**The Objective**

Develop a model that predicts/classifies whether a website is a Phishing website.

explaination:

Fraudsters send fake emails or set up fake web sites that mimic Yahoo!'s sign-in pages (or the sign-in pages of other trusted companies, such as eBay or PayPal) to trick you into disclosing your user name and password. This practice is sometimes referred to as "phishing" — a play on the word "fishing" — because the fraudster is fishing for your private account information. Typically, fraudsters try to trick you into providing your user name and password so that they can gain access to an online account. Once they gain access, they can use your personal information to commit identity theft, charge your credit cards, empty your bank accounts, read your email, and lock you out of your online account by changing your password.

If you receive an email (or instant message) from someone you don't know directing you to sign in to a website, be careful! You may have received a phishing email with links to a phishing website. A phishing website (sometimes called a "spoofed" site) tries to steal your account password or other confidential information by tricking you into believing you're on a legitimate website. You could even land on a phishing site by mistyping a URL (web address).

Is that website legitimate? Don't be fooled by a site that looks real. It's easy for phishers to create websites that look like the genuine article, complete with the logo and other graphics of trusted website

Important: If you're at all unsure about a website, do not sign in. The safest thing to do is to close and then reopen your browser, and then type the URL into your browser's URL bar. Typing the correct URL is the best way to be sure you're not redirected to a spoofed site.