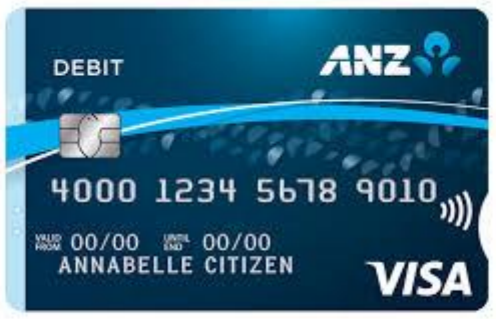
Cyber @ ANZ Internship

Digital Investigation

Submitted by: Valency Colaco, Masters of Information Technology, University of Sydney

Sub-task 1:

- *anz-logo.jpg and bank-card.jpg are two images that show up in the user's network traffic.*
- *I followed the TCP Stream for both the files, copied the contents between FFD8 and FFD9 which is a JPG Signature into the HEX Editor and saved the files in .jpg format as shown below,*

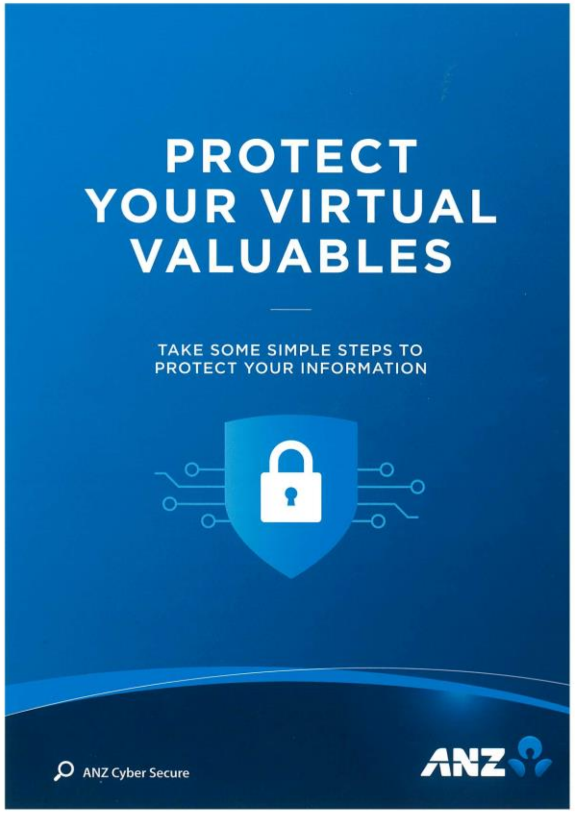


bank-card.jpg

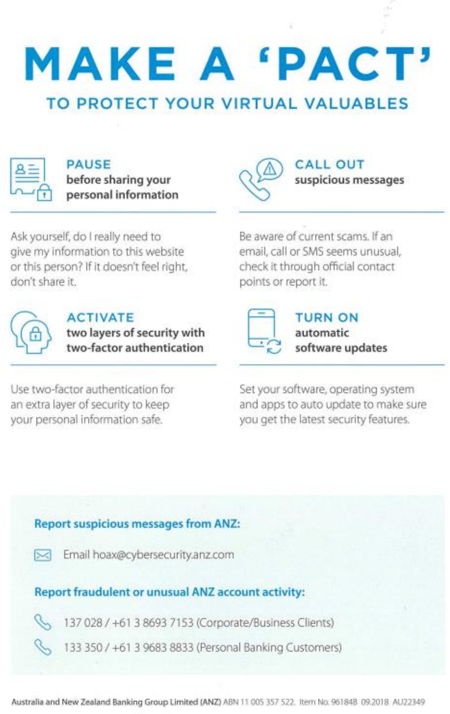
anz-logo.jpg

Sub-task 2:

- *The network traffic for the images "ANZ1.jpg" and "ANZ2.jpg" is more than it appears.*
- *I followed the TCP Stream for both files and got the following messages at the end of the stream,*
  - ○ *You've found a hidden message in this file! Include it in your write up.*
  - ○ *You've found the hidden message!*
    Images are sometimes more than they appear.
- *I, then copied the contents between FFD8 and FFD9 into the HEX Editor for both files and saved them as .jpg files as shown below,*


PROTECT YOUR VIRTUAL VALUABLES
TAKE SOME SIMPLE STEPS TO PROTECT YOUR INFORMATION
ANZ Cyber Secure
ANZ

ANZ1.jpg



MAKE A 'PACT'
TO PROTECT YOUR VIRTUAL VALUABLES

PAUSE
before sharing your personal information

Ask yourself, do I really need to give my information to this website or this person? If it doesn't feel right, don't share it.

