# Social Engineering: A Survey

Theodore Longtchi

***Abstract*—Social Engineering has been existing before the surge of the term in the advert of computer and Information Security. The rampant use of the term is also due to the increase use of the technique to lure information from victims. Several research works have been carried out in this domain to identify the techniques, the medium and in some cases the counter measures. Despite of the availability of these resources, the use of Social Engineering to circumvent security continues to rise. This paper review investigate the reason for the increase of social engineering attacks despite the increase in the strength and capacity of technological advancement to counter these attacks. This review also classifies existing literature on social engineering according to their relative technical approaches with respect to the human vulnerability characteristics.**

## I. Introduction

As security for information systems are building up in strength, breaking through is therefore becoming more and more difficult for the bad actors, and they turn to the weakest link in the security of a system – Human. This is how the connotation of social engineering has been borrowed from the discipline of social science to information science. Unlike Social Engineering in social science, which is the use of centralized planning in an attempt to manage social change and regulate the future development and behavior of a society, social engineering in Information Science is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes, according to the Oxford Dictionary. Although both domains involves a sort of people management, in Social Science it does not involve the divulging of confidential information as in Information Science.

It goes without saying that the weakest point in security is human. The means the strongest security is as strong as the weakest human in the line of that security in question. Is the human weakness a biological characteristic attributed to humans by default or it happens because humans cannot compete with machines? Although there is lots of automation in computer systems nowadays, the need for humans to operate and manage some of the machine processes is undeniable. In order to answer these questions, we looked into the research works of other authors base on social engineering, which is considered as the most common means of breaking the human link in the security chain of a system. Survey looks into the reasons why social engineering is so successful in divulging secret information.

## II. Related Literature

## III. Social Engineering Techniques

## IV. Comparison of Techniques

There are three main media through which Social Engineering is carried out: Internet; Short Message Services (SMS); and Voice. Each medium has specialized vectors, which are used to applied the technical approach that the phisher deems necessary for the attack. Fig 3. summarizes the link among these media, the vectors and the technical approaches. Phishing may use one or more vectors, as well as multiple technical approaches to reach the target victim.

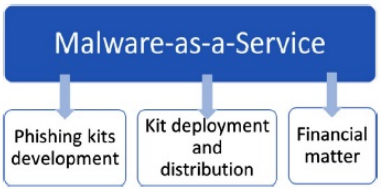


Fig. 1. Note3: Highlighting a claim that technique improve state-of-the-art. [**?** ]

Both Chiew et al (2018) and Aleroud et al (2017) classified the Phishing Process in three main phases. But while Aleroud et al classified the three phases as Attack Preparation, Attack Execution, and Attack Result Exploitation as seen on figure 2, Aleroud et al classified the three phases as Planing, collection, and Fraud as seen on figure 3. A closer look at each phase of both classifications shows that there are sub-phases or at least different stages that do not align the same with the other publication.

## V. Technical Approaches Redundancy

## VI. Result

There is an increase in Social Engineering as there is an expansion of the available media through which this act can be executed, including application vulnerabilities that are exploited. Although this increase may also signify the increase in the technological knowledge of the bad actors, it is also true that the increase is due to the readily availability of Social Engineering tools for novices who want to carry out such attacks. A development in the domain is the availability of XYZ-as-a-service, where XYZ can be Ransomware (McAfee Labs Threats Report, 2018), or Malware. Cybercriminals have shifted from just selling phishing kits in the cybercriminal marketplace to service-based business model on top of the phishing kit itself as a product. With a score of identified Social Engineering attacks, the users of these information and computer systems are overwhelmed with where to place guard.

## VII. Conclusion and Future Work

Without trust, there will be a reasonable decline in the success rate of Social Engineering. Trust makes a person susceptible to the deception of a bad actor. Most methods of Social Engineering exploit the trust of the victim who usually believes he/she is doing the right thing. It should be noted

that the victim may not display 100% trust in order to be deceived. The degree of trust varies from person to person. But the smallest degree of trust can be amplified with other characteristics such as:

**Greed**. A Nigerian Prince that has millions in a Bank, but needs your help to transfer the money out of Nigeria, and you will have a percentage of the millions, is so luring to most people such that they stop thinking except to think of how they will become rich overnight. We see greed here, but the center of this fallibility is trust. If the there was zero trust, the victim would not have succumbed to the enticing email of the fake Nigerian Prince.

