REFERENCES

Aassal, A. E., Baki, S., Das, A., & Verma, R. M. (2020). An in-depth benchmarking and evaluation of phishing detection research for security needs. *IEEE Access*, *8*, 22170–22192. Retrieved from `https://doi.org/10.1109/access.2020.2969780` doi: 10.1109/access.2020.2969780

Aburrous, M., Hossain, M., Dahal, K., & Thabtah, F. (2010, December). Intelligent phishing detection system for e-banking using fuzzy data mining. *Expert Systems with Applications*, *37*(12), 7913–7921. Retrieved from `https://doi.org/10.1016/j.eswa.2010.04.044` doi: 10.1016/j.eswa.2010.04.044

Afroz, S., & Greenstadt, R. (2011, September). PhishZoo: Detecting phishing websites by looking at them. In *2011 IEEE fifth international conference on semantic computing.* IEEE. Retrieved from `https://doi.org/10.1109/icsc.2011.52` doi: 10.1109/icsc.2011.52

Alabdan, R. (2020, September). Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet*, *12*(10), 168. Retrieved from `https://doi.org/10.3390/fi12100168` doi: 10.3390/fi12100168

AlEroud, A., & Karabatis, G. (2020, March). Bypassing detection of URL-based phishing attacks using generative adversarial deep neural networks. ACM. Retrieved from `https://doi.org/10.1145/3375708.3380315` doi: 10.1145/3375708.3380315

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021, March). Phishing attacks: A recent comprehensive study and a new anatomy. , *3*. Retrieved from `https://doi.org/10.3389/fcomp.2021.563060` doi: 10.3389/fcomp.2021.563060

APWG. (2021a). Phishing activity trends report: 2nd quarter 2021. *Anti-Phishing Working Group. Retrieved September, 22*, 12.

APWG. (2021b). Phishing activity trends report: 4th quarter 2020. *Anti-Phishing*

Working Group. Retrieved February, 09, 13.

Ariyadasa, S., Fernando, S., & Fernando, S. (2020, July). Detecting phishing attacks using a combined model of LSTM and CNN. *International Journal of ADVANCED AND APPLIED SCIENCES*, *7*(7), 56–67. Retrieved from `https://doi.org/10.21833/ijaas.2020.07.007` doi: 10.21833/ijaas.2020.07.007

Bahnsen, A. C., Bohorquez, E. C., Villegas, S., Vargas, J., & Gonzalez, F. A. (2017, April). Classifying phishing URLs using recurrent neural networks. In *2017 APWG symposium on electronic crime research (eCrime).* IEEE. Retrieved from `https://doi.org/10.1109/ecrime.2017.7945048` doi: 10.1109/ecrime.2017.7945048

Bahnsen, A. C., Torroledo, I., Camacho, L. D., & Villegas, S. (2018). Deepphish : Simulating malicious ai..

Baslyman, M., & Chiasson, S. (2016, June). "smells phishy?": An educational game about online phishing scams. In *2016 APWG symposium on electronic crime research (eCrime).* IEEE. Retrieved from `https://doi.org/10.1109/ecrime.2016.7487946` doi: 10.1109/ecrime.2016.7487946

Beck, K., & Zhan, J. (2010, August). Phishing using a modified bayesian technique. In *2010 IEEE second international conference on social computing.* IEEE. Retrieved from `https://doi.org/10.1109/socialcom.2010.100` doi: 10.1109/socialcom.2010.100

Bell, S., & Komisarczuk, P. (2020, January). An analysis of phishing blacklists: Google safe browsing, OpenPhish, and PhishTank. In *Proceedings of the australasian computer science week multiconference.* ACM. Retrieved from `https://doi.org/10.1145/3373017.3373020` doi: 10.1145/3373017.3373020

Bianchi, F. M., Grattarola, D., Livi, L., & Alippi, C. (2021). Graph neural networks with convolutional ARMA filters. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1–1. Retrieved from `https://doi.org/10.1109/tpami.2021.3054830` doi: 10.1109/tpami.2021.3054830

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176. Retrieved from https://doi.org/10.1109/comst.2015.2494502 doi: 10.1109/comst.2015.2494502

