Innovation. Lecture Notes in Information Systems and Organisation. vol. 27. Springer, Cham; 2019. p. 179–188. Available from: http://link.springer.com/10.1007/978-3-319-90500-6{_}14.

[17] CJ G, Pandit S, Vaddepalli S, Tupsamudre H, Banahatti V, Lodha S. PHISHY - A Serious Game to Train Enterprise Users on Phishing Awareness. In: 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts, CHI PLAY '18 Extended Abstracts. ACM; 2018. p. 169–181.

[18] Landers RN, Auer EM, Collmus AB, Armstrong MB. Gamification Science, Its History and Future: Definitions and a Research Agenda. Simulation & Gaming. 2018 jun;49(3):315–337.

[19] Misra G, Arachchilage NAG, Berkovsky S. Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks. In: Steven Furnell NLC, editor. Eleventh International Symposium on Human Aspects of Information Security & Assurance, HAISA 2017; 2017. p. 41–51.

[20] Amran A, Zaaba ZF, Singh MM, Marashdih AW. Usable Security: Revealing End-Users Comprehensions on Security Warnings. Procedia Computer Science. 2017 jan;124:624–631.

[21] Jamil A, Asif K, Ghulam Z, Nazir MK, Mudassar Alam S, Ashraf R. MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook. In: 2018 IEEE International Conference on Big Data (Big Data). vol. 1. IEEE; 2018. p. 5040–5048.

[22] Tsalis N, Mylonas A, Nisioti A, Gritzalis D, Katos V. Exploring the Protection of Private Browsing in Desktop Browsers. Computers & Security. 2017 jun;67:181–197.

[23] Virvilis N, Mylonas A, Tsalis N, Gritzalis D. Security Busters: Web Browser Security vs. Rogue Sites. Computers & Security. 2015 jul;52:90–105.

[24] Santos L, Rabadao C, Goncalves R. Intrusion Detection Systems in Internet of Things: A Literature Review. In: 2018 13th Iberian Conference on Information Systems and Technologies (CISTI). IEEE; 2018. p. 1–7.

[25] Singh R, Kumar H, Singla RK, Ketti RR. Internet Attacks and Intrusion Detection System: A Review of the Literature. Online Information Review. 2017 apr;41(2):171–184.

[26] El-Alfy ESM. Detection of Phishing Websites Based on Probabilistic Neural Networks and K-Medoids Clustering. The Computer Journal. 2017 dec;60(12):1745–1759.

[27] Jain AK, Gupta BB. Towards Detection of Phishing Websites on Client-Side using Machine Learning based Approach. Telecommunication Systems. 2018 aug;68(4):687–700.

[28] Mahdavifar S, Ghorbani AA. Application of Deep Learning to Cybersecurity: A Survey. Neurocomputing. 2019 jun;347:149–176.

[29] McCluskey L, Thabtah F, Mohammad RM. Intelligent Rule-based Phishing Websites Classification. IET Information Security. 2014 may;8(3):153–160.

[30] Sahoo D, Liu C, Hoi SCH. Malicious URL Detection using Machine Learning: A Survey. 2017 jan;Available from: http://arxiv.org/abs/1701.07179.

[31] Shibahara T, Yamanishi K, Takata Y, Chiba D, Akiyama M, Yagi T, et al. Malicious URL Sequence Detection using Event De-noising Convolutional Neural Network. In: 2017 IEEE International Conference on Communications (ICC). IEEE; 2017. p. 1–7.

[32] Jain AK, Gupta BB. A Novel Approach to Protect Against Phishing Attacks at Client Side using Auto-updated White-List. EURASIP J Inf Secur. 2016 dec;2016(1):9. Available from: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-016-0034-3.

[33] Sonowal G, Kuppusamy KS. PhiDMA – A Phishing Detection Model with Multi-Filter Approach. Journal of King Saud University - Computer and Information Sciences. 2017;p. 1–14.

[34] Jain AK, Gupta BB. Phishing Detection: Analysis of Visual Similarity Based Approaches. Security and Communication Networks. 2017 jan;2017:1–20.

[35] Shiva S, Dasgupta D, Wu Q. Game Theoretic Approaches to Protect Cyberspace. University of Memphis, Department of Computer Science; 2010. Available from: https://apps.dtic.mil/dtic/tr/fulltext/u2/a519126.pdf.