**Fear**. People want to keep their job so much so that when they receive an email from the superior, they act impulsively without a second thought. This can also be due to:

**Respect**. In most circumstances, people do not question their superior and respect for them turns to loyalty, upon which they act when they receive any call of action from them.

**Ignorance**. Most people may be aware of Social Engineering, but there are not aware of its technical approaches due to:

**Lack of Employee awareness**, which can be due to:

**Lack of training**; **Impatience**; **Emotion**; **Laziness**; etc.

**Application vulnerability** is the second major problem in computer security systems. Here, the victims usually have little or no role to play in protecting themselves, when bad actors exploit these software/application and system vulnerabilities.

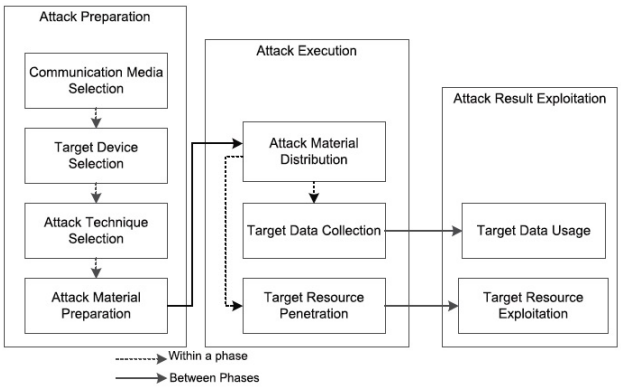


Fig. 2. The phishing process phases. [5]

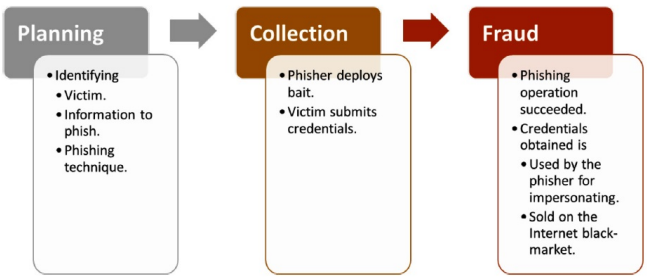


Fig. 3. The phishing process phases. [15]

[0]

## References


[1] Noelle Abe and Michael Soltys. Deploying health campaign strategies to defend against social engineering threats. *Procedia Computer Science*, 159:824–831, 2019.

[2] Samar Muslah Albladi and George RS Weir. User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, 8(1):5, 2018.

[3] Hussain Aldawood and Geoffrey Skinner. A taxonomy for social engineering attacks via personal devices. *International Journal of Computer Applications*, 975:8887.

[4] Hussain Aldawood and Geoffrey Skinner. Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues. *Future Internet*, 11(3):73, 2019.

[5] Ahmed Aleroud and Lina Zhou. Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, 68:160–196, 2017.

[6] Abdullah Algarni, Yue Xu, and Taizan Chan. An empirical study on the susceptibility to social engineering in social networking sites: the case of facebook. *European Journal of Information Systems*, 26(6):661–687, 2017.

[7] Manal Alohali, Nathan Clarke, Fudong Li, and Steven Furnell. Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information & Computer Security*, 26(3):306–326, 2018.

[8] Brendan Anthony. *Social Engineering: The Human Element of Cybersecurity*. PhD thesis, Utica College, 2019.

[9] Alison JC Bell, M Brooke Rogers, and Julia M Pearce. The insider threat: Behavioral indicators and factors influencing likelihood of intervention. *International Journal of Critical Infrastructure Protection*, 24:166–176, 2019.

[10] Aniket Bhadane and Sunil B Mane. Detecting lateral spear phishing attacks in organisations. *IET Information Security*, 13(2):133–140, 2018.

[11] Parnika Bhat and Kamlesh Dutta. A survey on various threats and current state of security in android platform. *ACM Computing Surveys (CSUR)*, 52(1):21, 2019.