Butnaru, A., Mylonas, A., & Pitropakis, N. (2021, June). Towards lightweight URL-based phishing detection. *Future Internet*, *13*(6), 154. Retrieved from https://doi.org/10.3390/fi13060154 doi: 10.3390/fi13060154

Canova, G., Volkamer, M., Bergmann, C., & Borza, R. (2014). NoPhish: An anti-phishing education app. In *Security and trust management* (pp. 188–192). Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-319-11851-2_14 doi: 10.1007/978-3-319-11851-2_14

Cao, Y., Han, W., & Le, Y. (2008). Anti-phishing based on automated individual white-list. In *Proceedings of the 4th ACM workshop on digital identity management - dim' 08.* ACM Press. Retrieved from https://doi.org/10.1145/1456424.1456434 doi: 10.1145/1456424.1456434

Chang, J. C., Amershi, S., & Kamar, E. (2017, May). Revolt: Collaborative crowdsourcing for labeling machine learning datasets. In *Proceedings of the 2017 CHI conference on human factors in computing systems.* ACM. Retrieved from https://doi.org/10.1145/3025453.3026044 doi: 10.1145/3025453.3026044

Chatterjee, M., & Namin, A. S. (2019). Deep reinforcement learning for detecting malicious websites. *CoRR*, *abs/1905.09207*. Retrieved from http://arxiv.org/abs/1905.09207

Chauhan, N. K., & Singh, K. (2018, September). A review on conventional machine learning vs deep learning. In *2018 international conference on computing, power and communication technologies (GUCON).* IEEE. Retrieved from https://doi.org/10.1109/gucon.2018.8675097 doi: 10.1109/gucon.2018.8675097

Chen, J.-L., Ma, Y.-W., & Huang, K.-L. (2020, October). Intelligent visual similarity-based phishing websites detection. *Symmetry*, *12*(10), 1681. Retrieved from https://doi.org/10.3390/sym12101681 doi: 10.3390/sym12101681

Chen, W., Zhang, W., & Su, Y. (2018). Phishing detection research based on LSTM recurrent neural network. In *Communications in computer and information science* (pp. 638–645). Springer Singapore. Retrieved from `https://doi.org/10.1007/978-981-13-2203-7\_52` doi: 10.1007/978-981-13-2203-7_52

Chiew, K. L., Chang, E. H., Tan, C. L., Abdullah, J., & Yong, K. S. C. (2018). Building standard offline anti-phishing dataset for benchmarking. *International Journal of Engineering & Technology*, *7*(4.31), 7–14.

Chiew, K. L., Tan, C. L., Wong, K., Yong, K. S., & Tiong, W. K. (2019, May). A new hybrid ensemble feature selection framework for machine learning-based phishing detection system. *Information Sciences*, *484*, 153–166. Retrieved from `https://doi.org/10.1016/j.ins.2019.01.064` doi: 10.1016/j.ins.2019.01.064

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018, September). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, 1–20. Retrieved from `https://doi.org/10.1016/j.eswa.2018.03.050` doi: 10.1016/j.eswa.2018.03.050

Creswell, A., White, T., Dumoulin, V., Arulkumaran, K., Sengupta, B., & Bharath, A. A. (2017). Generative adversarial networks: An overview. *CoRR*, *abs/1710.07035*. Retrieved from `http://arxiv.org/abs/1710.07035`

Denning, T., Lerner, A., Shostack, A., & Kohno, T. (2013). Control-alt-hack. In *Proceedings of the 2013 ACM SIGSAC conference on computer & communications security - CCS '13*. ACM Press. Retrieved from `https://doi.org/10.1145/2508859.2516753` doi: 10.1145/2508859.2516753

Desai, A., Jatakia, J., Naik, R., & Raul, N. (2017, May). Malicious web content detection using machine leaning. In *2017 2nd IEEE international conference on recent trends in electronics, information & communication technology (RTEICT)*. IEEE. Retrieved from `https://doi.org/10.1109/rteict.2017.8256834` doi: 10.1109/rteict.2017.8256834

