure by claimed the requested information itself was time sensitive
  - That tactic is potentially less disconcerting to a victim, allowing the attacker to apply time pressure in a less overt way

Practical Implications

- Training Users
  - For example, vishers stressed the benefits of complying with their request in a majority of vishing calls. That could be used to help develop a training program that encourages employees to be suspicious of a caller who offers benefits in exchange for sensitive information
- Training Penetration Testers
  - For example, vishers applied time pressure by claiming the requested information is time sensitive, but not by claiming to be in a hurry. A penetration tester could use this information to realistically role play a visher
- Developing Automated Vishing Detectors
  - For example, in ADS-type attacks, vishers claimed to be from a reputable institution, try to heighten the victim's emotional state, and express benefits of compliance. If a caller mentions they are from a bank, claims the recipient's account is compromised and they will lose a large amount of money, and offers to protect the recipient's assets if they comply, an automated system could detect this combination of elements and alert the call recipient of the potential scam

References

- Cialdini, R. B. (2007), Influence: The Psychology of Persuasion, HarperCollins Publishers, New York, NY.
- Ferreira, A. and Teles, S. (2019), "Persuasion: How phishing emails can influence users and bypass security measures", International Journal of Human-Computer Studies, Vol. 125, pp. 19-31. doi:10.1016/j.ijhcs.2018.12.004
- Ferreira, A. and Chilro, R. (2017), "What to phish in a subject?", in International Conference on Financial Cryptography and Data Security, FC 2017 Workshops, pp. 597-609. doi:10.1007/978-3-319-70278-0_38
- Ferreira, A. and Jakobsson, M. (2016), "Persuasion in scams", Jakobsson, M. (Ed.), Understanding Social Engineering Based Scams, Springer Science & Business Media, New York, NY, pp. 29-47. doi:10.1007/978-1-4939-6457-4_4
- Ferreira, A. and Lenzini, G. (2015), "An analysis of social engineering principles in effective phishing", in 2015 Workshop on Socio-Technical Aspects in Security and Trust, pp. 9-16. doi:10.1109/STAST.2015.10

References

- Ferreira, A., Coventry, L., and Lenzini, G. (2015), "Principles of persuasion in social engineering and their use in phishing", in Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust, HAS 2015, pp. 36-47. doi:10.1007/978-3-319-20376-8_4
- Gragg, D. (2003), A multi-level defense against social engineering, available at www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920.
- Gupta, S., Gupta, P., Ahamad, M., and Kumaraguru, P. (2015), "Abusing phone numbers and cross-application features for crafting targeted attacks", arXiv:1512.07330.
- Jones, K.S., Armstrong, M.E., Tornblad, M.K., & Namin, A. (2021). How social engineers use persuasion principles during vishing attacks. Information and Computer Security, 29(2), 314-331.

References

- Maggi, F. (2010), “Are the con artists back? A preliminary analysis of modern phone frauds”, in Proceedings of the 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010), pp. 824-831. doi: 10.1109/CIT.2010.156
- Mouton, F., Malan, M. M., Leenen, L., and Venter, H. S. (2014), “Social engineering attack framework”, in 2014 Information Security for South Africa, IEEE 2014, pp. 1-9. doi:10.1109/ISSA.2014.6950510
- Stajano, F. and Wilson, P. (2011), “Understanding scam victims: Seven principles for systems security”, Communications of the ACM, Vol. 54 No. 3, pp. 70-75. doi:10.1145/1897852.1897872