CALL OUT
suspicious messages

Be aware of current scams. If an email, call or SMS seems unusual, check it through official contact points or report it.

ACTIVATE
two layers of security with two-factor authentication

Use two-factor authentication for an extra layer of security to keep your personal information safe.

TURN ON
automatic software updates

Set your software, operating system and apps to auto update to make sure you get the latest security features.

Report suspicious messages from ANZ:

Email hoax@cybersecurity.anz.com

Report fraudulent or unusual ANZ account activity:

137 028 / +61 3 8693 7153 (Corporate/Business Clients)

133 350 / +61 3 9683 8833 (Personal Banking Customers)

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. Item No. 961848 09.2018 AU22349

ANZ2.jpg

Sub-task 3:

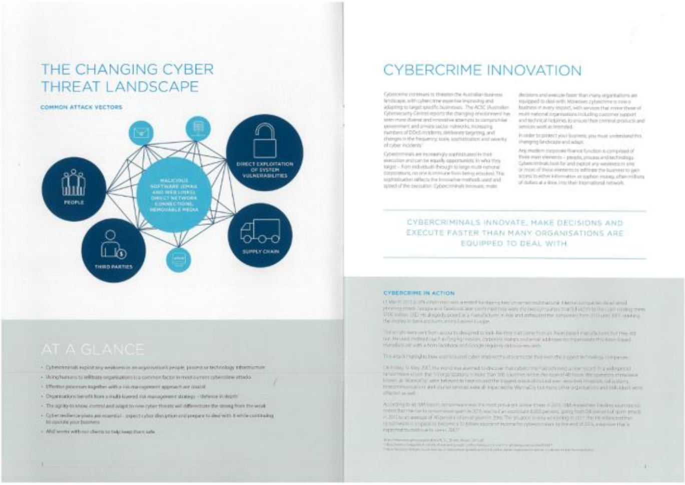
- *The user downloaded a suspicious document called "how-to-commit-crimes.docx"*
- *After following the TCP Stream, the contents of the file were revealed in plain text as follows,*

  Step 1: Find target
  Step 2: Hack them

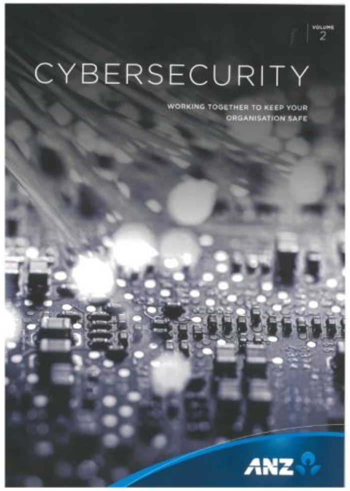
  This is a suspicious document.

Sub-task 4:

- *The user accessed 3 pdf documents: ANZ_Document.pdf, ANZ_Document2.pdf, evil.pdf*
- *After following the TCP Stream, I detected the file signature for PDF Files which is 25 50 44 46. I then copied this into a HEX Editor and saved the files as .pdf as shown below,*


THE CHANGING CYBER THREAT LANDSCAPE
COMMON ATTACK VECTORS
PEOPLE
THIRD PARTIES
MALICIOUS SOFTWARE (EMAIL AND WEB LINKS), DIRECT NETWORK CONNECTIONS, REMOVABLE MEDIA
DIRECT EXPLOITATION OF SYSTEM VULNERABILITIES
SUPPLY CHAIN
AT A GLANCE
CYBERCRIME INNOVATION
CYBERCRIMINALS INNOVATE, MAKE DECISIONS AND EXECUTE FASTER THAN MANY ORGANISATIONS ARE EQUIPPED TO DEAL WITH
CYBERCRIME IN ACTION