Dixon, M., Arachchilage, N. A. G., & Nicholson, J. (2019, May). Engaging users with educational games. In *Extended abstracts of the 2019 CHI conference on* *human factors in computing systems.* ACM. Retrieved from `https://doi.org/10.1145/3290607.3313026` doi: 10.1145/3290607.3313026

Donahue, J., Anne Hendricks, L., Guadarrama, S., Rohrbach, M., Venugopalan, S., Saenko, K., & Darrell, T. (2015, June). Long-term recurrent convolutional networks for visual recognition and description. In *Proceedings of the ieee conference on computer vision and pattern recognition (cvpr).*

Dong, X., Clark, J. A., & Jacob, J. (2008, May). Modelling user-phishing interaction. In *2008 conference on human system interactions.* IEEE. Retrieved from `https://doi.org/10.1109/hsi.2008.4581513` doi: 10.1109/hsi.2008.4581513

Dong, Z., Kane, K., & Camp, L. J. (2016). Detection of rogue certificates from trusted certificate authorities using deep neural networks. *ACM Transactions on Privacy and Security (TOPS)*, *19*(2), 1–31.

Dong, Z., Kapadia, A., Blythe, J., & Camp, L. J. (2015). Beyond the lock icon: real-time detection of phishing websites using public key certificates. In *2015 apwg symposium on electronic crime research (ecrime)* (pp. 1–12).

Dou, Z., Khalil, I., Khreishah, A., Al-Fuqaha, A., & Guizani, M. (2017). Systematization of knowledge (SoK): A systematic review of software-based web phishing detection. *IEEE Communications Surveys & Tutorials*, *19*(4), 2797–2819. Retrieved from `https://doi.org/10.1109/comst.2017.2752087` doi: 10.1109/comst.2017.2752087

Drury, V., & Meyer, U. (2019). Certified phishing: taking a look at public key certificates of phishing websites. In *Fifteenth symposium on usable privacy and security (soups 2019)* (pp. 211–223).

Drutsa, A., Farafonova, V., Fedorova, V., Megorskaya, O., Zerminova, E., & Zhilinskaya, O. (2019). Practice of efficient data collection via crowdsourcing at large-scale. *CoRR*, *abs/1912.04444*. Retrieved from `http://arxiv.org/abs/1912.04444`

Dunlop, M., Groat, S., & Shelly, D. (2010). GoldPhish: Using images for content-based phishing analysis. In *2010 fifth international conference on internet mon-*

itoring and protection. IEEE. Retrieved from https://doi.org/10.1109/icimp.2010.24 doi: 10.1109/icimp.2010.24

Eickhoff, C. (2018, February). Cognitive biases in crowdsourcing. In *Proceedings of the eleventh ACM international conference on web search and data mining.* ACM. Retrieved from https://doi.org/10.1145/3159652.3159654 doi: 10.1145/3159652.3159654

El-Alfy, E.-S. M. (2017, April). Detection of phishing websites based on probabilistic neural networks and k-medoids clustering. *The Computer Journal*, *60*(12), 1745–1759. Retrieved from https://doi.org/10.1093/comjnl/bxx035 doi: 10.1093/comjnl/bxx035

ENISA. (2020). *Enisa threat landscape - phishing.* Publications Office. Retrieved from https://data.europa.eu/doi/10.2824/552242 doi: 10.2824/552242

ENISA. (2021). *Enisa threat landscape 2021: April 2020 to mid july 2021.* Publications Office. Retrieved from https://data.europa.eu/doi/10.2824/324797 doi: 10.2824/324797

Feng, J., Zou, L., Ye, O., & Han, J. (2020). Web2vec: Phishing webpage detection method based on multidimensional features driven by deep learning. , *8*, 221214–221224. Retrieved from https://doi.org/10.1109/access.2020.3043188 doi: 10.1109/access.2020.3043188

François-Lavet, V., Henderson, P., Islam, R., Bellemare, M. G., & Pineau, J. (2018). An introduction to deep reinforcement learning. *Foundations and Trends® in Machine Learning*, *11*(3-4), 219–354. Retrieved from https://doi.org/10.1561/2200000071 doi: 10.1561/2200000071

Fu, A. Y., Wenyin, L., & Deng, X. (2006, October). Detecting phishing web pages with visual similarity assessment based on earth mover's distance (EMD). *IEEE Transactions on Dependable and Secure Computing*, *3*(4), 301–311. Retrieved from https://doi.org/10.1109/tdsc.2006.50 doi: 10.1109/tdsc.2006.50

Goodfellow, I., Bengio, Y., & Courville, A. (2017). Deep learning (adaptive computation and machine learning series). *Cambridge Massachusetts*.

