# Team Members

J.M.Lindamulage -team leader

Mandira Pabasari L.-member

Yapa S.P.J.- member

Perera I.S.S.-member

Supervisor – Ms.Jenny Krishara

# Background

Phishing has become one of the most common cyberattacks today. Attackers launch phishing attacks now in a variety of ways, like spoof calls, messages, social networking, and emails, with the intention of obtaining sensitive information from victims. The most common way victims fall for phishing is by clicking on a fraudulent link in an email that was sent by an attacker. This is called email phishing. This link will take victims to websites that appear legitimate but are run by the attackers. Attackers construct illegal email accounts using real company details and send the email to victims, impersonating a real person, while making the victim click on the link to the fraud website using social engineering. If a person clicks on the link and visits the site and tries to login or perform any action, then the attackers can get passwords, login credentials, credit card information, and other sensitive information.

**PhishTrap**

**Main objective**

**To develop a mobile app that runs in the background and a web browser extension that is capable of classifying phishing websites from legitimate websites powered by machine learning and deep learning models to provide the user with warnings regarding any potential risk of being navigated into a phishing website while preserving the privacy of the user, and if the user gets a phishing email, warn the user before the user clicks on any links or is misled by false information.**

**Research Problems**