**GO phish Instruction Sheet**

1. **Open command prompt**
2. **Using ‘cd’ move to file directory.**

For example, you can type: *cd file/path*

1. **If not already on device install python –**

<https://www.python.org/downloads/>

1. **Enter following commands into terminal –**

‘python user\_interface\_build.py’

1. **If errors are shown you need to Install Packages using pip -**

pip install customtkinter

pip install imapclient

pip install bs4

pip install pandagui

pip install pandas

pip install requests

pip install matplotlib

pip install selenium

pip install pandas

pip install pandasgui

pip install scikit-learn

pip install nltk

1. **Alternatively, you can open the project in an IDE and install the packages there using the terminal and then click start to run the code.**

**About –**

**GO-Phish is an email-based phishing detection tool that be connected to your mailbox. It has the capabilities to investigate a potential phishing URL through the VirusTotal API or its very own custom built machine learning model. If you want to see what the webpage looks like, just simply select a URL and click the screenshot button which will show you the webpage in seconds ! And if you’re worried someone has clicked the link or received the same email just click on the search logs button to investigate further 😊**

**Tool Help –**

1. Virus Total is a service that can take a URL and check it against multiple security vendors and report back if the URL may be malicious or clean!

**Remember: The API is an open-source intelligence tool so its important you do not just use this technique by itself as it very well could tell you a link is clean but in reality, it is not !**

1. The machine learning in this tool is a smart bit of code that can take a URL and predict if it can be phishing or not, it will give you a prediction score to tell you how likely it is a phishing URL.
2. The redirect label is populated when you scan a URL, it checks that there is no redirects within the link that might take you to another web page!  
   **Hint: If the redirect link is very different to the URL in the email it is likely they are directing you to a phishing website!**
3. The ‘search logs’ button searches through your mail server logs for any emails that have the same sender. It can also check for anyone who has visited the URL within your business.

**Hint: This can help you find more phishing emails, if the email you are exploring is phishing and the logs show this sender has sent other emails it is likely these emails are also phishing!**

**Tips:**

**Check the grammar of the email?**

**Check the sender of the email, is it trying to pretend to be someone it isn’t?**

**Is the webpage trying to redirect you?**

**Does the webpage look like a fake log in page?**

**Are there any POST 200 connections to the URL! This shows someone has entered their credentials!**