Gowtham, R., & Krishnamurthi, I. (2014). A comprehensive and efficacious architecture for detecting phishing webpages. *Computers & Security*, *40*, 23–37.

Gu, X., Wang, H., & Ni, T. (2013). An efficient approach to detecting phishing web. *Journal of Computational Information Systems*, *9*(14), 5553–5560.

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2017, May). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247–267. Retrieved from `https://doi.org/10.1007/s11235-017-0334-z` doi: 10.1007/s11235-017-0334-z

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2016, March). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629–3654. Retrieved from `https://doi.org/10.1007/s00521-016-2275-y` doi: 10.1007/s00521-016-2275-y

Hansen, D. L., Schone, P. J., Corey, D., Reid, M., & Gehring, J. (2013). Quality control mechanisms for crowdsourcing. In *Proceedings of the 2013 conference on computer supported cooperative work - CSCW '13.* ACM Press. Retrieved from `https://doi.org/10.1145/2441776.2441848` doi: 10.1145/2441776.2441848

Huang, C.-Y., Ma, S.-P., Yeh, W.-L., Lin, C.-Y., & Liu, C.-T. (2010, November). Mitigate web phishing using site signatures. In *TENCON 2010 - 2010 IEEE region 10 conference.* IEEE. Retrieved from `https://doi.org/10.1109/tencon.2010.5686582` doi: 10.1109/tencon.2010.5686582

Huang, H., Zhong, S., & Tan, J. (2009). Browser-side countermeasures for deceptive phishing attack. In *2009 fifth international conference on information assurance and security.* IEEE. Retrieved from `https://doi.org/10.1109/ias.2009.12` doi: 10.1109/ias.2009.12

Jain, A. K., & Gupta, B. B. (2016, May). A novel approach to protect against phishing attacks at client side using auto-updated white-list. *EURASIP Journal on Information Security*, *2016*(1). Retrieved from `https://doi.org/10.1186/s13635-016-0034-3` doi: 10.1186/s13635-016-0034-3

Jain, A. K., & Gupta, B. B. (2017). Phishing detection: Analysis of visual similarity based approaches. *Security and Communication Networks*, *2017*, 1–20. Retrieved from https://doi.org/10.1155/2017/5421046 doi: 10.1155/2017/5421046

Jain, A. K., & Gupta, B. B. (2018a, April). A machine learning based approach for phishing detection using hyperlinks information. *Journal of Ambient Intelligence and Humanized Computing*, *10*(5), 2015–2028. Retrieved from https://doi.org/10.1007/s12652-018-0798-z doi: 10.1007/s12652-018-0798-z

Jain, A. K., & Gupta, B. B. (2018b). PHISH-SAFE: URL features-based phishing detection system using machine learning. In *Advances in intelligent systems and computing* (pp. 467–474). Springer Singapore. Retrieved from https://doi.org/10.1007/978-981-10-8536-9_44 doi: 10.1007/978-981-10-8536-9_44

Jeeva, S. C., & Rajsingh, E. B. (2016, July). Intelligent phishing url detection using association rule mining. *Human-centric Computing and Information Sciences*, *6*(1). Retrieved from https://doi.org/10.1186/s13673-016-0064-3 doi: 10.1186/s13673-016-0064-3

Joshi, Y., Saklikar, S., Das, D., & Saha, S. (2008, December). PhishGuard: A browser plug-in for protection from phishing. In *2008 2nd international conference on internet multimedia services architecture and applications.* IEEE. Retrieved from https://doi.org/10.1109/imsaa.2008.4753929 doi: 10.1109/imsaa.2008.4753929

Kamiri, J., & Mariga, G. (2021). Research methods in machine learning: A content analysis. *International Journal of Computer and Information Technology (2279-0764)*, *10*(2).

