# Phishing Analysis Tools

## Task 3 Email header analysis

ANSWER: capitalone.com

## Task 4 Email body analysis

ANSWER: Copy Link Location

## Task 6 PhishTool

ANSWER: #454326\_PDF.exe

## Task 7 Phishing Case 1

ANSWER 1: Netflix

ANSWER 2: N e t f l i x JGQ47wazXe1xYVBrkeDg-JOg7ODDQwWdR@JOg7ODDQwWdR-yVkCaBkTNp.gogolecloud.com

ANSWER 3: 209[.]85[.]167[.]226

ANSWER 4: etekno[.]xyz

ANSWER 5: hxxps[://]t[.]co/yuxfZm8KPg?amp=3D

## Task 8 Phishing Case 2

ANSWER 1: Suspicious activity

ANSWER 2: Payment-updateid.pdf

ANSWER 3: CC6F1A04B10BCB168AEEC8D870B97BD7C20FC161E8310B5BCE1AF8ED420E2C24

ANSWER 4: 2[.]16[.]107[.]24,2[.]16[.]107[.]83

ANSWER 5: svchost.exe

## Task 9 Phishing Case 3

ANSWER 1: Malicious activity

ANSWER 2: CBJ200620039539.xlsx

ANSWER 3: 5f94a66e0ce78d17afc2dd27fc17b44b3ffc13ac5f42d3ad6a5dcfb36715f3eb

ANSWER 4: findresults[.]site,biz9holdings[.]com, ww38[.]findresults[.]site

ANSWER 5: 75[.]2[.]11[.]242,103[.]224[.]182[.]25,204[.]11[.]56[.]48

ANSWER 6: CVE-2017-11882