Internship Report for January - February 2018

Yash Saboo

2015-2019 Batch

T.Y.C.S.

15070121170

# ABOUT THE COMPANY

**Symantec Corporation** is a Fortune 500 company headquartered in Mountain View, USA. It specializes in digital security. Products such as Norton Antivirus and Norton Mobile Security have made it a household name. Besides these products, Symantec also has presence in areas such as data loss prevention (Backup Services), Anti-Theft Measures and Continuous Availability of Data. Symantec also secures many online transactions, which can be recognized from its famous logo with *the yellow circle and the black check mark (as seen below)*. In fact, it is the most used certification authority in the world, as found out by NetCraft. It operates in 40 countries with 3 offices in India in Pune, Bengaluru, and Chennai.



# ABOUT THE PROJECT

**Problem Statement:**

To develop a Google Chrome Web Extension which can detect phishing/imitation websites and alert users about the same based on previously browsed websites.

**Technology Used and Technical Details:**

The technologies are unknown yet because the proof of concept must be developed concretely before we move on to the technical details. Once I am finished with Literature Survey, my task is to find evidence which demonstrates that the algorithms and methods, which we intend to apply, are feasible or not. If it is feasible, then we'll move on ahead with the project and consider technical aspects.

**Background Information:**

My aim for the first month was to seek out the background information of the project and understand the fundamental concepts required for the project. The overall details of the task are bound by a confidentiality clause but I have briefly mentioned what all task I did to get the background information of the project.

**Benchmarks:**

The first month is basically given to understand the ins-and-outs of the project that I’ll be working on. The second month is dedicated to Literature Survey and to demonstrate that the product being developed is feasible. If POC (Proof-of-concept) results that it is feasible, then we’ll start to implement the project. The concrete timeline of the project execution will then be planned accordingly.

# 

# TASKS DONE

* Understand the following concepts from the Symantec’s wiki page:
  + What exactly is a malware?
  + What are the types of malware?
  + What exactly makes a malware fall in a specific category?
* Listen to Tech Talks given by Symantec Executives on Malware Analysis
* Imitate a Phisher and implement live phishing.
  + I successfully phished using a type of Phishing called Email Spam Phishing.
  + I imitated as LinkedIn official and gathered the Sign In details – Username and Password - of the user by phishing.
* Once I successfully executed the live phishing, I explored following topics:
  + How Phishing Works in detail?
  + Ways to avoid Phishing
  + Case Studies on Phishing
* After learning above topics, I acted as a user who got phished and understand what are the impotence of a user which facilitates Phishing in real world.
* As the final aim is to develop a software product, I examined various software, hardware, chrome plugins and simulations already present in the market, and understand their rudimentary working. To help me in this domain, I also explored various research papers that were published on Anti-Phishing Techniques.

At the end of January, I was assigned to explore, exclusively, the algorithms and methods that will be used by the anticipated product and work on proof-of-concept. They will be described in the next report (February - March).