[12] Josip Bozic and Franz Wotawa. Planning-based security testing of web applications. In *Proceedings of the 13th International Workshop on Automation of Software Test*, pages 20–26. ACM, 2018.

[13] Birgit Bräuchler. Social engineering the local for peace. *Social Anthropology*, 25(4):437–453, 2017.

[14] Curtis C Campbell. Solutions for counteracting human deception in social engineering attacks. *Information Technology & People*, 2018.

[15] Kang Leng Chiew, Kelvin Sheng Chek Yong, and Choon Lin Tan. A survey of phishing attacks: their types, vectors and technical approaches. *Expert Systems with Applications*, 106:1–20, 2018.

[16] Nabie Y Conteh and Paul J Schmick. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23):31, 2016.

[17] Matthew Edwards, Robert Larson, Benjamin Green, Awais Rashid, and Alistair Baron. Panning for gold: automatically analysing online social engineering attack surfaces. *Computers & Security*, 69:18–34, 2017.

[18] El-Sayed M El-Alfy. Detection of phishing websites based on probabilistic neural networks and k-medoids clustering. *The Computer Journal*, 60(12):1745–1759, 2017.

[19] Amir Mohammad Fathollahi-Fard, Mostafa Hajiaghaei-Keshteli, and Reza Tavakkoli-Moghaddam. The social engineering optimizer (seo). *Engineering Applications of Artificial Intelligence*, 72:267–293, 2018.

[20] Shivi Garg, RK Singh, and AK Mohapatra. Analysis of software vulnerability classification based on different technical parameters. *Information Security Journal: A Global Perspective*, pages 1–19, 2019.

[21] Ibrahim Ghafir, Jibran Saleem, Mohammad Hammoudeh, Hanan Faour, Vaclav Prenosil, Sardar Jaf, Sohail Jabbar, and Thar Baker. Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing*, 74(10):4986–5002, 2018.

[22] Diksha Goel and Ankit Kumar Jain. Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & Security*, 73:519–544, 2018.

[23] Frank Greitzer, Justin Purl, DE Becker, Paul Sticha, and Yung Mei Leong. Modeling expert judgments of insider threat using ontology structure: Effects of individual indicator threat value and class membership. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[24] Prashant Gupta and Manisha J. Nene. Cyberpsycho attacks: Techniques, causes, effects and recommendations to end-users. *International Journal of Computer Applications*, 156(11):11–16, Dec 2016.

[25] Surbhi Gupta, Abhishek Singhal, and Akanksha Kapoor. A literature survey on social engineering attacks: Phishing attack. In *2016 international conference on computing, communication and automation (ICCCA)*, pages 537–540. IEEE, 2016.

[26] Joseph M Hatfield. Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, 73:102–113, 2018.

[27] Joseph M Hatfield. Virtuous human hacking: The ethics of social engineering in penetration-testing. *Computers & Security*, 83:354–366, 2019.

[28] Ryan Heartfield and George Loukas. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys (CSUR)*, 48(3):37, 2016.

[29] Ryan Heartfield and George Loukas. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security*, 76:101–127, 2018.

[30] D Henshel, MG Cains, B Hoffman, and T Kelley. Trust as a human factor in holistic cyber security risk assessment. *Procedia Manufacturing*, 3:1117–1124, 2015.

[31] HS Hota, AK Shrivas, and Rahul Hota. An ensemble model for detecting phishing attack with proposed remove-replace feature selection technique. *Procedia computer science*, 132:900–907, 2018.

[32] Linan Huang and Quanyan Zhu. Adaptive strategic cyber defense for advanced persistent threats in critical infrastructure networks. *ACM SIGMETRICS Performance Evaluation Review*, 46(2):52–56, 2019.

[33] Ankit Kumar Jain and BB Gupta. Rule-based framework for detection of smishing messages in mobile environment. *Procedia Computer Science*, 125:617–623, 2018.

[34] Ankit Kumar Jain and Brij B Gupta. A novel approach to protect against phishing attacks at client side using auto-updated white-list. *EURASIP Journal on Information Security*, 2016(1):9, 2016.

