


## Report on Phishing Detection and Machine Learning


Organized by IEEE Computer Society and Cyber Security of Excellence (CCoE) a joint initiative of DSCI and the Government of Telangana on 14<sup>th</sup> September 2020 from 5:00 pm to 6:15 pm

Mr. Sriram started the session by addressing the gathering and sharing his views on “Cyber Security” which is booming right now. He explained briefly about the Importance of cybersecurity and the vulnerability of data we are facing in this virtual world and great initiatives by them like Indian Dutch Cyber Security (IDCS) 2020 collaborated with Russia which is going to be held this October.

Later Dr. Bruhadeswar Bezawada Professor & Head of the Computer Science & Engineering Department at Mahindra Ecole Centrale took on the stage and explained on the topic “Phishing Detection and Machine Learning”. He said phishing website that really look like a real website where there will be a financial loss and lot of things goes wrong for the users and URL Phishing where the attackers using these sites for their benefit and challenges in phishing detection and solutions.

### Our Story

The infographic is set against a dark blue background with a faint world map. On the left, there is a white trophy icon. To its right, there are three paragraphs of white text. In the center-right, there is a white laptop icon with a blue padlock on its screen. Lines connect the text paragraphs to the laptop icon. The bottom right corner of the infographic has a decorative orange and blue triangle.

 The Cybersecurity Centre of Excellence (CCoE) is a joint initiative of Data Security Council of India (DSCI) and the Government of Telangana.

The CCoE is created to accelerate the cybersecurity and privacy momentum and create a conducive cybersecurity and privacy ecosystem which *nurtures innovation, entrepreneurship and capability building.*

It aims to provide a secure and resilient cyberspace to fulfil the needs of the digital economy and society by creating a GLOCAL cluster of cybersecurity organizations.

He gave great inputs on how to identify a phishing website and protect our data from the attackers and vulnerability level of phishing instances. Applied adversarial sampling techniques to evaluate the robustness of the trained model against the artificially generated adversarial samples. Introduced an approach to manipulate phishing instances and create new samples and demonstrated the shortcoming of using features such as URL length. Low feature extraction and classification time suitable for real-world deployment

## LIFECYCLE OF PHISHING DETECTION SOLUTIONS

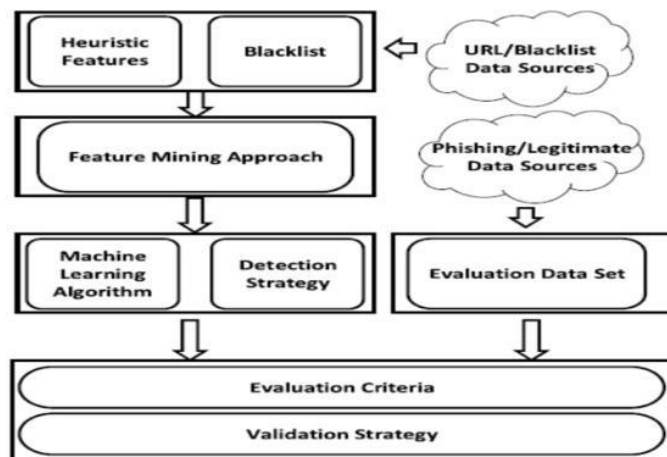


Image credit: Dou, Z., Khalil, I., Khreishah, A., Al-Fuqaha, A., & Guizani, M. (2017). Systematization of Knowledge (SoK): A systematic review of software-based web phishing detection. *IEEE Communications Surveys & Tutorials*, 19(4), 2797-2819.

Elimination of the possible bias in classification due to differently chosen datasets of phishing and legitimate pages and difficulty to bypass for attacker as our features explore the content found in the visible space of the web page Averaging the vulnerability level of each of the selected instances. Phishing is real problem and difficult to address.

He concluded the session with adding message for every individual to be careful from the phishing attacks and also to learn necessary precautions methods.