Task2

As a member of the cyber security division, your team must handle this incident and the team lead has assigned the issue to you. Below is the timeline of events:

10:30 a.m. – The IT Service Desk receives a report from one of your colleagues at the bank that they have received an email from HR telling all employees to update their timesheets in the company's support portal so the timesheets can be approved on time by their line managers against the next pay day. The colleague clicked the link in the email that opened what looked like the portal. However, following the employee's input of the user credentials, an unfamiliar error page appeared like the one below.

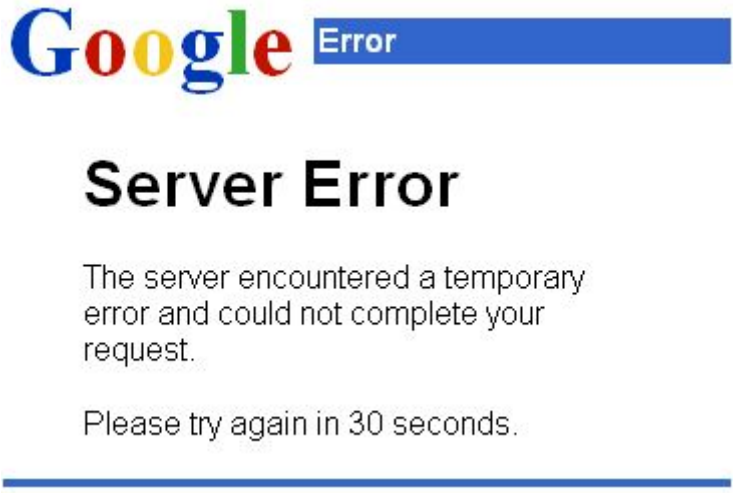

Fig. 1: Google error.png

2:00 p.m. – Eight more reports of emails similar to the one reported earlier are received by the IT Service Desk. Upon further investigation, it was found that 62 colleagues across the Risk Department received the same email over the course of two days. The emails directed the users to a fake website to steal their usernames and passwords and download a harmful program.

3:50 p.m. – The IT Service Desk receives calls and emails from more colleagues that the file-shares are not opening and they receive an error when trying to open a Word document they have always been able to open.