ANZ_Document2.pdf



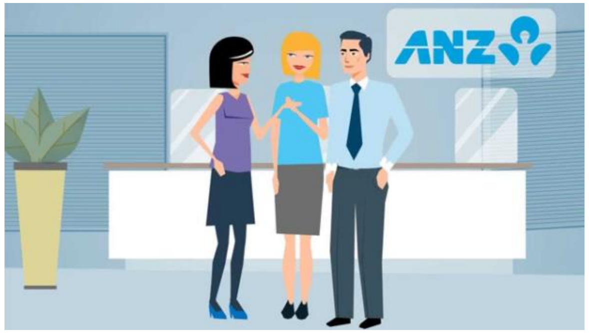
ANZ_Document.pdf

More suspicious stuff good job!

evil.pdf

Sub-task 5:

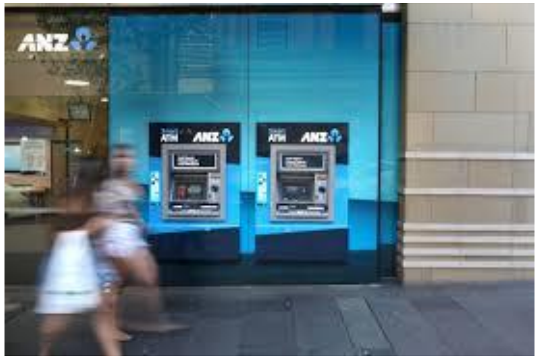
- *The user also accessed a file called "hiddenmessage2.txt"*
- *On following the TCP stream, I did not detect a text file signature, but I did detect a .jpg file signature and the image is shown below,*



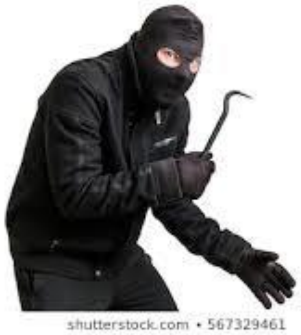
hiddenmessage2.jpg

Sub-task 6:

- *The user accessed an image called "atm-image.jpg"*
- *The request returned back two .jpg images which are shown below,*



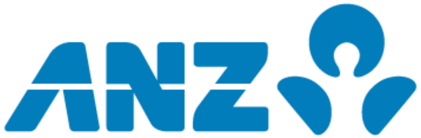
atm-image.jpg (1)



atm-image.jpg (2)

Sub-task 7:

- *The network traffic shows that the user accessed the image "broken.png"*
- *On following the TCP stream, I noticed that the data was in base64 format, which when decoded and converted into HEX and saved as a .png file yielded the image as shown below,*



broken.png

Sub-task 8:

- *The user accessed one more document called securepdf.pdf*
- *On following the TCP Stream, I noticed a message at the end which was as follows - Password is "secure"*
- *The stream did not contain a PDF Signature, but it did contain a "PKZIP archive_1" File signature of 50 4B 03 04. So, I saved the data as a .zip file shown in image 1 below,*

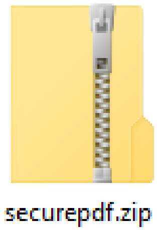


Image 1

- *The password to this .zip file was "secure" (from the message above)*
- *On extracting the .zip file, I discovered a file called rawpdf.pdf and its contents are shown below,*