Kashyap, R. (2020, Jan). *Council post: Are you ready for the age of adversarial ai? attackers can leverage artificial intelligence too.* Forbes Magazine. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2020/01/09/are-you-ready-for-the-age-of-adversarial-ai-attackers-can-leverage-artificial-intelligence-too/?sh=76e9150d4703

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys & Tutorials*, *15*(4), 2091–2121. Retrieved from https://doi.org/10.1109/surv.2013.032213.00009 doi: 10.1109/surv.2013.032213.00009

Kipf, T. N., & Welling, M. (2016). Semi-supervised classification with graph convolutional networks. *CoRR*, *abs/1609.02907*. Retrieved from http://arxiv.org/abs/1609.02907

Knickerbocker, P., Yu, D., & Li, J. (2009). Humboldt: A distributed phishing disruption system. In *2009 ecrime researchers summit* (pp. 1–12).

Le, H., Pham, Q., Sahoo, D., & Hoi, S. C. H. (2018). Urlnet: Learning a URL representation with deep learning for malicious URL detection. *CoRR*, *abs/1802.03162*. Retrieved from http://arxiv.org/abs/1802.03162

Le, Q., & Mikolov, T. (2014, 22–24 Jun). Distributed representations of sentences and documents. In E. P. Xing & T. Jebara (Eds.), *Proceedings of the 31st international conference on machine learning* (Vol. 32, pp. 1188–1196). Bejing, China: PMLR. Retrieved from https://proceedings.mlr.press/v32/le14.html

LeCun, Y., Bengio, Y., & Hinton, G. (2015, May). Deep learning. *Nature*, *521*(7553), 436–444. Retrieved from https://doi.org/10.1038/nature14539 doi: 10.1038/nature14539

Levine, S., Kumar, A., Tucker, G., & Fu, J. (2020). Offline reinforcement learning: Tutorial, review, and perspectives on open problems. *CoRR*, *abs/2005.01643*. Retrieved from https://arxiv.org/abs/2005.01643

Li, Y., Yang, Z., Chen, X., Yuan, H., & Liu, W. (2019, May). A stacking model using URL and HTML features for phishing webpage detection. *Future Generation Computer Systems*, *94*, 27–39. Retrieved from https://doi.org/10.1016/j.future.2018.11.004 doi: 10.1016/j.future.2018.11.004

Lin, Y., Liu, R., Divakaran, D. M., Ng, J. Y., Chan, Q. Z., Lu, Y., ... Dong, J. S. (2021, August). Phishpedia: A hybrid deep learning based approach to visually identify phishing webpages. In *30th usenix security symposium (usenix security 21)* (pp. 3793–3810). USENIX Association. Retrieved from https://www.usenix.org/conference/usenixsecurity21/presentation/lin

Mao, J., Tian, W., Li, P., Wei, T., & Liang, Z. (2017). Phishing-alarm: Robust and efficient phishing detection via page component similarity. *IEEE Access*, *5*, 17020–17030. Retrieved from https://doi.org/10.1109/access.2017.2743528 doi: 10.1109/access.2017.2743528

Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., ... Hassabis, D. (2015, February). Human-level control through deep reinforcement learning. *Nature*, *518*(7540), 529–533. Retrieved from https://doi.org/10.1038/nature14236 doi: 10.1038/nature14236

Mohammad, A. H., & Al Saiyd, N. A. M. (2010). A framework for expert knowledge acquisition. *IJCSNS*, *10*(11), 145.

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2012). An assessment of features related to phishing websites using an automated technique. In *2012 international conference for internet technology and secured transactions* (pp. 492–497).

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2013, November). Predicting phishing websites based on self-structuring neural network. *Neural Computing and Applications*, *25*(2), 443–458. Retrieved from https://doi.org/10.1007/s00521-013-1490-z doi: 10.1007/s00521-013-1490-z

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2014). Intelligent rule-based phishing websites classification. *IET Information Security*, *8*(3), 153–160.

