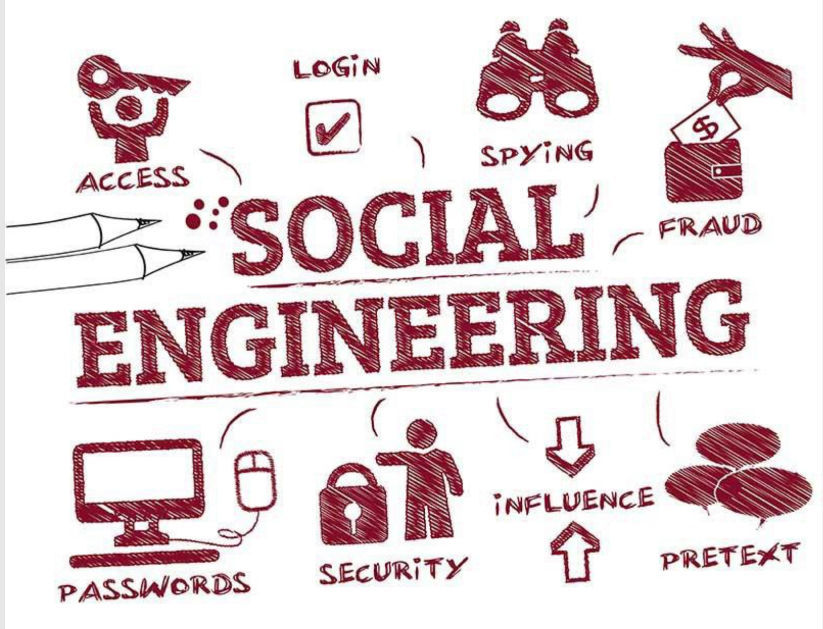
SWINBURNE UNIVERSITY OF TECHNOLOGY

Social Engineering

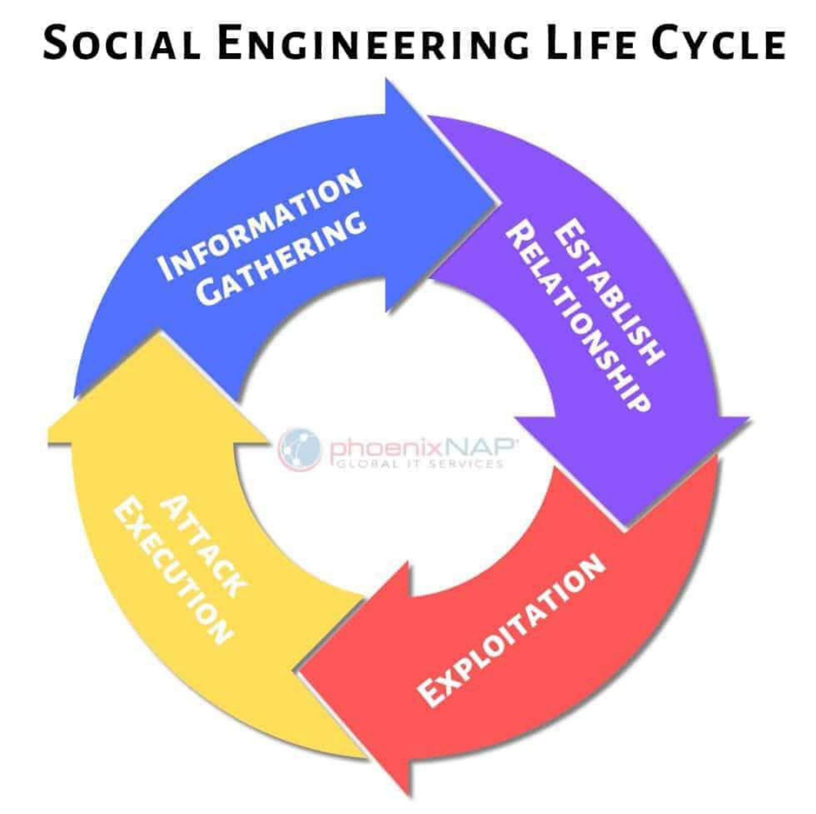
Social Engineering

- Social Engineering is a component of the attack in nearly 1 of 3 successful data breaches
- Manipulation of individuals in seeking action or the release (divulging) of sensitive information
- Influence over another which is not in their best interest



Life Cycle of Social Engineering

- Information gathering
- Engaging with victim
- Attacking
- Closing interaction



Types

Baiting: Like phishing, but using different items to lure victims
Dumpster diving: Physically sorting through rubbish
Pretexting: Providing background or pretending to be another
Phishing: Baiting with fake links to fake resources
Pharming: DNS level redirection to fake resources
Reconnaissance: Information gathering
Surveillance: Observing
Shoulder surfing: Watching over someone's shoulder for information or passwords
Tailgating: Trick employees to open doors for attackers

Baiting

- Similar to Phishing
- Different items used to entice victim
- Free music, movies, keygens, software…

Dumpster diving

- Attacker physically visits target's location and searches the rubbish to find useful information
- Financial paperwork
- User manuals (software, hardware)
- Used to support future pretexting attack