[36] Tchakounté F, Nyassi VS, Udagepola KP. True Request–Fake Response: A New Trend of Spear Phishing Attack. Journal of Network Security. 2019;7(3):1–17.

[37] Yu M, Liu C, Qiu X, Zhao S. Modelling and Analysis of Phishing Attack using Stochastic Game Nets. In: International Conference on Cyberspace Technology (CCT 2013). Institution of Engineering and Technology; 2013. p. 300–305.

[38] Figueroa N, L'Huillier G, Weber R. Adversarial Classification using Signaling Games with an Application to Phishing Detection. Data Mining and Knowledge Discovery. 2017 jan;31(1):92–133.

[39] Pawlick J, Zhu Q. Phishing for Phools in the Internet of Things: Modeling One-to-Many Deception using Poisson Signaling Games. 2017 mar;Available from: http://arxiv.org/abs/1703.05234.

[40] Zhao M, An B, Kiekintveld C. Optimizing Personalized Email Filtering Thresholds to Mitigate Sequential Spear Phishing Attacks. In: Thirtieth AAAI Conference on Artificial Intelligence. AAAI Press; 2016. p. 658–664.

[41] McCubbins MD, Turner MB, Weller N. Testing the Foundations of Quantal Response Equilibrium. In: International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction. SSRN; 2013. p. 10p.

[42] Binmore K. Playing for Real : a Text on Game Theory. Oxford University Press; 2007.

[43] Osborne MJ, Rubinstein A, Osborne M, Rubinstein A. A Course in Game Theory. vol. 1. MIT Press; 1994.

[44] Roy S, Ellis C, Shiva S, Dasgupta D, Shandilya V, Wu Q. A Survey of Game Theory as Applied to Network Security. In: the 2010 43rd Hawaii International Conference on System Sciences. IEEE; 2010. p. 1–10.

[45] Richard D M, Andrew M, Theodore T. Gambit: Software Tools for Game Theory, Version 16.0.1. Gambit Project; 2019. Available from: https://buildmedia.readthedocs.org/media/pdf/gambitproject/latest/gambitproject.pdf.

[46] Shen S, Hu K, Huang L, Li H, Han R, Cao Q. Quantal Response Equilibrium-Based Strategies for Intrusion

Detection in WSNs. Mobile Information Systems. 2015 aug;2015:1–10.
[47] Mckelvey RD, Palfrey TR. Quantal Response Equilibria for Extensive Form Games. Experimental Economics. 1998;1(1):9–41.
[48] Kantzavelou I, Katsikas S. A Game-based Intrusion Detection Mechanism to Confront Internal Attackers. Computers & Security. 2010 nov;29(8):859–874.
[49] Chin T, Xiong K, Hu C. Phishlimiter: A Phishing Detection and Mitigation Approach Using Software-Defined Networking. IEEE Access. 2018;6:42516–42531.
[50] Qamar A, Karim A, Chang V. Mobile Malware Attacks: Review, Taxonomy & Future Directions. Futur Gener Comput Syst. 2019;97:887–909.
[51] Volkamer M, Renaud K, Reinheimer B, Kunz A. User experiences of TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. Computers & Security. 2017 nov;71:100–113.
[52] OpenPhish. Timely. Accurate. Relevant Threat Intelligence.;. Available from: https://www.openphish.com/.
[53] Gupta S, Sachdeva S. Invitation or Bait? Detecting Malicious URLs in Facebook Events. In: 2018 Eleventh International Conference on Contemporary Computing (IC3). IEEE; 2018. p. 1–6.
[54] Shirazi H, Bezawada B, Ray I. "Kn0w Thy Doma1n Name": Unbiased Phishing Detection Using Domain Name Based Features. In: The 23nd ACM on Symposium on Access Control Models and Technologies, SACMAT '18. ACM; 2018. p. 69–75.
[55] Zhu Q, Rass S. On Multi-Phase and Multi-Stage Game-Theoretic Modeling of Advanced Persistent Threats. IEEE Access. 2018 Mar;6:13958–13971.
[56] Yu M, Liu C, Qiu X, Zhao S. Modelling and Analysis of Phishing Attack using Stochastic Game Nets. In: International Conference on Cyberspace Technology (CCT 2013). Institution of Engineering and Technology; 2013. p. 300–305.