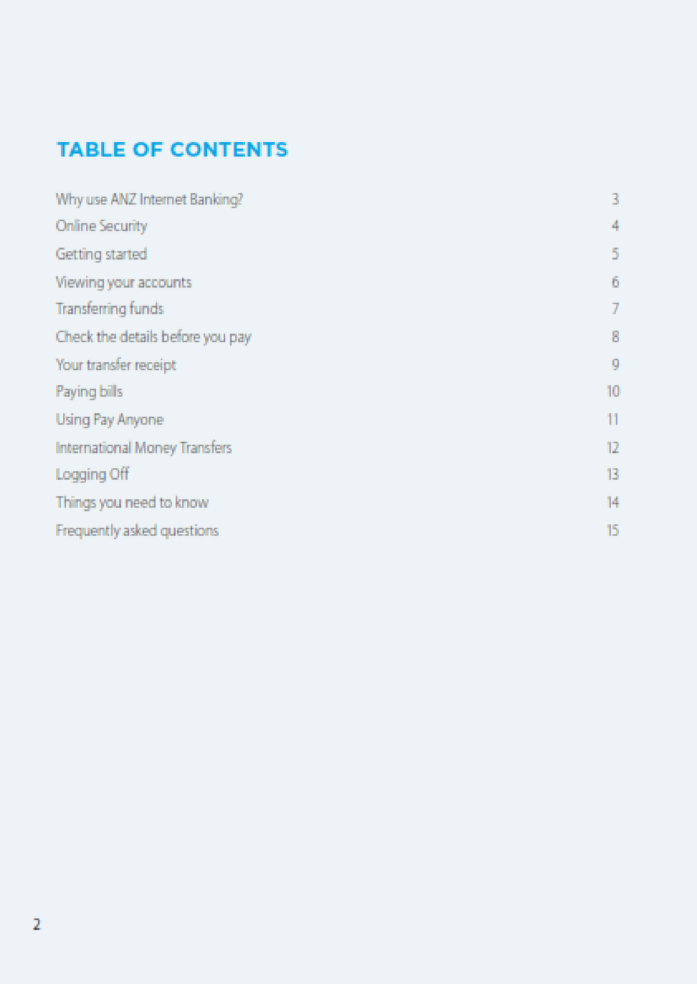
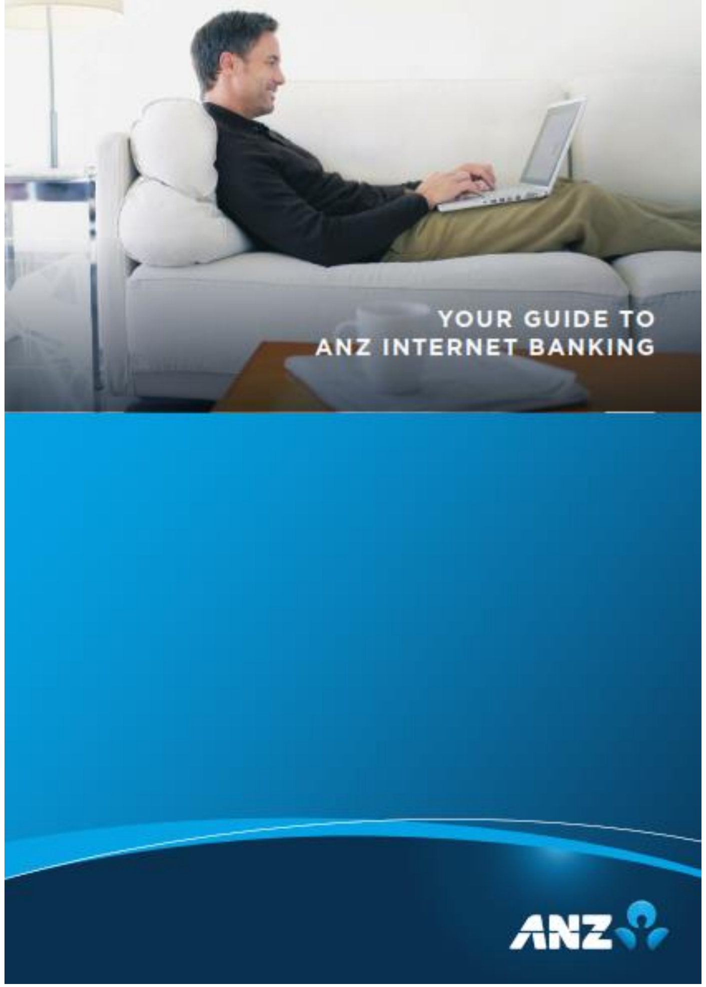


TABLE OF CONTENTS

rawpdf.pdf (1)



YOUR GUIDE TO
ANZ INTERNET BANKING

rawpdf.pdf (2)