**Part A:**

Phishing is a method of trying to gather personal information using deceptive emails and websites. The goal of phishing is to trick an email recipient into believing that the message is something they want or need such as a request from bank or note from someone in their company to click a link or download an attachment. It is a form of fraud in which an attacker masquerades as a reputable entity or person in email or any other forms of communication. A phishing website is a fake website designed by cybercriminals to mainly commit fraud actions and distribute malware/virus computer. In terms of website interface and uniform resource locator (URL), most phishing webpages look identical to the actual webpages. There are some features and characteristics that can detect that this website is phishing or not such as:

1. IP address.

If the domain name has an IP address as an alternative of the domain name in the URL, such as “http://125.98.3.123/fake.html”, then users can be sure that someone is trying to steal their personal information. Also, sometimes, the IP address is even transformed into hexadecimal code as shown in the following link “http://0x58.0xCC.0xCA.0x62/2/paypal.ca/index.html”.

1. Long URL to Hide the Suspicious Part.

Phishers can use long URLs to hide the doubtful part in the address bar. For example:

<http://federmacedoadv.com.br/3f/aze/ab51e2e319e51502f416dbe46b773a5e/?cmd=_home&amp;dispatch=11004d58f5b74f8dc1e7c2e8dd4105e811004d58f5b74f8dc1e7c2e8dd4105e8@phishing.website.html>

If the length of the URL is greater than or equal 54 characters, then the URL classified as phishing.

1. Using URL Shortening Services “TinyURL”.

URL shortening is a method on the “World Wide Web” in which a URL may be made considerably smaller in length and still leads to the required webpage. This is accomplished by means of an “HTTP Redirect” on a domain name that is short, which links to the webpage that has a long URL. For example, the URL “http://portal.hud.ac.uk/” can be shortened to “bit.ly/19DXSk4”.

1. URL’s having “@” Symbol.

Using “@” symbol in the URL leads the browser to ignore everything preceding the “@” symbol and the real address often follows the “@” symbol.

1. Adding Prefix or Suffix Separated by (-) to the Domain.

The dash symbol is rarely used in legitimate URLs. Phishers tend to add prefixes or suffixes separated by (-) to the domain name so that users feel that they are dealing with a legitimate webpage. For example, <http://www.Confirme-paypal.com/>.

1. Domain Registration Length.

Because of a phishing website lives for a short time, and trustworthy domains are regularly paid for several years. So, the longest fraudulent domains maybe used for one year or less. So. If the domain expires in one year or less, then this website is considered almost phishing website.

1. Favicon

A favicon is a graphic image (icon) associated with a specific webpage. Many existing user agents such as graphical browsers and newsreaders show favicon as a visual reminder of the website identity in the address bar. If the favicon is loaded from a domain other than that shown in the address bar, then the webpage is likely to be considered a Phishing attempt.

**Part B:**

The DNN model used for this experiment in detecting phishing websites uses Keras and Tensorflow libraries. It has three layers (the input layer has 256 neurons with Sigmoid as an activation function, the hidden layer with 10 neurons with ReLU as an activation function, and the output layer from 1 neuron and Softmax as an activation function). Also, the model use Adam as an optimizer and ‘binary\_crossentropy’ as a loss function.