- https://youtu.be/c81NYcP2C0E

Pretexting

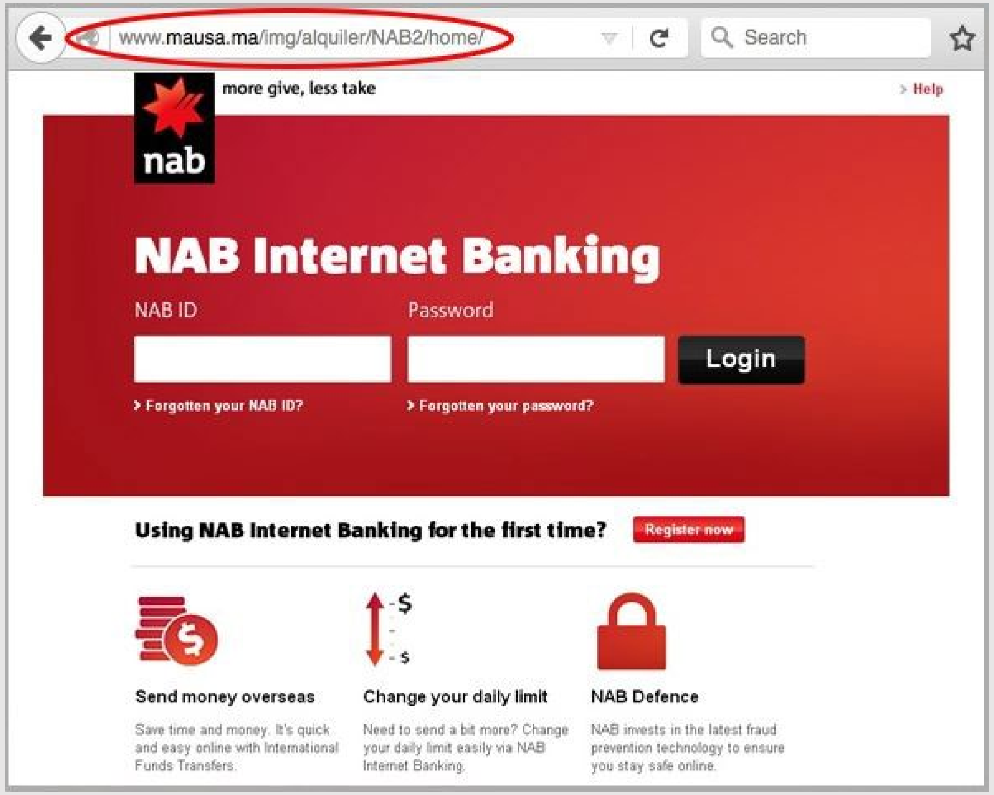
- **Defined as the practice of presenting oneself as someone else in order to obtain private information**
  - ➢ Good, compelling story
  - ➢ Fabricated scenario
  - ➢ Not a one-size fits all
    - ➢ Good targets: help desk, librarians

Phishing

- **Most phishing scams endeavour to accomplish three things:**
  - ➢ Obtain personal information
  - ➢ Redirect users to suspicious websites
  - ➢ Manipulate the user into responding quickly

Pharming

- **Setting up a fake web site which harvests user input**
  - ➢ Fake banking site
  - ➢ Uses current graphics, styles from real site
  - ➢ stores user name and password and then re-directs user to the real site
  - ➢ Fake anti-virus site (download "patches " containing malware)
  - ➢ Similar domain name to legitimate sites



www.mausa.ma/img/alquiler/NAB2/home/

more give, less take

NAB Internet Banking

NAB ID

Password

Using NAB Internet Banking for the first time?

Send money overseas

Save time and money. It's quick and easy online with International Funds Transfers.

Change your daily limit

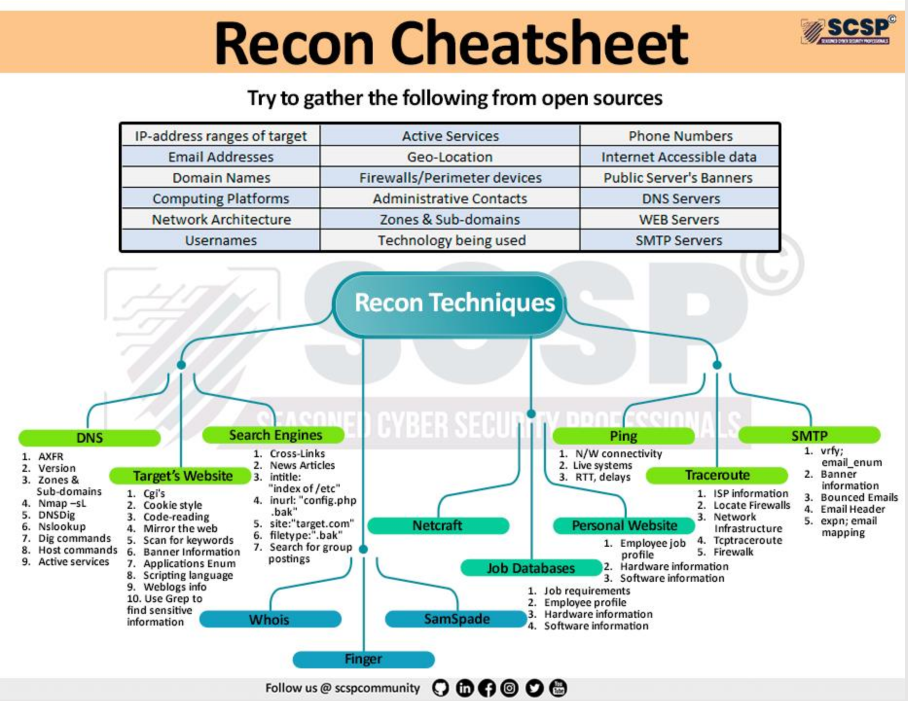
Need to send a bit more? Change your daily limit easily via NAB Internet Banking.

