# Social Engineering

The use of deception to manipulate individuals into disclosing information for fraudulent purposes

# Goals

- Unauthorised Access
- Personally Identifiable Information (PII)
- Intellectual Property
- Identity Theft
- Disruption

# Threat Actors

- Malicious Insiders
- Organised Crime
- Hacktivists
- Nation States
- Terrorists
- Accidental

# Stages

- Reconnaissance
- Attack

# Reconnaissance

# Target

- New employees
- Busy people
- Non-technical people

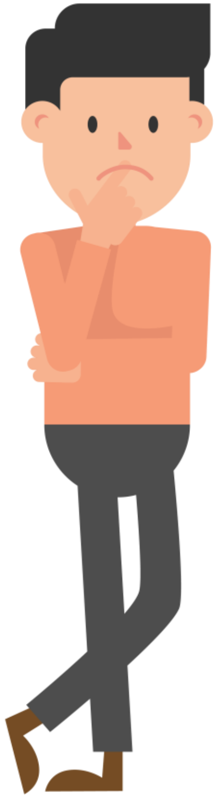


Image source: vecteezy.com

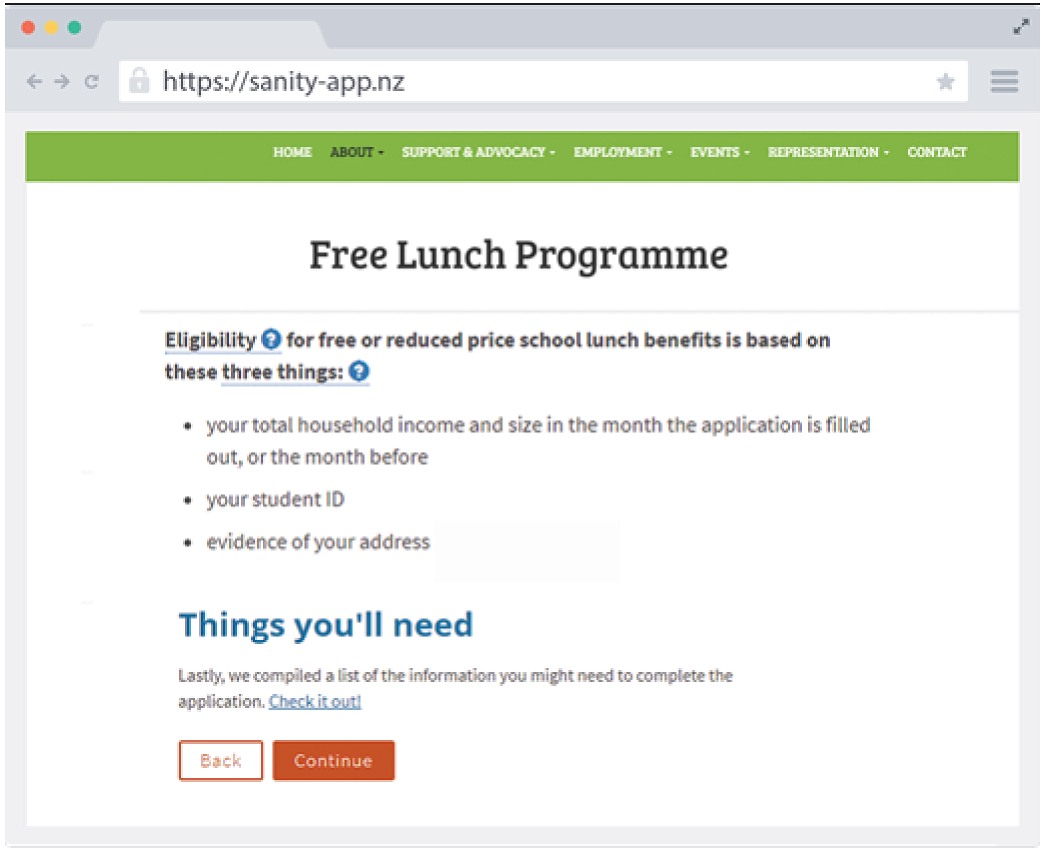
# Information

- Reconnaissance or foot printing starts with gathering harmless information, such as names, emails and phone numbers.
- Familiarity with targets can be developed and leveraged to extract more personal information.
- The information can be used to authenticate the next action.

# Attack

# Phishing

- Phishing doesn't necessarily need to involve comprising a target’s computer.
- It can simply be a method to obtain personal information from a target.



Free Lunch Programme

**Eligibility for free or reduced price school lunch benefits is based on these three things:**

- your total household income and size in the month the application is filled out, or the month before
- your student ID
- evidence of your address

Things you'll need

Lastly, we compiled a list of the information you might need to complete the application. Check it out!

# Impersonation – (Pretexting)

- Many social engineering techniques are complicated, however often a threat actor can take the direct approach and ask for the information.
- Most employees handle information as part of their job.
- Employees wouldn't give one customers information to another customer; however different rules apply for work colleagues.
- If they think the threat actor is a colleague, they can often just ask for the information.

# Trust

- Building trust is the key to deception.
- The more the threat actor can make contact seem like business as usual, the less the target will be suspicious.
- The threat actor can make multiple calls over a few weeks to build a relationship.
- Once the threat actor has gained trust the doors are open, and they may be able to ask for the information

# Other Psychological Techniques

- Sympathy,
- Guilt
- Intimidation

# Assistance

- Let me help you
- Can you help me?

# The Reverse Sting

- Laying a trap – here, the social engineer creates a situation where the target comes to them for help.
- This can be as simple as forwarding a phone call.
- When the target calls, the social engineer can ask them for identification; this can then use this information for another attack.

# Dumpster Diving

People often throw away important information

- Meeting notes
- Appointments
- Work notes

# Entering Premises

- Could be either an external or internal agent such as a disgruntled employee.
- A threat actor may prepare for a breach by going dumpster diving

# Combining Technology and Social Engineering

- Combining technology and social engineering is a powerful technique to breach security.
- This can work either by using social engineering to gain access to plant a technical device or using a technical hack to support a social engineering attack.

# Caller ID

- Caller ID can be used to hide internal direct dial numbers but this same capability, of course, provides a handy tactic for social engineers.
- Employees need to be aware that the caller id does not indicate the identity of the caller.

# Controls

# Security Awareness and Training

- Policies
- Procedures
- Guidelines
- Controls
- Education and Training

# Further Reading

Mitnick, K. D., & Simon, W. L. (2002). The art of deception: controlling the human element of security. Indianapolis, Ind: Wiley.