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015, August). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, *17*, 1–24. Retrieved from https://doi.org/10.1016/j.cosrev.2015.04.001 doi: 10.1016/j.cosrev.2015.04.001

Mousavi, S. S., Schukat, M., & Howley, E. (2017, August). Deep reinforcement learning: An overview. In *Proceedings of SAI intelligent systems conference (IntelliSys) 2016* (pp. 426–440). Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-319-56991-8_32 doi: 10.1007/978-3-319-56991-8_32

Netcraft. (2021, Dec). *Web server survey.* Retrieved from https://news.netcraft.com/archives/category/web-server-survey/

Nguyen, D. T., Alam, F., Ofli, F., & Imran, M. (2017). *Automatic image filtering on* *social networks using deep learning and perceptual hashing during crises.*

Nguyen, L. A. T., To, B. L., Nguyen, H. K., & Nguyen, M. H. (2014, October). An efficient approach for phishing detection using single-layer neural network. In *2014 international conference on advanced technologies for communications (ATC 2014).* IEEE. Retrieved from https://doi.org/10.1109/atc.2014.7043427 doi: 10.1109/atc.2014.7043427

Nguyen, L. D., Le, D.-N., & Vinh, L. T. (2014). Detecting phishing web pages based on DOM-tree structure and graph matching algorithm. In *Proceedings of the fifth symposium on information and communication technology - SoICT '14.* ACM Press. Retrieved from https://doi.org/10.1145/2676585.2676596 doi: 10.1145/2676585.2676596

Odeh, A., Keshta, I., & Abdelfattah, E. (2021). Phiboost-a novel phishing detection model using adaptive boosting approach. *Jordanian Journal of Computers and Information Technology (JJCIT)*, *7*(01).

Opara, C., Chen, Y., & Wei, B. (2020). Look before you leap: Detecting phishing web pages by exploiting raw URL and HTML characteristics. *CoRR*, *abs/2011.04412*. Retrieved from https://arxiv.org/abs/2011.04412

Opara, C., Wei, B., & Chen, Y. (2020, July). HTMLPhish: Enabling phishing web page detection by applying deep learning techniques on HTML analysis. In *2020 international joint conference on neural networks (IJCNN).* IEEE. Retrieved from https://doi.org/10.1109/ijcnn48605.2020.9207707 doi: 10.1109/ijcnn48605.2020.9207707

Orunsolu, A., Sodiya, A., & Akinwale, A. (2019, December). A predictive model for phishing detection. *Journal of King Saud University - Computer and Information Sciences*. Retrieved from https://doi.org/10.1016/j.jksuci.2019.12.005 doi: 10.1016/j.jksuci.2019.12.005

Pham, T. T. T., Hoang, V. N., & Ha, T. N. (2018). Exploring efficiency of character-level convolution neuron network and long short term memory on malicious URL detection. In *Proceedings of the 2018 VII international conference on network, communication and computing - ICNCC 2018.* ACM Press. Retrieved from https://doi.org/10.1145/3301326.3301336 doi: 10.1145/3301326.3301336

Prakash, P., Kumar, M., Kompella, R. R., & Gupta, M. (2010, March). PhishNet: Predictive blacklisting to detect phishing attacks. In *2010 proceedings IEEE INFOCOM.* IEEE. Retrieved from https://doi.org/10.1109/infcom.2010.5462216 doi: 10.1109/infcom.2010.5462216

Pratiwi, M. E., Lorosae, T. A., & Wibowo, F. W. (2018, December). Phishing site detection analysis using artificial neural network. *Journal of Physics: Conference Series*, *1140*, 012048. Retrieved from https://doi.org/10.1088/1742-6596/1140/1/012048 doi: 10.1088/1742-6596/1140/1/012048

Ramasubramanian, K., & Singh, A. (2018, December). Deep learning using keras and TensorFlow. In *Machine learning using r* (pp. 667–688). Apress. Retrieved from https://doi.org/10.1007/978-1-4842-4215-5_11 doi: 10.1007/978-1-4842-4215-5_11

