

Week 8 - Social Engineering and IOS

Task 1

Screenshot of details being taken in via Phishing simulator

```
[ - ] Select an option : 01

  ZPHISHER 2.3.5

[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]

[ - ] Select a port forwarding service : 01

[?] Do You Want A Custom Port [y/N]: n

[ - ] Using Default Port 8080...

[ - ] Initializing... ( http://127.0.0.1:8080 )

[ - ] Setting up server...

[ - ] Starting PHP server...

  ZPHISHER 2.3.5

[ - ] Successfully Hosted at : http://127.0.0.1:8080

[ - ] Waiting for Login Info, Ctrl + C to exit...

[ - ] Victim IP Found !

[ - ] Victim's IP : 127.0.0.1

[ - ] Saved in : auth/ip.txt

[ - ] Login info Found !!

[ - ] Account : Benjamin.R.Chiu@student.uts.edu.au

[ - ] Password : Student-ID

[ - ] Saved in : auth/usernames.dat

[ - ] Waiting for Next Login Info, Ctrl + C to exit. ^C

[!] Program Interrupted.

solarslayer2@cloudshell:~/cloudshell_open/zphisher/zphisher$
```

Question 1- What happens when i get a phishing link and input my details.

The phishing link directs you to a similarly designed website login page. It is good to note that the URL is different. When inputting the details. It will lead you to an error page saying the details are wrong. However, your login details are then stolen by the owner of the phishing details (See screenshot above)

Question 2 - How do you defend yourself?

You can defend yourself by not clicking suspicious links and double checking the URL to ensure it is indeed the correct website you are logging into. Changing passwords is also a good way to prevent people using these details if you do find yourself in the situation where you have input your details in.

Task 2

Who is (Screenshot)

```

$ whois google.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-10-02T14:46:54Z
<<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

```

WGet Screenshot

```

- $ wget google.com
--2024-10-03 00:57:57-- http://google.com/
Resolving google.com (google.com)... 2404:6800:4006:80f::200e, 142.250.204.14
Connecting to google.com (google.com)|2404:6800:4006:80f::200e|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.google.com/ [following]
--2024-10-03 00:57:57-- http://www.google.com/
Resolving www.google.com (www.google.com)... 2404:6800:4006:814::2004, 142.250.71.68
Connecting to www.google.com (www.google.com)|2404:6800:4006:814::2004|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html      21.86K  --.-KB/s   in 0.01s

2024-10-03 00:57:58 (1.68 MB/s) - 'index.html' saved [2380]

```

NS Lookup Screenshot

```
- $ nslookup google.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.66.238
Name:   google.com
Address: 2404:6800:4006:811::200e
```

Curl Screenshot

```
- $ curl -i google.com
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Content-Security-Policy-Report-Only: object-src 'none'
base-uri 'self';script-src 'nonce-kENWKvVcdZqFjn6aSZer
w' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'uns
fe-inline' https: http://report-uri https://csp.withgoo
le.com/csp/gws/other-hp
Date: Wed, 02 Oct 2024 14:57:24 GMT
Expires: Fri, 01 Nov 2024 14:57:24 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN

<HTML><HEAD><meta http-equiv="content-type" content="t
xt/html; charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
- $
```