[35] Keith S Jones, Akbar Siami Namin, and Miriam E Armstrong. The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Transactions on Computing Education (TOCE)*, 18(3):11, 2018.

[36] Marianne Junger, Lorena Montoya, and F-J Overink. Priming and warnings are not effective to prevent social engineering attacks. *Computers in human behavior*, 66:75–87, 2017.

[37] SADTP Kaushalya, RMRSB Randeniya, and ADS Liyanage. An overview of social engineering in the context of information security. In *2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, pages 1–6. IEEE, 2018.

[38] Wayne D Kearney and Hennie A Kruger. Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, 61:46–58, 2016.

[39] Amin Kharraz, William Robertson, and Engin Kirda. Surveylance: automatically detecting online survey scams. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 70–86. IEEE, 2018.

[40] Duncan Ki-Aries and Shamal Faily. Persona-centred information security awareness. *computers & security*, 70:663–674, 2017.

[41] Hyeob Kim, HyukJun Kwon, and Kyung Kyu Kim. Modified cyber kill chain model for multimedia service environments. *Multimedia Tools and Applications*, 78(3):3153–3170, 2019.

[42] Jian Mao, Jingdong Bian, Wenqian Tian, Shishi Zhu, Tao Wei, Aili Li, and Zhenkai Liang. Detecting phishing websites via aggregation analysis of page layouts. *Procedia Computer Science*, 129:224–230, 2018.

[43] Thomas Richard McEvoy and Stewart James Kowalski. Deriving cyber security risks from human and organizational factors–a socio-technical approach. *Complex Systems Informatics and Modeling Quarterly*, (18):47–64, 2019.

[44] Weina Niu, Xiaosong Zhang, Guowu Yang, Ruidong Chen, and Dong Wang. Modeling attack process of advanced persistent threat using network evolution. *IEICE TRANSACTIONS on Information and Systems*,

100(10):2275–2286, 2017.

[45] Marcus Pendleton, Richard Garcia-Lebron, Jin-Hee Cho, and Shouhuai Xu. A survey on systems security metrics. *ACM Computing Surveys (CSUR)*, 49(4):62, 2017.

[46] Nader Sohrabi Safa, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani, and Tutut Herawan. Information security conscious care behaviour formation in organizations. *Computers & Security*, 53:65–78, 2015.

[47] Fatima Salahdine and Naima Kaabouch. Social engineering attacks: A survey. *Future Internet*, 11(4):89, 2019.

[48] Peter Schaab, Kristian Beckers, and Sebastian Pape. Social engineering defence mechanisms and counteracting training strategies. *Information & Computer Security*, 25(2):206–222, 2017.

[49] Jordan Shropshire, Merrill Warkentin, and Shwadhin Sharma. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49:177–191, 2015.

[50] Hossein Siadati, Toan Nguyen, Payas Gupta, Markus Jakobsson, and Nasir Memon. Mind your smses: Mitigating social engineering in second factor authentication. *Computers & Security*, 65:14–28, 2017.

[51] Arun Vishwanath. Getting phished on social media. *Decision Support Systems*, 103:70–81, 2017.

[52] Emma J Williams, Amy Beardmore, and Adam N Joinson. Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72:412–421, 2017.

[53] Liu Xiangyu, Li Qiuyang, and Sonali Chandel. Social engineering and insider threats. In *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pages 25–34. IEEE, 2017.

[54] Yixue Zhao, Marcelo Schmitt Laser, Yingjun Lyu, and Nenad Medvidovic. Leveraging program analysis to reduce user-perceived latency in mobile applications. In *Proceedings of the 40th International Conference on Software Engineering*, pages 176–186. ACM, 2018.

[55] Kangfeng Zheng, Tong Wu, Xiujuan Wang, Bin Wu, and Chunhua Wu. A session and dialogue based social engineering framework. *IEEE Access*, 2019.

[56] Zakiah Zulkefli, Manmeet Mahinderjit Singh, Azizul Rahman Mohd Shariff, and Azman Samsudin. Typosquat cyber crime attack detection via smartphone. *Procedia Computer Science*, 124:664–671, 2017.