Rosiello, A. P. E., Kirda, E., Kruegel, C., & Ferrandi, F. (2007). A layout-similarity-based approach for detecting phishing pages. In *2007 third international conference on security and privacy in communications networks and the workshops - SecureComm 2007.* IEEE. Retrieved from https://doi.org/10.1109/seccom.2007.4550367 doi: 10.1109/seccom.2007.4550367

Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019, March). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, *117*, 345–357. Retrieved from https://doi.org/10.1016/j.eswa.2018.09.029 doi: 10.1016/j.eswa.2018.09.029

Sahoo, D., Liu, C., & Hoi, S. C. H. (2017). Malicious URL detection using machine learning: A survey. *CoRR*, *abs/1701.07179*. Retrieved from http://arxiv.org/abs/1701.07179

Sameen, M., Han, K., & Hwang, S. O. (2020). PhishHaven—an efficient real-time AI phishing URLs detection system. , *8*, 83425–83443. Retrieved from https://doi.org/10.1109/access.2020.2991403 doi: 10.1109/access.2020.2991403

Sánchez-Paniagua, M., Fidalgo, E., González-Castro, V., & Alegre, E. (2020, August). Impact of current phishing strategies in machine learning models for phishing detection. In *13th international conference on computational intelligence in security for information systems (CISIS 2020)* (pp. 87–96). Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-030-57805-3_9 doi: 10.1007/978-3-030-57805-3_9

Scarselli, F., Gori, M., Tsoi, A. C., Hagenbuchner, M., & Monfardini, G. (2009, January). The graph neural network model. *IEEE Transactions on Neural Networks*, *20*(1), 61–80. Retrieved from https://doi.org/10.1109/tnn.2008.2005605 doi: 10.1109/tnn.2008.2005605

Settles, B. (2009). *Active learning literature survey* (Computer Sciences Technical Report No. 1648). University of Wisconsin–Madison.

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell system technical journal*, *27*(3), 379–423.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing phil. In *Proceedings of the 3rd symposium on usable privacy and security - soups' 07.* ACM Press. Retrieved from https://doi.org/10.1145/1280680.1280692 doi: 10.1145/1280680.1280692

Shirazi, H., Bezawada, B., Ray, I., & Anderson, C. (2019). Adversarial sampling attacks against phishing detection. In *Data and applications security and privacy XXXIII* (pp. 83–101). Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-030-22479-0_5 doi: 10.1007/978-3-030-22479-0_5

SLCERT. (2020). Annual activity report 2020. *Sri Lanka CERT Annual Reports. Retrieved November, 04*, 15.

Smadi, S. (2017). *Detection of online phishing email using dynamic evolving neural network based on reinforcement learning* (Unpublished doctoral dissertation). Northumbria University.

Subasi, A., Molah, E., Almkallawi, F., & Chaudhery, T. J. (2017, November). Intelligent phishing website detection using random forest classifier. In *2017 inter-*

national conference on electrical and computing technologies and applications (ICECTA). IEEE. Retrieved from `https://doi.org/10.1109/icecta.2017.8252051` doi: 10.1109/icecta.2017.8252051

Sutton, R. S., & Barto, A. G. (2018). *Reinforcement learning: An introduction.* MIT press.

Tally, G. (2009, March). Phisherman: A phishing data repository. In *2009 cybersecurity applications & technology conference for homeland security.* IEEE. Retrieved from `https://doi.org/10.1109/catch.2009.24` doi: 10.1109/catch.2009.24

Tally, G., Sames, D., Chen, T., Colleran, C., Jevans, D., Omiliak, K., & Rasmussen, R. (2006, July). The phisherman project: Creating a comprehensive data collection to combat phishing attacks. *Journal of Digital Forensic Practice*, *1*(2), 115–129. Retrieved from `https://doi.org/10.1080/15567280601015564` doi: 10.1080/15567280601015564

Tchakounté, F., Wabo, L. K., & Atemkeng, M. (2020). A review of gamification applied to phishing.

Teraguchi, N. C. R. L. Y., & Mitchell, J. C. (2004). Client-side defense against web-based identity theft. *Computer Science Department, Stanford University. Available: http://crypto. stanford. edu/SpoofGuard/webspoof. pdf*.

