Internships

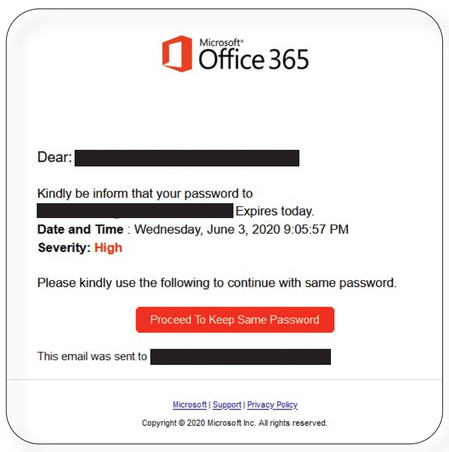
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

CBG Cyber@ Ben-Gurion University of the Negev

Cyber@BGU is an umbrella organization at Ben Gurion University, being home to various cyber security, big data analytics and AI applied research activities.Residing in newly established R&D center at the new Hi-Tech park of Beer Sheva (Israel's Cyber Capital), Cyber@BGU serves as a platform for the most innovative and technologically challenging projects with various industrial and governmental partners.

URL-BASED PHISHING DETECTION USING TRANSFER LEARNING

1 problem



Malicious websites pose as legitimate sites in order to lure individuals into providing sensitive information such as bank details, etc.

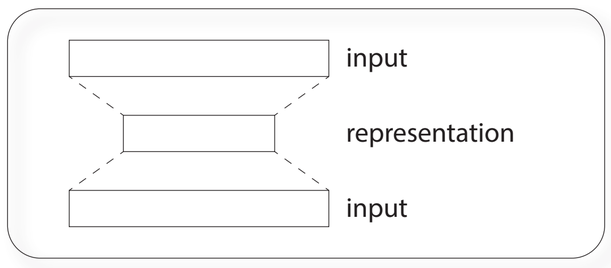
There have been research work into building systems that automatically classifies URLs as potential phishing sites. However, these models only work when tested under controlled environments; They are unable to generalise well to external, real-world data.

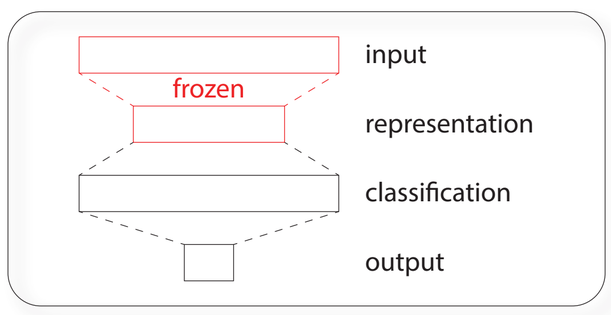
Can we build a system that solves this issue?

2 idea

Train an auto-encoder on to learn a "summarised" representation of URL features

Unlabelled data sets (meant to simulate real-world conditions) are used to train the auto-encoder





Freeze encoding layers, and use the learned representation as inputs to the classification layers

Labelled data sets (URLs with a malicious/benign label) are used as inputs for training

Obtain models' predictions of the unlabelled URLs and estimate false positive rate by verifying if URLs predicted to be malicious are actually malicious

Other than auto-encoders, other model architectures and features were used, developed and tested.

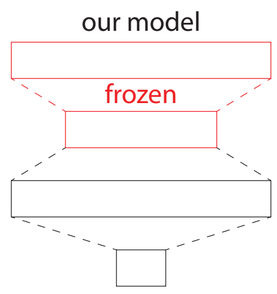
These include: character frequencies, trigram extraction, attention networks, and LSTM-based models.

3 results

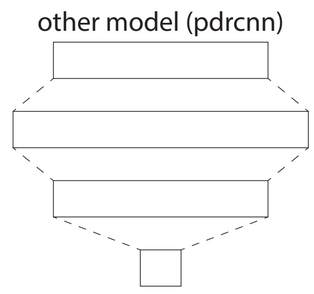
Our models outperformed other competitive models.

Internally, within the set of models designed and tested, the architecture that utilised auto-encoders and trigram-encodings gave the best performance.

statistics



val acc. 0.93
val f1 0.93
eval fpr* 0.50



val acc. 0.94
val f1 0.94
eval fpr* 0.89

* false positive rate (lower is better)

KEY TAKEAWAYS

1 research

Keep an open mind and learn as much as you can. Research is a lot of trying various things (within reason) and seeing what sticks. Results can be unprecedented (and even negative) but that's fine, they're still results.

2 responsibility

Telecommuting overseas basically meant I was left to my own devices for the most part. In scenarios such as these, it is important to take charge of your responsibilities and ensure that you can complete your work on time.

Jeremy Chew ISTD