NAB Defence

NAB invests in the latest fraud prevention technology to ensure you stay safe online.

Reconnaissance

- **After enumerating the names of people in the Target premises, search social media f**
  password reset info.
  - ➢ Date of birth (age + birthday)
  - ➢ Names or relatives, pets
  - ➢ Car Rego
  - ➢ Password dumps from hacked sites



Recon Cheatsheet

SCSP©

Try to gather the following from open sources

IP-address ranges of target	Active Services	Phone Numbers
Email Addresses	Geo-Location	Internet Accessible data
Domain Names	Firewalls/Perimeter devices	Public Server's Banners
Computing Platforms	Administrative Contacts	DNS Servers
Network Architecture	Zones & Sub-domains	WEB Servers
Usernames	Technology being used	SMTP Servers

Recon Techniques

DNS
1. AXFR
2. Version
3. Zones & Sub-domains
4. Nmap –sL
5. DNSDig
6. Nslookup
7. Dig commands
8. Host commands
9. Active services

Target's Website
1. Cgi's
2. Cookie style
3. Code-reading
4. Mirror the web
5. Scan for keywords
6. Banner Information
7. Applications Enum
8. Scripting language
9. Weblogs info
10. Use Grep to find sensitive information

Search Engines
1. Cross-Links
2. News Articles
3. intitle: "index of /etc"
4. inurl: "config.php .bak"
5. site:"target.com"
6. filetype:".bak"
7. Search for group postings

Whois

Finger

SamSpade

Netcraft

Job Databases
1. Job requirements
2. Employee profile
3. Hardware information
4. Software information

Personal Website
1. Employee job profile
2. Hardware information
3. Software information

Ping
1. N/W connectivity
2. Live systems
3. RTT, delays

Traceroute
1. ISP information
2. Locate Firewalls
3. Network Infrastructure
4. Tcptraceroute
5. Firewalk

SMTP
1. vrfy; email_enum
2. Banner information
3. Bounced Emails
4. Email Header
5. expn; email mapping

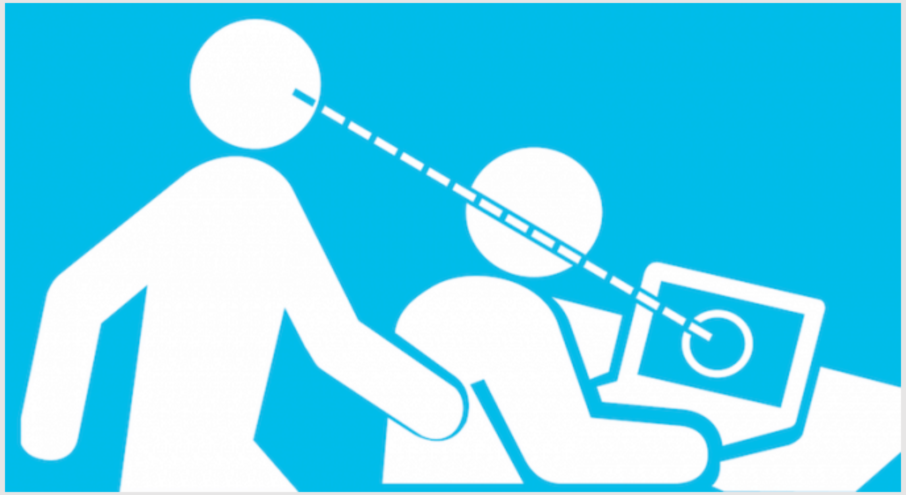
Follow us @ scspcommunity

Surveillance

- **Google Earth**
- **Street View**
- **Surveillance cams**
    - ➢ http://mashable.com/2014/11/10/naked-security-webcams/
    - ➢ https://brinkshome.com/smartcenter/hacked-home-security-cameras-list
    - ➢ http://www.insecam.org/en/bycountry/AU/

Shoulder Surfing

- After gaining entry to the target premises, attacker watches people logging on to their computers to get credentials



Tailgating

- Trick employees to open doors for attackers
- Existed in every organisation

Helpful Tips - Defence

- Slow down
- Research the facts
- Don’t let a link be in control of where you land.
- Email hijacking is rampant
- Beware of any download
- Foreign offers are fake