Thakur, T., & Verma, R. (2014). Catching classical and hijack-based phishing attacks. In (pp. 318–337). Springer International Publishing. Retrieved from `https://doi.org/10.1007/978-3-319-13841-1\_18` doi: 10.1007/978-3-319-13841-1_18

Tizhoosh, H. R. (2005). Reinforcement learning based on actions and opposite actions. In *International conference on artificial intelligence and machine learning* (Vol. 414).

Verma, R. M., Zeng, V., & Faridi, H. (2019, November). Data quality for security challenges. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security.* ACM. Retrieved from `https://doi.org/10.1145/3319535.3363267` doi: 10.1145/3319535.3363267

Villiers, M. R. R. D. (2012). Models for interpretive information systems research, part 1. In *Research methodologies, innovations and philosophies in software systems engineering and information systems* (pp. 222–237). IGI Global. Retrieved from `https://doi.org/10.4018/978-1-4666-0179-6.ch011` doi: 10.4018/978-1-4666-0179-6.ch011

Wang, W., Zhang, F., Luo, X., & Zhang, S. (2019, October). PDRCNN: Precise phishing detection with recurrent convolutional neural networks. *Security and Communication Networks*, *2019*, 1–15. Retrieved from `https://doi.org/10.1155/2019/2595794` doi: 10.1155/2019/2595794

Wen, Z. A., Lin, Z., Chen, R., & Andersen, E. (2019, May). What.hack. In *Proceedings of the 2019 CHI conference on human factors in computing systems.* ACM. Retrieved from `https://doi.org/10.1145/3290605.3300338` doi: 10.1145/3290605.3300338

Wu, C.-Y., Kuo, C.-C., & Yang, C.-S. (2019, August). A phishing detection system based on machine learning. In *2019 international conference on intelligent computing and its emerging applications (ICEA).* IEEE. Retrieved from `https://doi.org/10.1109/icea.2019.8858325` doi: 10.1109/icea.2019.8858325

Yang, P., Zhao, G., & Zeng, P. (2019). Phishing website detection based on multidimensional features driven by deep learning. *IEEE Access*, *7*, 15196–15209. Retrieved from `https://doi.org/10.1109/access.2019.2892066` doi: 10.1109/access.2019.2892066

Younis, Y. A., & Musbah, M. (2020, August). A framework to protect against phishing attacks. In *Proceedings of the 6th international conference on engineering & MIS 2020.* ACM. Retrieved from `https://doi.org/10.1145/3410352.3410825` doi: 10.1145/3410352.3410825

Yu, W. D., Nargundkar, S., & Tiruthani, N. (2008, July). A phishing vulnerability analysis of web based systems. In *2008 IEEE symposium on computers and communications.* IEEE. Retrieved from `https://doi.org/10.1109/iscc.2008.4625681` doi: 10.1109/iscc.2008.4625681

Yue, C., & Wang, H. (2008). Anti-phishing in offense and defense. In *2008 annual* *computer security applications conference (acsac)* (pp. 345–354).

Zauner, C. (2010). Implementation and benchmarking of perceptual image hash functions.

Zeng, V., Baki, S., Aassal, A. E., Verma, R., Moraes, L. F. T. D., & Das, A. (2020, March). Diverse datasets and a customizable benchmarking framework for phishing. In *Proceedings of the sixth international workshop on security and privacy analytics.* ACM. Retrieved from `https://doi.org/10.1145/3375708.3380313` doi: 10.1145/3375708.3380313

Zhang, Y., Hong, J. I., & Cranor, L. F. (2007). Cantina. In *Proceedings of the 16th international conference on world wide web - www' 07.* ACM Press. Retrieved from `https://doi.org/10.1145/1242572.1242659` doi: 10.1145/1242572.1242659

Zhao, L., Sukthankar, G., & Sukthankar, R. (2011, October). Incremental relabeling for active learning with noisy crowdsourced annotations. In *2011 IEEE third int'l conference on privacy, security, risk and trust and 2011 IEEE third int'l conference on social computing.* IEEE. Retrieved from `https://doi.org/10.1109/passat/socialcom.2011.193` doi: 10.1109/passat/socialcom.2011.193